Inhaltsverzeichnis

1 Einführung in Funknetzwerke 1

1.1 Einteilung der Funklösungen ... 3

1.2 Geschichte der drahtlosen Kommunikation ... 4

1.2.1 Das IEEE-Konsortium ... 4
1.2.2 Der IEEE-802.11-Standard ... 5

1.3 Weitere Funklösungen ... 10

1.3.1 HiperLAN ... 10
1.3.2 HomeRF ... 12
1.3.3 Bluetooth ... 12
1.3.4 ZigBee ... 15
1.3.5 WiMax ... 16

1.4 WLAN-Rechtsgrundlagen ... 17

1.4.1 Grundstücksübergreifende Datenübertragung ... 19
1.4.2 Rechtgrundlage für Hotspots ... 19

1.5 Drahtlos versus drahtgebunden ... 23

1.5.1 Multiple-Access-Problematik ... 24
1.5.2 Modulationsverfahren ... 26
1.5.3 Die Frequenz ... 27
1.5.4 Exkurs Pegelwerte und Dezibel ... 28
1.5.5 Bitrate und Datenrate ... 30
1.5.6 Paketvermittlung versus Leitungsvermittlung ... 30

1.6 Gesundheit ... 31

1.7 OSI-Referenzmodell ... 33

1.8 Ein Überblick über den Inhalt dieses Buchs ... 40

2 WLAN-Netzwerkformen 43

2.1 Ad-hoc-Netzwerk ... 43
2.2 Infrastruktur-Netzwerk ... 45
2.3 Roaming ... 48
2.4 Datenadressierung ... 51
2.5 Drahtloser Internetzugang ... 53
2.6 Drahtlose Gebäudeanbindung ... 54
2.7 Mesh-WLANs ... 56
2.8 Hotspots ... 58
2.9 Mobile IP ... 62
2.9.1 Mobile IP-Architektur ... 64
2.9.2 Routing ... 66

3 Der 802.11 Physical Layer 69

3.1 Aufbau des Physical Layers ... 69
3.1.1 PHY-Funktionen ... 70
3.1.2 Signalspreizung ... 73
3.2 FHSS-Technologie ... 74
3.2.1 FHSS-Modulationsverfahren ... 77
3.2.2 FHSS-Frameformat ... 79
3.2.3 FHSS-PHY-Umsetzung ... 81
3.2.4 FHSS-CS/CCA ... 82
3.2.5 FHSS-CCA-Empfindlichkeit ... 83
3.2.6 FHSS-PLCP-Datenempfang ... 84
3.2.7 FHSS-PMD_SAP ... 85
3.3 DSSS-Technologie ... 87
3.3.1 DSSS-Modulationsverfahren ... 90
3.3.2 DSSS-Spreiz-Codes ... 91
3.3.3 DSSS-Frameformat ... 99
3.3.4 DSSS-Short-Frameformat ... 101
3.3.5 DSSS-Kanalaufteilung ... 102
3.3.6 DSSS-PMD_SAP ... 104
3.3.7 DSSS-PLCP-Sendeprozedur ... 106
3.3.8 DSSS-PLCP-Empfangsprozedur ... 107
3.3.9 DSSS-CCA-Empfindlichkeit ... 108
3.3.10 DSSS-Empfängerempfindlichkeit ... 109
3.3.11 DSSS-Channel Agility ... 110
3.3.12 DSSS versus FHSS ... 111

3.4 OFDM-Technologie ... 112
3.4.1 OFDM-Frameformate ... 117
3.4.2 OFDM-PPDU-Codierungsprozess ... 119
3.4.3 OFDM-Datenempfang und -Decodierung ... 128
3.4.4 OFDM-Übertragungsverfahren ... 129
3.4.5 OFDM-Modulationsverfahren ... 134
3.4.6 OFDM-PMD_SAP ... 139
3.4.7 OFDM-PLCP-Sendeprozedur ... 139
3.4.8 OFDM-PLCP-Empfangsprozedur ... 140
3.4.9 OFDM-CCA-Empfindlichkeit ... 141
3.4.10 OFDM-Empfängerempfindlichkeit ... 141
3.4.11 OFDM-Kanalaufteilung ... 142
3.5 PBCC-Technologie ... 146
3.5.1 PBCC-5,5 und PBCC-11 ... 147
3.5.2 PBCC-22 ... 150
3.5.3 PBCC-33 ... 151
3.6 Die 802.11g-PHY-Erweiterungen ... 152
3.6.1 802.11g-PPDU-Frameformat ... 155
3.6.2 802.11g-Signalspektrum ... 158
3.6.3 802.11g-Empfängerempfindlichkeit ... 158
3.7 Die IEEE-Infrarot-Technologie ... 159
3.7.1 IR-Frameformat ... 161
3.8 802.11n ... 163
3.8.1 MIMO und SIMO ... 164
3.8.2 Beamforming ... 165
3.8.3 Raum-Zeit-Codes ... 166
3.8.4 Raum-Multiplex-Verfahren ... 167
3.8.5 TGn Sync versus WWiSE ... 168
4 Der 802.11 MAC Layer 173
4.1 Problematik eines Funkmediums ... 173
4.2 Distribution Coordination Function ... 175
4.2.1 CSMA/CA ... 175
4.2.2 Virtuelle Carrier-Sense-Funktion ... 176
4.2.3 Acknowledgement ... 178
4.2.4 Interframe Space ... 178
4.3 Das Hidden-Station-Problem ... 183
4.4 Fragmentierung ... 185

4.5 802.11-Frameformat ... 187
4.5.1 Datenframes ... 194
4.5.2 Kontrollframes ... 195
4.5.3 Managementframes ... 199
4.5.4 Informationselemente ... 207
4.5.5 Managementframetypen ... 216
4.5.6 Frameklassen ... 221
4.6 Managementfunktionen ... 222
4.6.1 Passives und aktives Scanning ... 222
4.6.2 Power-Management ... 226
4.6.3 Wired-Equivalent-Privacy-Algorithmus ... 230
4.6.4 Authentifizierung ... 235
4.6.5 Assoziierung ... 238
4.6.6 Protection-Mechanismus ... 240
4.6.7 Datenratenunterstützung ... 242
4.6.8 Transmit Power Control ... 243
4.6.9 Dynamic Frequency Selection ... 244
4.7 Point Coordination Function ... 247
4.8 802.11d-Erweiterung ... 251
4.9 802.11e-MAC-Erweiterung ... 252
4.9.1 Enhanced Distribution Coordination Function ... 253
4.9.2 EDCF-TXOP-Bursting ... 256
4.9.3 Hybrid Coordination Function ... 257
5 Antennentechnik 259
5.1 Grundlagen der drahtlosen Kommunikation ... 260
5.2 Antennenprinzip ... 260
5.3 Antennenparameter ... 263
5.3.1 Impedanz ... 263
5.3.2 VSWR/Rückflussdämpfung ... 264
5.3.3 Polarisation ... 264
5.3.4 Antennengewinn ... 266
5.3.5 Strahlungsdiagramme ... 267
5.3.6 Halbwertsbreite ... 269
5.3.7 Vor-Rück-Verhältnis ... 270

5.4 Reichweiten von Richtfunkstrecken 270
5.4.1 Sendeleistung 271
5.4.2 Antennengewinn 272
5.4.3 Antennendiagramm 273
5.4.4 Freiraumdämpfung 273
5.4.5 Fresnel-Zone 277
5.4.6 Erdkrümmung 281
5.4.7 Witterungseinflüsse 282
5.4.8 Empfängerrauschen 284
5.4.9 Notwendiges Signal-Rauschverhältnis 284
5.4.10 Verluste auf Antennenkabel und Verbindungskomponenten 285
5.4.11 Position und Ausrichtung der Antennen 286
5.5 Antennentypen 288
5.5.1 Omnidirektionale Antennen 288
5.5.2 Notebook-Antenne 290
5.5.3 Dipol-Antennen 290
5.5.4 Omnidirektionale Antennen mit Gewinn 291
5.5.5 Patch-Antennen 294
5.5.6 Yagi-Antennen 296
5.5.7 Panel-Antennen 298
5.5.8 Parabolantennen 299
5.5.9 Sektorantennen 300
5.5.10 Kreuzpolarisierte Antennen 302
5.5.11 Zirkularpolarisierte Antennen 302
5.5.12 Dualbandantennen 303
5.5.13 Aktive Antennen 303
5.5.14 Diversity-Antennen 304
5.6 Antennenstecker 305
5.6.1 MC-Card-Steckergesicht 305
5.6.2 MMCX-Steckergesicht 306
5.6.3 U.FL-Steckergesicht 306
5.6.4 SMA-Steckergesicht 307
5.6.5 TNC-Steckergesicht 308
5.6.6 BNC-Steckergesicht 309
5.6.7 N-Steckergesicht 309
5.6.8 Pigtails 310
5.6.9 Indoor- und Outdoor-Antennen 311

5.7 Sicherheitsrelevante Bestimmungen ... 311
5.7.1 Mechanische Sicherheit ... 312
5.7.2 Elektrische Sicherheit ... 317

6 WLAN-Produkte 321

6.1 WLAN-Produktgrundsätze ... 321
6.2 WLAN-Client-Adapter ... 322
6.2.1 PCMCIA-Adapter ... 324
6.2.2 Cardbus-Adapter ... 325
6.2.3 Cardbus-Express-Adapter ... 327
6.2.4 Compact-Flash-Adapter ... 327
6.2.5 PCI-Adapter ... 328
6.2.6 USB-Adapter ... 329
6.2.7 Mini-PCI-Module ... 330
6.2.8 Mini-PCI-Express-Module ... 330
6.3 Access Points ... 331
6.3.1 Standard Access Point ... 334
6.3.2 Erweiterte Access Points (Internet Gateway) ... 335
6.3.3 Modulare Access Points ... 336
6.3.4 Dualband Access Points ... 337
6.3.5 Micro Access Point ... 338
6.3.6 Access-Point-Kombigeräte ... 339
6.4 WLAN-Switches ... 340
6.5 Management-Plattform ... 341
6.6 WLAN-Telefon ... 342
6.7 WLAN-Produktzertifizierungen ... 342
6.7.1 Wi-Fi ... 343
6.7.2 CCX-Programm ... 344

7 Praktische WLAN-Umsetzung 345

7.1 Reichweitenbetrachtungen ... 345
7.1.1 Detaillierte Reichweitenbetrachtung ... 347
7.1.2 Reichweitenberechnung ... 349
7.1.3 Reichweitenreduzierung durch Signalreflexionen ... 353
7.2 Funkausleuchtung ... 354

7.3 Professionelle Site Survey Utilities ... 357
7.4 Vorbereitung der Funkausleuchtung ... 361
7.4.1 Wichtige Voraussetzungen für die Funkausleuchtung ... 362
7.4.2 Störquellenermittlung ... 362
7.5 Spektrumanalyse ... 363
7.5.1 Richtige Platzierung von Access Points und Antennen ... 365
7.5.2 Stör- und Reflexionsquellen ... 365
7.5.3 Polarisation ... 366
7.5.4 Funkschatten ... 367
7.5.5 Leckkabel ... 368
7.5.6 Kanalwahl ... 368
7.5.7 RF-Management ... 371
7.5.8 Automatische Kanalwahl ... 372
7.5.9 Bandbreite ... 373
7.6 Performance-Betrachtungen ... 374
7.6.1 Fallstricke – TCP/IP im Wireless LAN ... 378
7.6.2 Reichweitenbedingte Performance-Reduzierung ... 380
7.6.3 Störungsbedingte Performance-Reduzierung ... 381
7.6.4 Zukünftige Performance-Steigerung ... 382
7.6.5 Performance-Betrachtungen bei Richtfunkstrecken ... 383
7.7 WLAN-Parameter ... 384
7.7.1 Erweiterte Datenrateneinstellung ... 384
7.7.2 Tx-Power ... 385
7.7.3 Diversity ... 386
7.7.4 Short-Präambel ... 386
7.7.5 Short Slot Time ... 386
7.7.6 Maximale Clients ... 387
7.7.7 Multiple SSIDs ... 387
7.7.8 Beacon Interval ... 387
7.7.9 RTS/CTS-Threshold ... 388
7.7.10 Fragmentation-Threshold ... 389
7.7.11 Listen Interval ... 389
7.7.12 DTIM Window ... 390
7.7.13 ATIM Window ... 390

7.7.14 Active Scan Timer 390
7.7.15 Passive Scan Timer 391
7.7.16 Long Retry Limit 391
7.7.17 Short Retry Limit 391
7.7.18 Association Timeout 392
7.7.19 Reassociation Timeout 392
7.7.20 Authentication Timeout 392

8 WLAN-Sicherheit 393

8.1 Angriffsszenarien und Sicherheitsmechanismen 394
8.1.1 802.11-Sicherheitsmechanismen 396
8.1.2 War Driving 397

8.2 Problemfall WEP 401
8.2.1 Umgehen des WEP-Schlüssels 402
8.2.2 Schwachstellen der WEP-Authentifizierung ausnutzen 408
8.2.3 Datenmanipulation 410
8.2.4 MAC-Spoofing 410

8.3 WLAN-Sicherheitsrisiken aufdecken 411

8.4 Maßnahmen zur Steigerung der Sicherheit 413
8.4.1 802.11i-Erweiterung 415
8.4.2 Wi-Fi Protected Access 417

8.5 Authentifizierung und Schlüsselmanagement 419
8.5.1 802.1X-Authentifizierung 419
8.5.2 802.1X-Zugangspunkte 422
8.5.3 Extensible Authentication Protocol 423
8.5.4 EAP-Nachrichten 423
8.5.5 EAP over LANs 425
8.5.6 EAP-Methoden 427
8.5.7 RSN-Informationselement 431
8.5.8 Schlüsselhierarchie 433
8.5.9 PMK und PTK 433
8.5.10 GMK und GTK 435
8.5.11 Ablauf der EAP-Authentifizierung 435
8.5.12 4-Wege-Handshake 437
8.5.13 2-Wege-Handshake 438
8.5.14 PTKSA und GTKSA 439
8.5.15 Pre-Shared Key 440
8.5.16 Roaming-Verzögerungen 441
8.5.17 RSN-Migration 443

8.6 TKIP ... 443
8.6.1 TKIP-Mixing-Funktion ... 444
8.6.2 TSC ... 445
8.6.3 Message Integrity Check ... 446
8.6.4 Replay-Attackenschutz ... 448
8.6.5 MIC-Fehler ... 448
8.6.6 TKIP-MPDU-Format ... 450
8.7 AES-CCMP ... 451
8.7.1 Rijndael-Algorithmus ... 451
8.7.2 CCMP-Replay-Schutz ... 453
8.7.3 CCMP-MIC-Berechnung ... 453
8.7.4 CCM-Verschlüsselung ... 454
8.7.5 CCMP-MPDU-Format ... 455
8.8 Virtual Private Network im WLAN ... 456
9 Fehleranalyse im WLAN 459
9.1 Einkreisen von Fehlerquellen ... 460
9.1.1 Überprüfung der Verkabelung ... 462
9.1.2 Überprüfung der aktiven WLAN-Komponenten ... 463
9.1.3 Auswerten der Netzwerkstatistiken ... 465
9.1.4 Überprüfung externer Antennen ... 466
9.1.5 Ping-Verbindungstest ... 467
9.2 WLAN-Fehlerquellen ... 469
9.3 Protokollanalyse ... 471
9.3.1 Ausführungen von Protokollanalysatoren ... 472
9.3.2 Systemanforderungen für Protokollanalyser ... 473
9.3.3 Standortfrage ... 474
9.3.4 Channel Surfing ... 474
9.3.5 Dashboard ... 476
9.3.6 Host Table ... 478
9.3.7 Matrix ... 478
9.3.8 Application Response Time ... 480
9.3.9 History ... 481
9.3.10 Global Statistics ... 483
9.3.11 Capture Panel ... 484
9.3.12 Alarm Log ... 485
9.3.13 Address Book ... 487
9.3.14 Paketfilter ... 488
9.3.15 WEP-Entschlüsselung ... 490

9.4 Beispiele einer WLAN-Protokollanalyse 490
9.4.1 Beacon-Frames 493
9.4.2 Scanning 494
9.4.3 Authentication 495
9.4.4 Assoziierung 496
9.4.5 Datenaustausch über den Access Point 497
9.4.6 Datenaustausch zwischen Access Points 499
9.4.7 Wiederholte Datenaussendung 500

Anhnag

Abkürzungen **501**

Literatur **507**

Index **513**