
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	20
1.5	Drahtlos versus drahtgebunden	23
1.5.1	Multiple-Access-Problematik	25
1.5.2	Modulationsverfahren	27
1.5.3	Die Frequenz	28
1.5.4	Exkurs Pegelwerte und Dezibel	29
1.5.5	Bitrate und Datenrate	31
1.5.6	Paketvermittlung versus Leitungsvermittlung	31
1.6	Gesundheit	32
1.7	OSI-Referenzmodell	34
1.8	Ein Überblick über den Inhalt dieses Buchs	41

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	83
3.2.5	FHSS-CCA-Empfindlichkeit	84
3.2.6	FHSS-PLCP-Datenempfang	85
3.2.7	FHSS-PMD_SAP	85
3.3	DSSS-Technologie	88
3.3.1	DSSS-Modulationsverfahren	90
3.3.2	DSSS-Spreiz-Codes	91
3.3.3	DSSS-Frameformat	100
3.3.4	DSSS-Short-Frameformat	101
3.3.5	DSSS-Kanalaufteilung	103
3.3.6	DSSS-PMD_SAP	104
3.3.7	DSSS-PLCP-Sendeprozedur	107
3.3.8	DSSS-PLCP-Empfangsprozedur	108
3.3.9	DSSS-CCA-Empfindlichkeit	109

3.3.10	DSSS-Empfängerempfindlichkeit	110
3.3.11	DSSS-Channel Agility	111
3.3.12	DSSS versus FHSS	112
3.4	OFDM-Technologie	113
3.4.1	OFDM-Frameformate	118
3.4.2	OFDM-PPDU-Codierungsprozess	120
3.4.3	OFDM-Datenempfang und -Decodierung	129
3.4.4	OFDM-Übertragungsverfahren	130
3.4.5	OFDM-Modulationsverfahren	135
3.4.6	OFDM-PMD_SAP	140
3.4.7	OFDM-PLCP-Sendeprozedur	140
3.4.8	OFDM-PLCP-Empfangsprozedur	141
3.4.9	OFDM-CCA-Empfindlichkeit	142
3.4.10	OFDM-Empfängerempfindlichkeit	142
3.4.11	OFDM-Kanalaufteilung	143
3.5	PBCC-Technologie	147
3.5.1	PBCC-5,5 und PBCC-11	148
3.5.2	PBCC-22	151
3.5.3	PBCC-33	152
3.6	Die 802.11g-PHY-Erweiterungen	153
3.6.1	802.11g-PPDU-Frameformat	156
3.6.2	802.11g-Signalspektrum	159
3.6.3	802.11g-Empfängerempfindlichkeit	160
3.7	Die IEEE-Infrarot-Technologie	160
3.7.1	IR-Frameformat	163
4	Der 802.11 MAC Layer	165
4.1	Problematik eines Funkmediums	165
4.2	Distribution Coordination Function	167
4.2.1	CSMA/CA	167
4.2.2	Virtuelle Carrier-Sense-Funktion	168
4.2.3	Acknowledgement	170
4.2.4	Interframe Space	170
4.3	Das Hidden-Station-Problem	175
4.4	Fragmentierung	177

4.5	802.11-Frameformat	179
4.5.1	Datenframes	186
4.5.2	Kontrollframes	187
4.5.3	Managementframes	191
4.5.4	Informationselemente	200
4.5.5	Herstellerspezifische Informationselemente	209
4.5.6	Managementframetypen	209
4.5.7	Frameklassen	214
4.6	Managementfunktionen	215
4.6.1	Passives und aktives Scanning	216
4.6.2	Power-Management	219
4.6.3	Wired-Equivalent-Privacy-Algorithmus	223
4.6.4	Authentifizierung	228
4.6.5	Assoziierung	231
4.6.6	Protection-Mechanismus	233
4.6.7	Datenratenunterstützung	235
4.6.8	Transmit Power Control	236
4.6.9	Dynamic Frequency Selection	237
4.7	Point Coordination Function	240
4.8	802.11d-Erweiterung	244
4.9	802.11e-MAC-Erweiterung	246
4.9.1	Enhanced Distribution Coordination Function	246
4.9.2	EDCF-TXOP-Bursting	249
4.9.3	Hybrid Coordination Function	250
4.9.4	Direct Link Setup	252
5	802.11n	255
5.1	MIMO-, SIMO- und MISO-Systeme	256
5.1.1	SIMO	256
5.1.2	Transmit Beamforming	258
5.1.3	Raum-Zeit-Codes	259
5.1.4	Raum-Multiplex-Verfahren	260
5.2	802.11n-PHY	262
5.2.1	OFDM-Unterträger	262
5.2.2	Zusätzliche OFDM-Coderate	263
5.2.3	Verkürztes Guard-Intervall	264
5.2.4	Kanalbandbreite von 20 MHz und 40 MHz	264
5.2.5	Low-Density Parity-Check	266

5.2.6	Modulation and Coding Schemes	267
5.2.7	Spektrale Effizienz	271
5.2.8	802.11n-PPDU-Formate	272
5.2.9	802.11n-HT-PHY-Parameter	275
5.3	802.11n-MAC	276
5.3.1	Reduced Interframe Space	276
5.3.2	A-MSDU und A-MPDU	277
5.3.3	Block-Acknowledgement	279
5.3.4	Spatial-Multiplexing-Power-Save-Funktion	280
5.3.5	802.11n-Betriebsmodi	281
5.3.6	20- und 20/40-MHz-Betrieb	282
5.3.7	Phased Coexistence Operation	283
5.3.8	Dual-CTS-to-Self-Verfahren	285
5.4	802.11n – Zusammenfassung und Umsetzung	285
5.4.1	802.11n-MIMO-Implementierung	286
5.4.2	802.11n in der Praxis	287
6	VHT-Erweiterungen	289
6.1	IEEE 802.11ac	289
6.1.1	802.11ac-Very-High-Throughput-PHY	290
6.1.2	802.11ac-Beamforming	290
6.1.3	802.11ac-VHT-PHY-Parameter	293
6.1.4	802.11ac-MCS	294
6.1.5	802.11ac-VHT-PPDU-Format	297
6.2	IEEE 802.11ad	298
6.2.1	802.11ad-Nomenklatur	299
6.2.2	802.11ad-Frequenzbereich und Kanalaufteilung	299
6.2.3	802.11ad-Medienzugriff	300
6.2.4	mmWave-Protected-Periode	302
6.2.5	PCP/AP-Clustering	302
6.2.6	Multi-Band-Operation	303
6.2.7	mmWave-Relay-Operation	304
6.2.8	802.11ad-Beamforming	305
6.2.9	802.11ad-Power-Management	308
6.2.10	GCMP	309
6.2.11	802.11ad-PHY-Typen	310
6.2.12	mmWave-Control-PHY	311
6.2.13	mmWave-SC-PHY	312
6.2.14	802.11ad-SC-PPDU-Format	314

6.2.15	mmWave-OFDM-PHY	315
6.2.16	Tone Mapping	317
6.2.17	802.11ad-OFDM-PPDU-Format	319
6.2.18	mmWave-Low-Power-PHY	320
7	Antennentechnik	323
7.1	Grundlagen der drahtlosen Kommunikation	324
7.2	Antennenprinzip	324
7.3	Antennenparameter	327
7.3.1	Impedanz	327
7.3.2	VSWR/Rückflussdämpfung	328
7.3.3	Polarisation	328
7.3.4	Antennengewinn	330
7.3.5	Strahlungsdiagramme	331
7.3.6	Halbwertsbreite	333
7.3.7	Vor-Rück-Verhältnis	334
7.4	Reichweiten von Richtfunkstrecken	334
7.4.1	Sendeleistung	335
7.4.2	Antennengewinn	336
7.4.3	Antennendiagramm	337
7.4.4	Freiraumdämpfung	337
7.4.5	Fresnel-Zone	341
7.4.6	Erdkrümmung	345
7.4.7	Witterungseinflüsse	346
7.4.8	Empfängerrauschen	348
7.4.9	Notwendiges Signal-Rausch-Verhältnis	348
7.4.10	Verluste auf Antennenkabel und Verbindungskomponenten	349
7.4.11	Position und Ausrichtung der Antennen	350
7.5	Antennentypen	352
7.5.1	Omnidirektionale Antennen	352
7.5.2	Notebook-Antenne	354
7.5.3	Dipol-Antennen	354
7.5.4	Omnidirektionale Antennen mit Gewinn	355
7.5.5	Patch-Antennen	358
7.5.6	Yagi-Antennen	360
7.5.7	Panel-Antennen	362
7.5.8	Parabolantennen	363
7.5.9	Sektorantennen	364

7.5.10	Kreuzpolarisierte Antennen	366
7.5.11	Zirkularpolarisierte Antennen	366
7.5.12	Dualbandantennen	367
7.5.13	Aktive Antennen	367
7.5.14	Diversity-Antennen	368
7.5.15	Dual-Slant-Antennen	369
7.6	Antennenstecker	370
7.6.1	MC-Card-Steckergesicht	370
7.6.2	MMCX-Steckergesicht	371
7.6.3	U.FL-Steckergesicht	371
7.6.4	SMA-Steckergesicht	372
7.6.5	TNC-Steckergesicht	373
7.6.6	BNC-Steckergesicht	373
7.6.7	N-Steckergesicht	374
7.6.8	Pigtails	374
7.6.9	Indoor- und Outdoor-Antennen	375
7.7	Sicherheitsrelevante Bestimmungen	375
7.7.1	Mechanische Sicherheit	376
7.7.2	Elektrische Sicherheit	381
8	WLAN-Produkte	385
8.1	WLAN-Produktgrundsätze	385
8.2	WLAN-Client-Adapter	386
8.2.1	PCMCIA-Adapter	388
8.2.2	Cardbus-Adapter	390
8.2.3	Cardbus-Express-Adapter	391
8.2.4	PCI-Adapter	391
8.2.5	USB-Adapter	392
8.2.6	Mini-PCI-Module	393
8.2.7	PCI-Express-Mini-Module	394
8.2.8	802.11n-PCIe-WLAN-Adapter	394
8.3	Access Points	395
8.3.1	Standard Access Point	398
8.3.2	Erweiterte Access Points (Internet Gateway)	399
8.3.3	Dualband Access Points	400
8.3.4	Micro Access Point	401
8.3.5	Access-Point-Kombigeräte	402
8.3.6	802.11n-Access-Points	403

8.4	WLAN-Switches	404
8.5	WLAN-Controller	406
8.6	Management-Plattform	408
8.7	WLAN-Telefon	409
8.8	WLAN-Produktzertifizierungen	410
8.8.1	Wi-Fi	410
8.8.2	CCX-Programm	411
9	Praktische WLAN-Umsetzung	413
9.1	Reichweitenbetrachtungen	413
9.1.1	Detaillierte Reichweitenbetrachtung	415
9.1.2	Reichweitenberechnung	417
9.1.3	Reichweitenreduzierung durch Signalreflexionen	421
9.2	Funkausleuchtung	423
9.3	Professionelle Site Survey Utilities	426
9.4	Vorbereitung der Funkausleuchtung	429
9.4.1	Wichtige Voraussetzungen für die Funkausleuchtung	430
9.4.2	Störquellenermittlung	431
9.5	Spektrumanalyse	432
9.5.1	Richtige Platzierung von Access Points und Antennen	434
9.5.2	Stör- und Reflexionsquellen	434
9.5.3	Polarisation	435
9.5.4	Funkschatten	436
9.5.5	Leckkabel	437
9.5.6	Kanalwahl	437
9.5.7	RF-Management	441
9.5.8	Automatische Kanalwahl	442
9.5.9	Bandbreite	442
9.5.10	Implementierung von 802.11n-Infrastrukturen	443
9.6	Performance-Betrachtungen	444
9.6.1	Fallstricke – TCP/IP im Wireless LAN	449
9.6.2	Reichweitenbedingte Performance-Reduzierung	451
9.6.3	Störungsbedingte Performance-Reduzierung	452
9.6.4	Zukünftige Performance-Steigerung	452
9.6.5	Performance-Betrachtungen bei Richtfunkstrecken	453

9.7	WLAN-Parameter	455
9.7.1	Erweiterte Datenrateneinstellung	455
9.7.2	Tx-Power	457
9.7.3	Diversity	457
9.7.4	Short-Präambel	457
9.7.5	Short Slot Time	457
9.7.6	Maximale Clients	458
9.7.7	Multiple SSIDs	458
9.7.8	Beacon Interval	459
9.7.9	RTS/CTS-Threshold	459
9.7.10	Fragmentation-Threshold	460
9.7.11	Listen Interval	460
9.7.12	DTIM Window	461
9.7.13	ATIM Window	461
9.7.14	Active Scan Timer	462
9.7.15	Passive Scan Timer	462
9.7.16	Long Retry Limit	462
9.7.17	Short Retry Limit	463
9.7.18	Association Timeout	463
9.7.19	Reassociation Timeout	463
9.7.20	Authentication Timeout	463
10	WLAN-Sicherheit	465
10.1	Angriffsszenarien und Sicherheitsmechanismen	466
10.1.1	802.11-Sicherheitsmechanismen	468
10.1.2	War Driving	470
10.2	Problemfall WEP	473
10.2.1	Umgehen des WEP-Schlüssels	474
10.2.2	Schwachstellen der WEP-Authentifizierung ausnutzen	480
10.2.3	Datenmanipulation	482
10.2.4	MAC-Spoofing	482
10.3	WLAN-Sicherheitsrisiken aufdecken	483
10.4	Maßnahmen zur Steigerung der Sicherheit	485
10.4.1	802.11i-Erweiterung	487
10.4.2	Wi-Fi Protected Access	489

10.5	Authentifizierung und Schlüsselmanagement	491
10.5.1	802.1X-Authentifizierung	491
10.5.2	802.1X-Zugangspunkte	494
10.5.3	Extensible Authentication Protocol	495
10.5.4	EAP-Nachrichten	495
10.5.5	EAP over LANs	497
10.5.6	EAP-Methoden	499
10.5.7	RSN-Informationselement	504
10.5.8	Schlüsselhierarchie	505
10.5.9	PMK und PTK	506
10.5.10	GMK und GTK	507
10.5.11	Ablauf der EAP-Authentifizierung	507
10.5.12	4-Wege-Handshake	509
10.5.13	2-Wege-Handshake	511
10.5.14	PTKSA und GTKSA	511
10.5.15	Pre-Shared Key	512
10.5.16	Roaming-Verzögerungen	513
10.5.17	RSN-Migration	515
10.6	TKIP	516
10.6.1	TKIP-Mixing-Funktion	517
10.6.2	TSC	518
10.6.3	Message Integrity Check	519
10.6.4	Replay-Attackenschutz	520
10.6.5	MIC-Fehler	521
10.6.6	TKIP-MPDU-Format	522
10.7	AES-CCMP	523
10.7.1	Rijndael-Algorithmus	524
10.7.2	CCMP-Replay-Schutz	525
10.7.3	CCMP-MIC-Berechnung	526
10.7.4	CCM-Verschlüsselung	527
10.7.5	CCMP-MPDU-Format	528
10.8	Wi-Fi Protected Setup	529
10.8.1	WPS-Architektur	529
10.8.2	WPS-Methoden	530
10.8.3	WPS-Protokoll	532
10.9	Virtual Private Network im WLAN	533

11	Fehleranalyse im WLAN	537
11.1	Einkreisen von Fehlerquellen	538
11.1.1	Überprüfung der Verkabelung	540
11.1.2	Überprüfung der aktiven WLAN-Komponenten	541
11.1.3	Auswerten der Netzwerkstatistiken	543
11.1.4	Überprüfung externer Antennen	544
11.1.5	Ping-Verbindungstest	545
11.2	WLAN-Fehlerquellen	547
11.3	Protokollanalyse	549
11.3.1	Ausführungen von Protokollanalyatoren	549
11.3.2	Systemanforderungen für Protokollanalyser	551
11.3.3	Standortfrage	552
11.3.4	Channel Surfing	553
11.3.5	Dashboard	555
11.3.6	Host Table	556
11.3.7	Matrix	557
11.3.8	Application Response Time	558
11.3.9	History	559
11.3.10	Global Statistics	561
11.3.11	Capture Panel	562
11.3.12	Alarm Log	565
11.3.13	Address Book	566
11.3.14	Paketfilter	567
11.3.15	WEP-Entschlüsselung	569
11.4	Beispiele einer WLAN-Protokollanalyse	569
11.4.1	Beacon-Frames	572
11.4.2	Scanning	573
11.4.3	Authentication	574
11.4.4	Assoziierung	575
11.4.5	Datenaustausch über den Access Point	576
11.4.6	Datenaustausch zwischen Access Points	578
11.4.7	Wiederholte Datenaussendung	579
	Abkürzungen	581
	Literatur	591
	Index	597