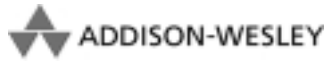
Wireless LAN

Axel Sikora

Wireless LAN

Protokolle und Anwendungen



An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Ein Titeldatensatz für diese Publikation ist bei
Der Deutschen Bibliothek erhältlich.**

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.
Für Verbesserungsvorschläge und Hinweise auf Fehler sind Verlag und Herausgeber dankbar.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Fast alle Hardware- und Softwarebezeichnungen, die in diesem Buch erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen oder sollten als solche betrachtet werden.

Umwelthinweis:
Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt.
Die Einschrumpffolie – zum Schutz vor Verschmutzung – ist aus
umweltfreundlichem und recyclingfähigem PE-Material.

10 9 8 7 6 5 4 3 2 1

04 03 02 01

ISBN 3-8273-1917-X

© 2001 by Addison-Wesley Verlag,
ein Imprint der Pearson Education Deutschland GmbH,
Martin-Kollar-Straße 10–12, D-81829 München/Germany
Alle Rechte vorbehalten
Einbandgestaltung: atelier für gestaltung, niesner & huber, Wuppertal
Lektorat: Rolf Pakendorf, rpakendorf@pearson.de
Korrektorat: Petra Kienle, Fürstenfeldbruck
Herstellung: Anna Plenk, aplenk@pearson.de
Satz: reemers publishing services gmbh, Krefeld, www.reemers.de
Druck und Verarbeitung: Freiburger Graphische Betriebe, Freiburg
Printed in Germany

Inhaltsverzeichnis

Vorwort **13**

1 Einführung **17**

1.1 Definition und Abgrenzung 17
1.2 Vor- und Nachteile im Überblick 18
1.3 Anwendungen im Überblick 20
1.3.1 Mehrwert durch WLAN 20
1.3.2 Mobile Arbeitsplätze 20
1.3.3 Einsparung der Kabelverbindungen 20
1.3.4 Schulungseinrichtungen 21
1.3.5 Mobile Datenerfassungssysteme 21
1.3.6 Hot-Spots 21
1.3.7 Externe Vernetzung 22
1.3.8 Wireless Local Loop 22
1.3.9 Industrielle Anwendungen 22
1.3.10 Ad-hoc-Networking 22
1.4 Marktgeschehen 23
1.4.1 Ausgangssituation 23
1.4.2 »Neuer Markt« 23
1.4.3 Ausreizen der Technologien 25
1.4.4 Konvergenz 25
1.4.5 Verschaltung statt Verschmelzung 26
1.4.6 Positionierung der Anbieter 27
1.4.7 Differenzierungsmöglichkeiten der Hersteller 28
1.4.8 Wachstumsmarkt 30
1.5 Organisationen und Gremien 31
1.5.1 Aufsichtsbehörden für Telekommunikation 31
1.5.2 Standards und Standardisierungsgremien 32
1.5.3 De-facto-Standards und Interessenvereinigungen 33

2 Grundlagen **35**

2.1 Geschichte der drahtlosen Nachrichtenübertragung 35
2.1.1 Drahtlos vs. drahtgebunden 35
2.1.2 Optische Telegrafie 35

2.1.3 Die Nutzung elektromagnetischer Wellen 36
2.1.4 Der drahtlose Vorläufer des Ethernet 36
2.1.5 Moderne Nutzung optischer Systeme 38
2.2 Modelle und Klassifizierung der technischen Kommunikation 38
2.2.1 Referenzmodelle 38
2.2.2 Klassifizierung des Kanalzugriffs 41
2.2.3 Modell der physischen Kommunikation 42
2.2.4 Klassifizierung von Kommunikation 43
2.3 Anforderungen an Übertragungsnetze 46
2.3.1 Verkehrstypen 46
2.3.2 Übertragungsgeschwindigkeit 47
2.4 Eigenschaften elektromagnetischer Wellen 47
2.4.1 Maxwellsche Gleichungen 47
2.4.2 Ausbreitung elektromagnetischer Wellen 48
2.4.3 Beeinträchtigung der Ausbreitung elektromagnetischer Wellen 49
2.4.4 Einsatz von Licht zur Kommunikation 52
2.5 Digitale Modulationstechnik 53
2.5.1 Grundlegendes 53
2.5.2 Phasenumtastverfahren 56
2.5.3 Frequenzumtastverfahren 57
2.6 Kanalzugriff 58
2.6.1 Überblick 58
2.6.2 Zeitmultiplexverfahren 59
2.6.3 Frequenzmultiplexverfahren 59
2.6.4 Kombinierte Verfahren 60
2.6.5 Raummultiplexverfahren 60
2.7 Frequenzspreizverfahren 60
2.7.1 Grundlegendes 60
2.7.2 Frequenzsprung-Spread-Spectrum-Verfahren 62
2.7.3 Direct-Sequence-Spread-Spectrum-Verfahren 63
2.8 Orthogonale Frequenzmultiplexverfahren 64
2.9 Antennen 66
2.9.1 Isotrope und anisotrope Antennen 66
2.9.2 Diversizität 67
2.9.3 Polarisation 67

2.9.4 Standort 68
2.9.5 Auswahl 68
2.10 Besonderheiten drahtloser Netze 69
2.10.1 Drahtlose Netze nutzen ein allgemeines Medium 69
2.10.2 Räumliche Charakteristik 69
2.11 Frequenzzuweisungen 70

3 Anwendungen, Geräte und Standards 73

3.1 Anwendungsszenarien 73
3.1.1 Personal Area Networks 73
3.1.2 Local Area Networks 74
3.1.3 SoHo-LAN 74
3.1.4 Büro-LAN 75
3.1.5 Kopplung von Netzwerken 75
3.2 Gerätetypen 76
3.3 Standards 76

4 IEEE802.11 79

4.1 Standard 79
4.1.1 Positionierung 79
4.1.2 Aufbau 80
4.1.3 Erweiterungen 81
4.2 Architekturen 81
4.2.1 Systemarchitekturen 81
4.2.2 Protokollarchitektur 83
4.3 Kanalzugriff 84
4.3.1 Einordnung 84
4.3.2 Distributed Coordination Function 85
4.3.3 RTS-CTS-Mechanismus 90
4.3.4 Fragmentierung von langen Nachrichten 92
4.3.5 Point Coordination Function 94
4.3.6 Rahmenformate auf der MAC-Ebene 96
4.3.7 Verwaltung von Stationen 99
4.3.8 Adressierung von Stationen 104
4.4 Bitübertragung 104
4.4.1 Einordnung 104

4.4.2 Frequency Hopping Spread Spectrum 105
4.4.3 Direct Sequence Spread Spectrum 107
4.5 Weitere Dienste 110
4.5.1 Synchronisation 110
4.5.2 Energiesparmodus 110
4.5.3 Dienste im ESS 110
4.6 Sicherheit 111
4.7 Erweiterungen des Standards 113
4.7.1 Der IEEE802.11a-Standard 113
4.7.2 Der IEEE802.11b-Standard 113
4.7.3 Weitere Standards 117

5 Bluetooth 119

5.1 Standard 119
5.1.1 Hintergrund 119
5.1.2 Aufbau 120
5.1.3 Bestandteile 121
5.1.4 Profile 122
5.2 Architekturen 123
5.3 Kanalzugriff 124
5.3.1 Einordnung 124
5.3.2 Rahmenformate 127
5.3.3 Audioübertragung 129
5.4 Zustandssteuerung 129
5.4.1 Einführung 129
5.4.2 Aufbau einer Verbindung 130
5.4.3 Betrieb einer Verbindung 132
5.4.4 Adressierung 134
5.5 Bitübertragung 134
5.6 Sicherheit 136
5.7 Systemimplementierung 137

6 DECT 139

6.1 Standard 139
6.2 Architekturen 139
6.3 Kanalzugriff 140
6.4 Bitübertragung 141

6.5 Anwendungsprofile 142
6.5.1 Sprachtelefonie 142
6.5.2 Datenverkehr 142

7 HomeRF 145

7.1 Standard 145
7.2 Architekturen 146
7.2.1 Systemarchitektur 146
7.2.2 Protokollarchitektur 146
7.3 Kanalzugriff 147
7.3.1 Einordnung 147
7.3.2 Asynchrone Übertragung 148
7.3.3 Synchrone Übertragung 148
7.3.4 Isochrone Übertragung 148
7.4 Bitübertragung 150
7.4.1 1 MHz-Kanäle 150
7.4.2 5 MHz-Kanäle 150

8 HiperLAN/2 153

8.1 Der Standard 153
8.1.1 Positionierung 153
8.1.2 Markteinführung 154
8.2 Architekturen 155
8.2.1 Systemarchitektur 155
8.2.2 Protokollarchitektur 155
8.3 Kanalzugriff 158
8.4 Bitübertragung 158
8.4.1 Frequenzzuweisungen 158
8.4.2 Modulationsverfahren 161
8.5 Weitere Dienste 162
8.6 Diskussion 162

9 Betrieb eines WLAN nach IEEE802.11b 163

9.1 Einführung 163
9.2 Mobile Stationen 163
9.2.1 Aufbau 163

9.2.2 Fähigkeiten 163
9.2.3 Administration 164
9.3 Zugangspunkte 167
9.3.1 Aufbau 167
9.3.2 Fähigkeiten 168
9.3.3 Administration 169
9.4 Erweiterte Netze 171
9.4.1 Verbundene Netze 171
9.4.2 Strukturierte Netze 172
9.4.3 Hohe Nutzerdichten 173
9.4.4 Verwaltung erweiterter Netze 173
9.5 Netzwerkanalyse 174
9.5.1 Übersicht 174
9.5.2 Einfache Analysewerkzeuge 174
9.5.3 Sniffer 177
9.6 Praxisbeispiele 180
9.6.1 LAN-LAN-Kopplung 180
9.6.2 Mobiler Rechnerraum 182
9.6.3 Wechselnde Stationen im Hotel 183

10 Verschiedene Aspekte 185

10.1 Sicherheit 185
10.1.1 Grundlegendes 185
10.1.2 Sicherheitsrisiken 185
10.1.3 Angriffe 186
10.1.4 Dynamische Verwaltung der Verschlüsselung 187
10.1.5 Fazit 187
10.1.6 Sicherheitsmaßnahmen 188
10.2 Störeinflüsse 188
10.2.1 Gliederung 188
10.2.2 Beeinflussung durch identische Systeme 189
10.2.3 Beeinflussung durch konkurrierende Systeme 189
10.2.4 Beeinflussung durch andere Funknetze 190
10.2.5 Beeinflussung durch andere Störsender 191
10.3 Wahl des Frequenzspreizverfahrens 191
10.3.1 Grundlegendes 191
10.3.2 Spektrale Effizienz 191

10.3.3 Sicherheit gegen Abhören 192
10.3.4 Störanfälligkeit 193
10.4 Aspekte der EMV-Belastung 193
10.4.1 Grundlegendes 193
10.4.2 Regularien 193
10.4.3 Vergleich mit GSM-Mobilfunk 194
10.5 WLAN und TCP/IP 194
10.6 Entscheidungskriterien 195
10.6.1 Grundlegendes 195
10.6.2 Auswahl einer LAN-Technologie 196
10.6.3 Auswahl einer WLAN-Technologie 196
10.6.4 Auswahl eines WLAN-Produkts 197
10.7 Ausblick 199

A Anhang 201
A.1 Maxwellsche Gleichungen 201
A.2 Physikalische Grundlagen des Direct-Sequence-Spread-Spectrum-Verfahrens 201
A.3 Antennen mit Richtcharakteristik 204

B Literatur 209

C Abkürzungen 215

Stichwortverzeichnis 221

Vorwort

Die Vernetzung von Computern und mikroelektronischen Geräten nimmt immer mehr zu, um das allumfassende *anybody, anything, anytime, anywhere* mit Leben zu füllen und durch den Zugriff auf Informationen und Ressourcen über beliebige Entfernungen den Mehrwert der Geräte und Anwendungen zu steigern. Dabei erfreuen sich insbesondere drahtlose lokale Netze (***W****ireless* ***L****ocal* ***A****rea* ***N****etworks* – WLAN) seit einigen wenigen Jahren einer außerordentlichen Beliebtheit, da sie den komfortablen, kostengünstigen und leistungsfähigen Anschluss der in zunehmendem Maße portablen oder pocketablen Anwendungen ermöglichen. Seitdem die Halbleiter-Technologien eine entsprechende Leistungsfähigkeit erreicht haben, lassen sich auch kommerziell interessante Produkte entwickeln.

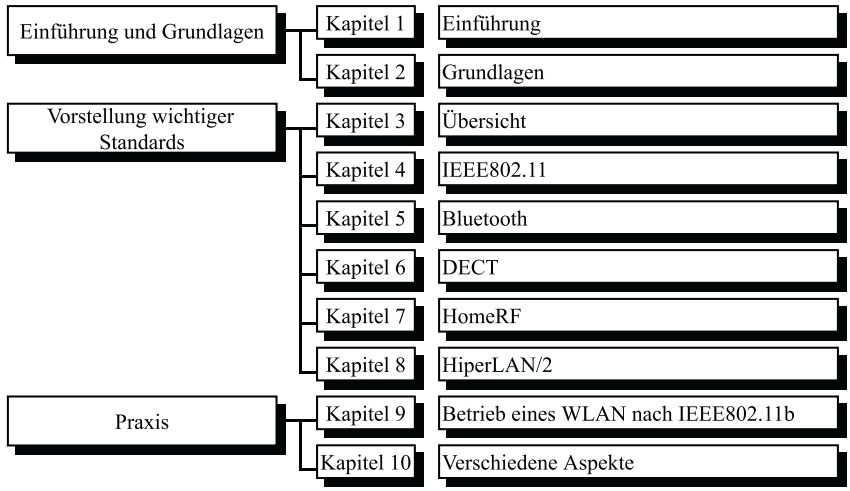
Damit ist das Thema der WLANs außerordentlich aktuell und hieraus ergibt sich für den Anwender der Systeme und für den Buchautor gleichermaßen eine grundlegende Problematik. Diese äußert sich in einer im Wesentlichen noch nicht konsolidierten Entwicklung einer Vielzahl von Technologien, Produkten und Marktteilnehmrn mit einer hohen technologischen Innovationsrate. Begleitet wird diese durch intensive Marketingaktivitäten, die zu einer weiteren Problematik bei der Erarbeitung eines Überblicks führen: Im Zeitalter des Internets ist eine Unmenge an Informationen verfügbar. Der Anwender muss also in besonderer Weise zwischen relevanter und unwichtiger Information unterscheiden, falsche Erwartungen identifizieren und realistische Einschätzungen und praxisnahe Szenarien erarbeiten.

Auf dem Weg zu einem aktuellen und umfassenden Überblick soll dieses Buch ein solides Fundament darstellen. Dabei nehmen notwendigerweise die technologischen Grundlagen einen breiten Raum ein, insbesondere auch, um die Unterschiede zwischen den verschiedenen Technologien verstehen zu können.

Das Buch gliedert sich in drei Abschnitte, wie in Abbildung 1 gezeigt:

- Das erste Kapitel befasst sich mit übergreifenden Aspekten von drahtlosen LAN-Netzwerken, ehe in den nächsten Kapiteln weitere Hintergrundinformationen zu Aufbau und physikalischen Grundlagen vermittelt werden.
- In den folgenden Kapiteln werden die für den gegenwärtigen und mittelfristigen Markt wichtigsten WLAN-Standards vorgestellt. Nach einer allgemeinen Übersicht sind dies die verschiedenen Standards IEEE802.11 (Kapitel 4), Bluetooth (Kapitel 5), DECT (Kapitel 6), HomeRF (Kapitel 7) und HiperLAN/2 (Kapitel 8).

Abbildung 1: Aufbau des Buchs



- Im dritten, praxisorientierten Abschnitt enthält das Kapitel 9 zunächst einen Überblick über Aufbau und Administration von WLAN-Netzwerken und Beispielinstallationen, bevor in Kapitel 10 einige ausgewählte Aspekte umfangreicher diskutiert werden. Hierzu zählen insbesondere Fragen der Sicherheit, der elektromagnetischen Verträglichkeit sowie Kriterien bei der Auswahl von WLAN-Produkten.

Das Buch wird ergänzt durch eine Webseite, die unter der Internetadresse *http://www.ba-loerrach.de/~sikora/wlanBuch/wlanBuch.htm* abgerufen werden kann. Hier finden sich zahlreiche Links zum Thema Wireless LAN.

Die Inhalte dieses Buchs sind zusammengestellt worden für die Vorlesungen »Rechnersysteme« bzw. »Kommunikationsnetze« an der Berufsakademie Lörrach (*http://www.ba-loerrach.de*) sowie für verschiedene Industrie-Seminare, die ich im Rahmen der lokalen Steinbeis-Transferzentren (*http://www.ba-loerrach.de/stz_index.html*) veranstaltet habe.

Bei der Aufarbeitung des Themas und der Bereitstellung von Materialien und Informationen haben mich eine Vielzahl von Personen engagiert unterstützt. Dabei sind besonders die Herren Claus Donner und Peter Schwindt vom Rechenzentrum der Berufsakademie Lörrach, Herr Jörg Luther vom Online-Magazin tecchannel (*http://www.tecchannel.de*), Herr Thomas Boele von Cisco Systems GmbH in Hallbergmoos, Herr Hans-Joachim Drude von Tenovis in Frankfurt, Herr Peter Schmitz von Network Associates GmbH in Nettetal, die Herren Ralf Keller und Hubert Kraus von Netlight GmbH in Offenburg und Herr Markus Radimirsch vom Institut für Allgemeine Nachrichtentechnik der Universität Hannover zu erwähnen. Herrn Rolf Pakendorf von Addison-Wesley danke ich für die Übernahme des Lektorats und die wie selbstverständliche Unterstützung des Buchprojekts.

Mein besonderer Dank gilt meiner Familie, die mich auch dieses Mal mit liebevollem Verständnis für Werken und Schreiben freigestellt hat.

Heitersheim

PS: Verlag und Autor freuen sich immer über Zuschriften, Anregungen und Änderungsvorschläge. Schicken Sie diese bitte an die E-Mail-Adresse *Axel.Sikora@addison-wesley.de*.

1 Einfuehrung

1.1 Definition und Abgrenzung

Unter drahtlosen lokalen Netzen (***W**ireless **L**ocal **A**rea **N**etworks* – WLAN) werden standardisierte Netzwerktechnologien verstanden, die LAN-Funktionalität mit einer drahtlosen Übertragung realisieren. Hierunter fällt vor allem der breitbandige Anschluss von mikroelektronischen Geräten im Umkreis von einigen zehn bis hundert Metern. Die Definition von lokalen Netzen findet sich in Abschnitt 3.1.2.

Dabei unterscheiden sich die WLAN-Technologien wesentlich von anderen drahtlosen Technologien, die ebenfalls als Wireless bezeichnet werden. Dies gilt, auch wenn ein Teil der in Abschnitt 1.3 genannten Anwendungen mit Hilfe anderer Wireless-Technologien realisiert werden kann. Hierbei sind insbesondere drei Bereiche der drahtlosen Nachrichtenübertragung zu nennen, gegen die WLAN-Technologien abgegrenzt werden können:

- Es stehen verschiedene proprietäre Systeme insbesondere für die Anbindung von Peripheriegeräten zur Verfügung (vgl. z.B. Abschnitt 3.1.1). Diese werden hier nicht näher besprochen, da sie keinem Standard folgen und im Allgemeinen auch keine Netzwerkfunktionalität erlauben.
- Zur Kopplung von lokalen Netzen im Sinne der Anwendung aus Abschnitt 3.1.5 stehen verschiedene Richtfunksysteme unter Nutzung von Lichtwellen (Laser-Link) oder elektromagnetischen Wellen zur Verfügung. Diese als ***P**oint-**to**-**P**oint-* (P2P) oder ***P**oint-to-**M**ulti**p**oint*-Systeme (PMP) ausgelegten Anlagen erlauben jedoch im Allgemeinen nicht den Aufbau von verknüpften Netzwerken.
- Auf der Grundlage der digitalen Mobilfunknetze kann auch Datenverkehr abgewickelt werden, wobei diese Möglichkeit oft zur drahtlosen Anbindung von Feldgeräten genutzt wird. Dabei handelt es sich jedoch nicht um ein lokales Netz, sondern um ein globales Netzwerk mit voller Mobilitätsunterstützung. Darüber hinaus ist im Allgemeinen auch keine breitbandige Anbindung möglich. Auch die Bandbreite der UMTS-Netze der dritten Mobilfunkgeneration wird auf maximal 2 Mbps beschränkt sein. In vielen Einsatzszenarien reduziert sich die Bandbreite auf Werte von 384 kbps oder auch nur 128 kbps [Sietmann 2001].

1.2 Vor- und Nachteile im Überblick

Die drahtlose Übertragung von Informationen bietet für alle Hierarchieebenen von Netzwerken potenzielle Vorteile. Von besonderem Interesse sind seit einiger Zeit die Netze auf persönlicher und lokaler Ebene, da hier in besonderer Weise die zahlreichen portablen und pocketablen Geräte der Sprach- und Datenverarbeitung bzw. -übertragung über drahtlose Übertragungsmedien unmittelbar miteinander kommunizieren können, ohne dass eine Kabelverbindung notwendig ist. Dabei ersetzen die drahtlosen lokalen Netze (***W**ireless **L**ocal **A**rea **N**etworks* - WLAN) die entsprechenden drahtgebundenen Lösungen auf der gleichen Netzwerkebene.

- *Kabel:* Das Kabelgewirr auf und unter dem Schreibtisch wird verringert oder entfällt ganz. Damit gehören Probleme mit fehlerhaften Kabeln der Vergangenheit an.
- *Steckverbinder:* Die Probleme mit inkompatiblen Steckverbindern sowie nicht vorhandenen Kabeln werden entschärft.
- *Kabelverbindungen im Büro:* Je nach Ebene der Netzwerkhierarchie, die mit Hilfe der drahtlosen Übertragung abgedeckt wird, werden kostenintensive Kabelinstallationen in Büro- und privaten Wohngebäuden vermieden werden.
- *Ad-hoc-Networking:* Von besonderer Faszination sind die Fähigkeiten einer aktiven Suche nach potenziellen Kommunikationspartnern und das automatische Aushandeln von Übertragungs- und Anwendungsprotokollen (vgl. Abschnitt 1.3.10).

  Viele der attraktiven Eigenschaften drahtloser Technologien können unter dem Einsatz ***I**ntelligenter **N**etze* (IN) zwar auch in drahtgebundenen Systemen umgesetzt werden und dies insbesondere dann, wenn diese Dienste auf den oberen Protokollebenen unabhängig von der physischen Übertragungsstrecke stattfinden. Da diese Dienste aber von den Herstellern der drahtlosen Kommunikationssysteme gefördert und implementiert – und vielleicht auch das erste Mal konsequent und einigermaßen konsistent umgesetzt werden – identifiziert man sie mit diesen Systemen.
- *Mobilität:* Abhängig von der Charakteristik der drahtlosen Übertragung können die Geräte auf diese Weise auch »mobil« eingesetzt werden. Die Größe der Funkzellen und die Ankopplung an andere Systeme hängen dabei sehr stark vom gewählten System ab. Auch die Geschwindigkeiten, mit denen ein Ortswechsel durchgeführt wird, unterscheiden sich maßgeblich.
- *Kostendegression:* Darüber hinaus konnten im Zuge der fortschreitenden Integrationsmöglichkeiten der Halbleitertechnologien die Produkte in einen preislich attraktiven Bereich vordringen. Diese Entwicklungen setzen allerdings hohe Stückzahlen voraus, so dass auch die Hersteller von

ihrer Seite aus versuchen, die Markteinführung zu forcieren, um das Henne-Ei-Problem hoher Stückzahlen und geringer Stückkosten zu lösen.

Allerdings sind beim Einsatz von drahtlosen Netzen auch eine Reihe von Einschränkungen zu verzeichnen:

- *Kosten pro Bandbreite:* Trotz der abnehmenden Kosten bei drahtlosen Systemen muss Bandbreite immer noch deutlich teurer als bei vergleichbaren drahtgebundenen Systemen erkauft werden. In Bezug auf die aktiven Komponenten ist hier mit etwa einer Größenordnung zu rechnen. Bezieht man auch die Installationskosten mit ein, kann sich die Kalkulation jedoch auch wieder deutlich zugunsten der drahtlosen Netze verschieben.
- *Verfügbare Bandbreite:* Die verfügbare Bandbreite ist auch bei höheren Kosten in vielen Fällen geringer als bei den drahtgebundenen Systemen. Auch hier ist mittelfristig ein Unterschied von etwa einer Größenordnung (Faktor 10) zu erwarten.
- *Reichweite:* Die Reichweite der drahtlosen Systeme ist in vielen Fällen empfindlich eingeschränkt, so dass die erhoffte Funktionalität nicht oder nur mit Abstrichen zu erreichen ist (vgl. Abschnitt 2.4).
- *EMV-Belastung:* Auch wenn die bei drahtlosen lokalen Netzen verwendeten Feldstärken nur etwa 5% der Feldstärken mobiler GSM-Telefonen erreichen, nimmt das Niveau der elektromagnetischen Belastung der Umwelt zu (vgl. Abschnitt 10.4).
- *Investitionssicherheit:* Gegenwärtig sind noch eine Vielzahl von Lösungen am Markt verfügbar, wobei nur in wenigen Fällen der mittelfristige Markterfolg gesichert ist. Vor dem Hintergrund der Investitionssicherheit führt diese Situation häufig zur Verschiebung der Investitionsentscheidung.
- *Interferenzen:* Wireless-LAN-Systeme übertragen über die Luftschnittstelle. Dabei handelt es sich im Gegensatz zu drahtgebundenen Systemen um ein gemeinsames Medium (*Shared Medium*) in dem Sinne, dass nicht nur die Stationen eines Kanals, sondern die unterschiedlichen Kanäle und Technologien auf ein gemeinsames Medium zugreifen.
- *Regularien und Internationalität:* Die Tatsache, dass Übertragungen in Wireless-LAN-Systemen über das öffentliche Medium Luft erfolgen, führt auch dazu, dass die jeweiligen hoheitlichen Organisationen Regeln für die Nutzung der verschiedenen Frequenzbereiche aufsetzen. Hierzu zählen die Bereiche der nutzbaren Frequenzen, aber auch die erlaubten Modulationsverfahren, die maximale Ausgangsleistung, Kompatibilität mit anderen Systemen und viele weitere Aspekte. Wenn auch die Details für den Anwender meist nicht von Interesse sind, muss er dennoch unter Umständen in Kauf nehmen, dass er sein System bei einer Auslandsreise nicht nutzen kann oder darf.

- *Sicherheit:* Aufgrund der Tatsache, dass die Reichweite der Funkübertragung nicht auf den Bereich der potenziellen Empfänger beschränkt ist, sondern auch in andere Bereiche abstrahlt, können auch parasitäre Empfänger die Signale aufnehmen. Hinzu kommt die Tatsache, dass viele Systeme eine automatisierte und dynamische Anmeldung der mobilen Stationen unterstützen. Um diese potenziellen Sicherheitslücken zu schließen, bieten die bestehenden Systeme verschiedene Ansätze auf allerdings sehr unterschiedlichem Sicherheitsniveau.

Die grundlegende Frage des Anwenders reduziert sich wie immer darauf, welchen Mehrwert er in seiner Anwendung durch den Einsatz einer drahtlosen Übertragungstechnologie erzielen kann.

1.3 Anwendungen im Überblick

1.3.1 Mehrwert durch WLAN

Um einen Überblick über den erzielbaren Mehrwert in konkreten Anwendungen zu erhalten, werden im Folgenden typische Beispiele in einer allgemeinen Darstellung aufgeführt. Die Vorstellung einiger ausgewählter und konkreter Installationen erfolgt in Abschnitt 9.6.

1.3.2 Mobile Arbeitsplätze

Der vielleicht am stärksten ins Auge springende Bereich ist die Unterstützung von mobilen Arbeitsplätzen. Dies gilt nicht nur für das Büroumfeld, in dem Laptop-gestützte Anwendungen in den unterschiedlichen Besprechungs- und Arbeitsräumen komfortabel unterstützt werden können, sondern ebenso für den Heimbereich, wo der Arbeitsplatz auch einmal in den Garten verlegt werden kann.

1.3.3 Einsparung der Kabelverbindungen

Bei drahtlosen Netzwerken werden die Kabelverbindungen zur Kommunikation ganz oder teilweise eingespart. Hierdurch entfallen die Kosten für die Kabelinstallation entsprechend ganz oder teilweise. Auch wenn in modernen Bürogebäuden Kabelkanäle für die einfache und kostengünstige Installation vorgesehen sind, gibt es doch zahlreiche Situationen, in denen dies noch nicht der Fall ist.

- Bei der Nutzung von historischen Gebäuden ist die Installation entweder sehr aufwändig oder aus Gründen des Denkmalschutzes nicht möglich.
- Bei Gründung und Aufbau von jungen Unternehmen verändert sich eine Infrastruktur unter Umständen sehr schnell, so dass hier eine flexible Anpassung sinnvoll erscheint.

- Im Heimbereich sind Kabelkanäle und Leerrohre bislang nur selten anzutreffen, so dass die Installation von zusätzlichen Netzwerkleitungen nur mit großem Aufwand oder offen verlegten Leitungen möglich ist.

Die Einsparung von Kabelverbindungen erscheint insbesondere dann vorteilhaft, wenn viele dezentrale Geräte mit Netzwerkverbindungen ausgestattet werden sollen. In Zusammenhang mit dem Vordringen der Internetfähigkeit der so genannten Embedded Systeme [Sikora2000(4)] kann die Nutzung von drahtlosen Netzen wichtige Vorteile erlangen.

1.3.4 Schulungseinrichtungen

In Schulungseinrichtungen können drahtlose Netze in zwei Szenarien eingesetzt werden:

- Immer häufiger verfügen Schüler und Studenten über eigene Laptops, die die Ausstattung von stationären Rechnerräumen in Schulungseinrichtungen zunehmend obsolet machen. Die Vernetzung der Schülerrechner kann komfortabel in jedem Unterrichtsraum, der mit einem Zugangspunkt ausgestattet ist, erfolgen.
- Die Einrichtung von mobilen Seminarräumen für spezielle Ereignisse, Seminare oder Messen wird durch den Einsatz drahtloser Netze erleichtert.

1.3.5 Mobile Datenerfassungssysteme

In vielen Einrichtungen erfolgt eine Datenerfassung vor Ort. Als typische Beispiele seien genannt:

- die Inventur in Handelsgeschäften oder Lagern,
- die Analyse technischer Geräte wie Auto oder Flugzeuge oder
- die Datenerfassung im Krankenhaus bei Visite oder im Operationssaal.

Diese Anwendungen können durch die unmittelbare Einbindung in das Unternehmensnetzwerk einen Datenabgleich mit der zentralen Datenbank unterstützen.

1.3.6 Hot-Spots

In zunehmendem Maße werden Wartezeiten am Flughafen oder Bahnhof oder Aufenthalte an öffentlichen Plätzen zur Kommunikation über E-Mail oder Informationsbeschaffung über aktuelle Online-Medien genutzt. Hier können drahtlose Netze ein komfortables und flexibles Zugangsmedium zum Internet darstellen. Insbesondere bei hohem Datenaufkommen in kleinen Bereichen sind Lösungen z.B. mit den Mobilfunknetzen der dritten Generation wirtschaftlich oft nicht realisierbar (vgl. Abschnitt 1.1). Hier stellen WLAN-Systeme eine interessante Ergänzung dar.

1.3.7 Externe Vernetzung

Die Kopplung von lokalen Netzen in zwei getrennten Gebäuden im Sinne einer LAN-LAN-Kopplung stellt insbesondere dann eine Herausforderung dar, wenn die Grundstücke nicht unmittelbar miteinander verbunden sind. Hier können Funkbrücken eine einfache und kostengünstige Alternative zur Nutzung des öffentlichen Telekommunikationsnetzes bieten.

1.3.8 Wireless Local Loop

Ebenso lassen sich die WLAN-Technologien auch einsetzen, um einen drahtlosen Hausanschluss unabhängig vom öffentlichen Telekommunikationsnetz bereitzustellen. Dieser so genannte ***W****ireless* ***L****ocal* ***L****oop* (WLL) zur Überbrückung der letzten Meile ist nicht nur im Bereich der Sprachtelefonie, sondern auch für Datennetze möglich.

1.3.9 Industrielle Anwendungen

Eine Vielzahl von industriellen Anwendungen im Produktionsbereich laufen in einer für eine Verkabelung ungünstigen Umgebung. Beschädigungen durch Hitze oder mechanische Einwirkungen sind hierbei häufige Einschränkungen, ebenso können die räumlichen Gegebenheiten eine kostengünstige Verkabelung unmöglich machen. Hier bieten drahtlose Netze wesentliche Vorteile.

Ein interessantes Anwendungsgebiet stellen auch flexible Fertigungsstraßen dar, die den jeweils zu fertigenden Produkten in Aufbau und Konfiguration immer wieder angepasst werden. Auch der Aufbau der Netzwerkverbindungen ist häufig sehr zeitraubend.

1.3.10 Ad-hoc-Networking

Allgemein bieten drahtlose Netzwerke in einer besonderen Weise die Fähigkeiten eines Ad-hoc-Networking. Dieses beschreibt zwei Verhaltensweisen:

- Die ursprüngliche Bedeutung, die auf die Entwicklung des Aloha-Netzes in den späten sechziger Jahren zurückgeht (vgl. Abschnitt 2.1.4), besagt, dass sich Stationen mit physischer Verbindung selbsttätig gegenseitig erkennen und die Kommunikation aufnehmen können [Frodigh 2000]. Dabei besteht die besondere Herausforderung darin, dass die Stationen Informationen austauschen, bevor eine Netzwerkverbindung aufgebaut ist. Darüber hinaus müssen auch entsprechende Sicherheitsvorkehrungen den Zugriff von unerlaubten Stationen zuverlässig verhindern können.
- Auf dieser Grundlage hat sich der Begriff des Ad-hoc-Networking dahingehend erweitert, dass über den reinen Aufbau einer Netzwerkverbindung hinaus auch die Anwendungen selbsttätig miteinander in Ver-

bindung treten können. Während sich die ursprüngliche Bedeutung also auf die unteren Schichten des Netzwerkmodells beschränkt, bezieht die erweiterte Bedeutung alle Netzwerkschichten ein (vgl. Abschnitt 2.2.1).

1.4 Marktgeschehen

1.4.1 Ausgangssituation

Die Vielzahl von Lösungen bei im Vergleich zu drahtgebundenen Systemen höheren Kosten der aktiven Komponenten begrenzt gegenwärtig immer noch den Markterfolg. Die hohe Anzahl der konkurrierenden Lösungen stellt einen frappierenden Gegensatz zur Dominanz der Ethernet-Standards im Bereich der drahtgebundenen LANs dar. Diese Situation beruht auf zwei Gegebenheiten:

1.4.2 »Neuer Markt«

Zum einen befindet sich der Wireless-Markt immer noch in der Einführungsphase, wobei für die nächsten Jahre immense Wachstumsraten prognostiziert werden. Dies führt dazu, dass viele Hersteller versuchen, sich durch besondere Merkmale eine aussichtsreiche Startposition zu verschaffen.

- Eine Besonderheit besteht im Wireless-Markt allerdings darin, dass es praktisch allen Herstellern klar ist, dass eine proprietäre Entwicklung keine Aussicht auf einen Markterfolg hat. Einerseits wäre die Akzeptanz am Markt wegen der verlangten Interoperabilität mit anderen Geräten nur gering. Andererseits müssen die Entwicklungs- und Marketingkosten so hoch veranschlagt werden, dass keine zufriedenstellende Rentabilität zu erwarten wäre. Aus diesen Gründen ist gerade im Bereich der Wireless LANs ein Konsortien-Boom entstanden, der auf der Basis von so genannten Non-Profit-Organisationen mithelfen soll, die Produktentwicklungen zu koordinieren und die Marketing-Arbeit übergreifend zu gestalten.
- Ein weiteres spezifisches Merkmal ist, dass praktisch alle großen Halbleiter-, System- und Software-Hersteller in mehr als einem Konsortium mitarbeiten. Dieses Verhalten lässt sich auf vier Gründe zurückführen.
  - Erstens sind die großen Hersteller mittlerweile so diversifiziert, dass das Engagement in den unterschiedlichen Konsortien zum Teil auf unterschiedliche Unternehmensbereiche zurückgeht.
  - Zweitens ist der Wireless-Markt noch so unübersichtlich, dass der Markterfolg einer Technologie nur sehr unsicher ist. Deswegen erscheint es vielen Herstellern sinnvoll, auf mehr als ein Pferd zu setzen.

- Drittens können die Anwendungen der verschiedenen Protokolle unterschiedlich sein, so dass disjunkte Zielmärkte ins Auge gefasst werden können.
- Und schließlich bedeutet die Mitarbeit in einem Gremium selbst dann den direkten Zugriff auf die jeweils aktuellen Informationen und diskutierten Themen, wenn keine aktive Beeinflussung beabsichtigt ist.

- Der Aufschwung der firmenübergreifenden Gremien und Kooperationen bedeutet aber nicht, dass es keine proprietären Produkte gibt. Dabei handelt es sich jedoch meist um firmenspezifische Erweiterungen bestehender Systeme. Auch diese Ansätze lassen sich auf vier Sachverhalte zurückführen:
  - Die große Schnelligkeit des Markts stellt die Hersteller oft genug vor die Entscheidung, ihr Produkt auch unter dem Risiko, dass es nicht vollständig standardkonform ist, so früh wie möglich auf den Markt zu bringen, um sich Marktanteile zu sichern, oder ihre Produktentwicklung bis zur Verabschiedung des Standards anzuhalten.
  - Da die Wireless-Produkte zum gegenwärtigen Zeitpunkt sehr hohe Anforderungen an den Schaltungs- und Systementwurf sowie die Produktionstechnologien stellen, beruhen manche leistungsfähige Systeme insbesondere der frühen Generationen auf firmenspezifischen Erweiterungen.
  - Ein Unternehmen kann mit einem frühen Markteintritt die Hoffnung hegen, dass es aufgrund mangelnder Interoperabilität seiner Geräte auch Folgeinvestitionen bei den Installationen für sich verbucht.
  - Darüber hinaus, und dies ist vielleicht der zentrale Punkt in der Diskussion, besteht für die Hersteller standardisierter Kommunikationsprodukte praktisch keine Möglichkeit, sich im Rahmen der eigentlichen Transportfunktionalität zu differenzieren. Die Produkte können nur über ihre zusätzlichen Dienste einen vermeintlichen Mehrwert erreichen. Dabei spielen die Bereiche der Netzwerkadministration eine zentrale Rolle. Zu beachten ist dabei aber leider auch, dass gerade diese Dienste die Interoperabilität wesentlich einschränken können.

Es zeigt sich aber, dass ein leistungsfähiger Standard, wie er mit dem IEEE802.11b für Datenraten von 11 Mbps vor etwa zwei Jahren bereitgestellt wurde, problemlos in der Lage ist, Anbieter nicht-standardisierter Produkte aus dem Markt zu verdrängen. Als Beispiele können hier zwei sehr unterschiedliche Fälle aufgeführt werden:

- »Radiolan« ist als ein früher Anbieter leistungsfähiger, aber proprietärer Systeme in Konkurs gegangen. Inwieweit die Investoren, die die Rechte an den Produkten und vor allem dem Markennamen übernommen haben, hieraus weitere Vorteile ziehen können, erscheint zumindest fraglich.

- Auch »Proxim« war bereits sehr früh mit proprietären Produkten auf dem Markt – hat aber nach langem Zögern einen Migrationspfad zu Produkten aufgelegt, die konform zu einem allgemein anerkannten Standard sind. Dies gilt sowohl für die Übertragungssysteme, die auf der Basis des IEEE802.11-Standards höhere Datenraten von 11 Mbps erzielten, als auch für die Migration von OpenAir-konformen Geräten, die nunmehr nach HomeRF überführt werden.

So ist eindeutig festzustellen, dass zum einen alle neuen Vorschläge auf offenen Standards beruhen und sich zum anderen proprietäre Systeme auf dem Rückzug befinden.

1.4.3 Ausreizen der Technologien

Die Tatsache, dass Wireless-Produkte weiterhin hohe und höchste Anforderungen an die Leistungsfähigkeit von Hardware und die Effizienz von Software stellen, hat eine zweite wichtige Auswirkung: Insbesondere kostengünstige Systeme für den Massenmarkt können gegenwärtig nur einen Kompromiss zwischen Leistungsfähigkeit und erreichbarem Kostenniveau darstellen. Im Bereich der Anforderungen an die Hardware ist insbesondere die monolithische Integration auch der Hochfrequenzbaugruppen hervorzuheben, die unter bestimmten Randbedingungen Kostenvorteile ermöglicht [Sikora 2000(5)]. Zwei Faktoren haben entscheidenden Einfluss auf die Produkteigenschaften:

- Die Positionierung des Systems in der Netzwerkhierarchie, die in erheblichem Maße Auswirkungen auf die benötigte Leistungsfähigkeit hat.
- Der Zeitpunkt, zu dem das Produkt in den Markt eingeführt werden soll, beeinflusst die angestrebte Leistungsfähigkeit ganz unmittelbar. Insbesondere die Bandbreite ist direkt abhängig von den Fähigkeiten der Halbleitertechnologie, die zu diesem Zeitpunkt verfügbar ist.

Die große Anzahl der unterschiedlichen Technologien birgt jedoch die Gefahr, dass sich der noch junge Markt insbesondere im Marketing verzettelt.

1.4.4 Konvergenz

Im Bereich der Kommunikationstechnologien lässt sich in zunehmendem Maße Konvergenz zwischen den ursprünglich unabhängig voneinander zu betrachtenden Technologien beobachten. Drei Beispiele illustrieren, dass dies nicht nur bei den leitungsgebundenen Kommunikationsprotokollen der Fall ist:

- *Sprach-Daten-Konvergenz:* Einige der Entwicklungen sind explizit auf die unterschiedlichen Verkehrsanforderungen ausgerichtet, die die Übertragung sowohl von Sprache als auch von Daten mit sich bringt. Als Beispiel seien hier Bluetooth oder HiperLAN/2 genannt. Andere Ent-

wicklungen setzen mit der Datenübertragung unmittelbar auf Protokolle für die Sprachübertragung auf, wie z.B. DECT.

- *LAN-WAN-Konvergenz:* Die Technologien im lokalen und im Weitverkehrsbereich konvergieren zunehmend. Dies gilt gegenwärtig in besonderem Maße für die Technologien, die sowohl für den lokalen Bereich als auch für die LAN-Kopplung eingesetzt werden können.
- *Wireless-Cordless-Konvergenz:* Andererseits finden viele Entwicklungen im LAN-Bereich auch im Bereich der globalen Netze ihre Entsprechung. Die GPRS-Erweiterungen des GSM-Systems können hier als Beispiel dienen. Insbesondere erscheint auch eine Verschaltung der Dienste von großem Interesse. So kann HiperLAN/2 als alternatives Zugangsnetz für UMTS-Netze im Bereich so genannter *Hot Spots* Einsatz finden.

1.4.5 Verschaltung statt Verschmelzung

Neben den hier dargestellten Konvergenzerscheinungen wird mit Sicherheit zunächst aber eine Zusammenschaltung der unterschiedlichen Netze zu beobachten sein. Dies betrifft sowohl die Verschaltung von drahtlosen und drahtgebundenen Netzwerken als auch die Kopplung der drahtlosen Netzwerke auf den unterschiedlichen Netzwerkebenen. Folgende Beispiele illustrieren dies:

- Verschaltung von drahtlosen und drahtgebundenen Netzwerken:

  Diese Verschaltung ist notwendig, um eine Einbindung der drahtlosen Geräte in die allgemein verfügbaren zu ermöglichen.

- Verschaltung von drahtlosen Netzwerken:
  - Eine Integration von DECT- und GSM-Endgeräten im Bereich der Sprachkommunikation erscheint sinnvoll und vorteilhaft und ist in ersten Produkten bereits regional verfügbar.
  - HiperLAN/2 ist so spezifiziert, dass es als lokal verfügbares Zugangsnetz zum Mobilfunknetz UMTS eingesetzt werden kann.
  - Die Einbindung von PAN-Systemen nach IEEE802.15 in IEEE802.1-1-WLAN-Netzwerke ist eines der expliziten Ziele der Standardisierungsbemühungen.

Folgende Voraussetzungen müssen für eine solche Verschaltung erfüllt sein:

- *Interoperabilität:* Die Systeme müssen ähnliche Netzwerk- und Dienstebenen aufweisen. Auch ähnliche Dienstzugangspunkte verbessern die Möglichkeiten des einfacheren modularen Aufbaus. Ein solcher Punkt könnte die Verschaltung von Bluetooth-PAN-Systemen und 802.11-LAN-Netzwerken behindern.
- *Ende-zu-Ende-Dienste:* Es müssen Ende-zu-Ende-Dienste bereitgestellt werden. Dies gilt insbesondere für die Identifizierung, Authentifizierung und Wegfindung (*Routing*).

Von grundlegender Bedeutung bei dieser Diskussion sind jedoch die Positionierung der verschiedenen Technologien und der jeweilige Markterfolg. Dabei muss besonders darauf hingewiesen werden, dass die Positionierung nur zum Teil von der gegenwärtigen technischen Spezifikation abhängt. Zu einem Gutteil hängt sich auch von den Zusatzdiensten der Systemlieferanten und von der Erweiterung der Dienste im Rahmen zukünftiger Standards ab. Die Integration der Roaming-Funktionalität beim HomeRF2.0-Standard eröffnet beispielsweise die Einsatzmöglichkeit auch in größeren Firmennetzen.

1.4.6 Positionierung der Anbieter

Bei der Betrachtung der Anbieterpositionierung lässt sich trotz des geringen Alters des Markts eine große Differenzierung der Hersteller und damit – zumindest in dieser Hinsicht – eine große Reife des Marktes feststellen. Insbesondere kann man folgende drei Gruppen unterscheiden:

- Die erste Gruppe der Anbieter beschäftigt sich mit der Entwicklung und meist auch mit der Herstellung der Chipsets, die Voraussetzung für die Erfüllung der gewünschten Funktionalität sind. Dabei handelt es sich sowohl um die Bereitstellung der Hardware in Form der jeweiligen Silizium-Chips als auch um einen Teil der hardwarenahen Software. Diese Gruppe soll als Hersteller der Chipsets bezeichnet werden.
- Eine zweite Gruppe von Anbietern stellt aus diesen Grundbestandteilen fertig einsetzbare Geräte und Systeme her. In Abgrenzung von der ersten Gruppe ist festzustellen, dass:
  - einige Systemlieferanten auf ihre eigenen Chipsets zurückgreifen. Dabei lässt sich noch weiter unterscheiden, ob die eigenen Chipsets exklusiv verwendet werden oder neben dem Einsatz in den eigenen Geräten auch an andere Systemhersteller vertrieben werden. Dieses Marktmodell der integrierten Hersteller (Chipset und System) trifft man vor allem bei Herstellern im Netzwerkbereich an, da dort die Kommunikation die Hauptfunktionalität der Geräte darstellt. Entsprechend ist dieser Anteil bei den Netzwerksystemen nach IEEE802.11 oder HomeRF besonders hoch, während die Hersteller von Bluetooth-Modulen besonders auf den Ausrüstungsmarkt zielen, in dem Geräte eine Zusatzfunktionalität erhalten sollen.
  - manche Chipset-Hersteller nur ihre Chipsets vertreiben und nicht in den Bereich der Systemlieferanten vordringen. Diese Konstellation trifft man vor allem in den Bereichen an, in denen die Kommunikation nur eine Zusatzfunktion für Geräte mit anderer Hauptfunktionalität darstellt. Die potenziell vielen Geräte aus den verschiedensten Anwendungsbereichen, in die eine Bluetooth-Anbindung integriert werden soll, können hier als Beispiel dienen.

- Als dritte Gruppe sind noch die regionalen Vertriebs- und Dienstleistungsorganisationen zu nennen, die die Inbetriebnahme und die Betreuung vor Ort vornehmen können.

1.4.7 Differenzierungsmöglichkeiten der Hersteller

Funktionale Differenzierung

Bei Geräten, die nach einem festen Standard funktionieren sollen, besteht für die Hersteller nur in einem geringen Umfang die Möglichkeit, sich von den Mitbewerbern zu differenzieren, da dies nicht durch die Funktionalität des Geräts möglich ist. Somit kann die Differenzierung eigentlich nur über Zusatzdienste erreicht werden, die über die Grundfunktionalität oder über die im Standard beschriebenen Dienste hinausgehen. Hier sind zusammenfassend insbesondere folgende Aspekte zu nennen:

- *Sicherheitsfunktionalitäten:* Die Architektur und die Verwaltung von Sicherheitsdiensten ist bei vielen wichtigen Technologien nur teilweise Bestandteil des Standards. Entsprechend finden sich in diesem Bereich notgedrungen proprietäre Lösungen auf sehr unterschiedlichem Sicherheitsniveau.
- *Netzwerkadministration:* Hersteller, die eine zentrale Geräte- oder Benutzerverwaltung anbieten, beziehen meist nur die eigenen Geräte in die Erkennung mit ein und können Geräte anderer Hersteller nicht oder nur eingeschränkt administrieren.
- *Installationstechnik:* Um die Installation von Zugangspunkten (*Access Points*) zu vereinfachen, integrieren manche Hersteller die Stromversorgung in das Netzwerkkabel zwischen Hub und Zugangspunkt. Auf diese Weise muss kein Elektroinstallateur in den Aufbau des drahtlosen Netzwerks einbezogen werden. Der Vorteil für den Hersteller besteht darin, dass der Hub den Stromanschluss unterstützen muss.
- *Leistungsfähigkeit der Datenübertragung:* Eine wichtige Einschränkung ist aber für den Bereich der drahtlosen Netze noch zu nennen. Da die erreichbare Übertragungsgeschwindigkeit bei einer Reihe von Standards sowohl von der Kanalqualität als auch von der Qualität der Empfänger abhängt, können die Systeme der unterschiedlichen Hersteller durchaus sehr unterschiedliche Durchsatzraten erzielen. Daher ist im Bereich der Wireless-LAN-Systeme auch die Transportfunktionalität Gegenstand der Produktdifferenzierung. Dies lässt sich bei den aktiven Komponenten für drahtlose Netze fast nicht mehr beobachten: Eine Netzwerkkarte für 100 Mb-Ethernet sendet oder empfängt alle 10 ns ein Bit, solange ein spezifiziertes Kabel mit einer Länge von unter 100 m angeschlossen ist. Bei drahtgebundenen Systemen werden im Standard die Qualitätseigenschaften von Sender und Empfänger genau spezifiziert, während es bei

den ungleich empfindlicheren drahtlosen Systemen den Anstrengungen der Hersteller überlassen bleibt, möglichst leistungsfähige Empfänger zu entwickeln.

Die genannten und verschiedene weitere kleingedruckte Aspekte beeinträchtigen die Interoperabilität der Systeme wesentlich. Aus diesem Grund empfehlen praktisch alle verfügbaren Testergebnisse, trotz des zugrunde liegenden einheitlichen Standards beim Aufbau nur die Geräte eines Herstellers zu verwenden.

Produktbündelung

Bei vielen Geräten stellt die Anschlussmöglichkeit an ein Netzwerk noch einen Mehrwertdienst dar. Dies gilt nur noch in eingeschränktem Maße für PCs[1], die immer seltener ohne Einbindung in ein Netzwerk verwendet werden. Für viele andere Embedded-Systeme dagegen behält diese Aussage ihre Gültigkeit. Hier ist jedoch festzustellen, dass je nach Positionierung und Funktionsumfang des Wireless-Standards zahlreiche Einbindungen in verschiedenste Geräte angestrebt werden.

- Leistungsfähigere und somit auch kostenaufwändigere Technologien halten Einzug auch in die Netzwerkanbindung von preisgünstigeren und einfacheren Systemen wie ***P**ersonal **D**igital **A**ssistants* (PDA).
- Einfachere und preiswertere Systeme versuchen, sich viele neue Anwendungen zu erschließen, die auch mit weniger teuren Geräten des Alltagsgebrauchs gekoppelt werden. Als Beispiele können hier Bediengeräte, drahtlose Headsets oder auch Haushaltsgeräte genannt werden.
- Auch die Bündelung mit anderen Geräten aus dem Netzwerkbereich kann zusätzlichen Absatz generieren. So sind beispielsweise ISDN-Router für Wireless-Anbindung verfügbar, die insbesondere im Markt für Heim- und kleinere Büroanwendungen auch die Bandbreitenanforderungen erfüllen würden. Auch die Integration einer einfachen Firewall findet sich in manchen Produkten.

Marketing-Aspekte

Über die technischen Fähigkeiten hinaus entscheiden zusätzlich zahlreiche Faktoren aus Marketing und Vertrieb über den Erfolg der verschiedenen Produkte am Markt. Von besonderer Bedeutung sind dabei folgende Aspekte:

1 Um Missverständnisse zu vermeiden, wird darauf hingewiesen, dass mit dem Begriff Personal Computer (PC) nicht nur die auf der Intel-Prozessor-Architektur basierenden »IBM-kompatiblen« PCs, sondern ebenso die von Apple hergestellten Mac-Computer gemeint sind. Letztere bieten im Bereich von integrierten WLAN-Lösungen interessante Ansätze.

- *Positionierung:* Die saubere Positionierung der unterschiedlichen Geräte am Markt hilft dem Kunden, das für die jeweilige Anwendung optimale Gerät auszuwählen.
- *Portfolio:* Die durchgängige Unterstützung des gesamten benötigten Produktportfolios von aktiven und passiven Komponenten aus einer Hand erschwert es weiteren Firmen, einen bereits besetzten Markt zu betreten. Bei den Wireless-LAN-Systemen spielen insbesondere die angebotenen Antennen eine wichtige Rolle.
- *Bündelung:* Die Bündelung von Angeboten zusammen mit Dienstleistern kann den Markteinstieg bei Neukunden erleichtern. So können beispielsweise bereits einige durch ***I**nternet **S**ervice **P**rovider* (ISP) subventionierte Geräte am Markt beobachtet werden.

1.4.8 Wachstumsmarkt

Trotz der genannten Schwierigkeiten steht dem Markt für drahtlosen lokale Netze ein kräftiges Wachstum bevor (siehe Frost 2001, in prinzipieller Übereinstimmung mit vielen anderen Einschätzungen für den Markt an Chips für den Kurzstreckenfunk). Ausgehend von einem bereits signifikanten Umsatz mit Silizium im Jahr 2000 von weltweit 1,34 Mrd. US-Dollar vergrößert sich das Marktvolumen in den folgenden sechs Jahren auf das Dreieinhalbfache (vgl. Abbildung 1.1). Unter Berücksichtigung des Preisverfalls sind entsprechend noch größere Anstiege bei den Stückzahlen zu erwarten. Dabei ist zu berücksichtigen, dass es sich nur um die Umsätze auf der Chipset-Ebene handelt. Die Umsätze der Systemhersteller und der Dienstleister erreichen Größen, die um den entsprechenden Mehrwert höher liegen.

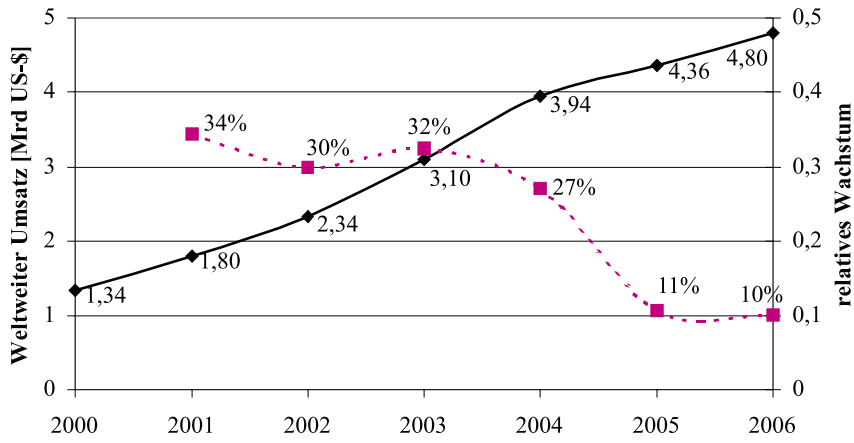


Abbildung 1.1: Wachstumsprognose für den WLAN-Markt [Frost 2001]

1.5 Organisationen und Gremien

An der Ausgestaltung des Umfelds, in dem drahtlose Übertragungssysteme eingesetzt werden, sind eine Vielzahl von internationalen und nationalen, staatlichen und privaten Organisationen und Gremien beteiligt. Diese lassen sich in drei Kategorien einteilen:

- die Aufsichtsbehörden für Telekommunikation, die die Rahmenbedingungen für die Nutzung der öffentliche Ressource »Luft« vorgeben.
- die Standardisierungsgremien, die die Spezifikationen für die interoperable Nutzung der verschiedenen Anwendungen erarbeiten, und
- weitere Gremien, die auf eigene Initiative Spezifikationen für Hersteller oder Benutzer erarbeiten.

1.5.1 Aufsichtsbehörden für Telekommunikation

- Die Aufsichtsbehörden für Telekommunikation sind im Wesentlichen zuständig für die Zuteilung von Frequenzbereichen und die Aufstellung der entsprechenden Nutzungsregeln.
- In den USA wird diese Aufgabe durch die ***F**ederal **C**ommunications **C**ommission* (FCC) als Regierungsagentur wahrgenommen, die unmittelbar dem Kongress verantwortlich ist.
- In Europa erfolgt die Zuteilung der Frequenzbereiche weitestgehend durch das ***E**uropean **C**onference for **P**osts and **T**elecommunications* (CEPT) in Zusammenarbeit mit dem ***E**uropean **T**elecommunications **S**tandards **I**nstitute* (ETSI). Hierbei ist allerdings zu berücksichtigen, dass die entsprechenden Empfehlungen weiterhin durch nationale Verordnungen umgesetzt werden müssen. Dies führt immer wieder zu Inkompatibilität aufgrund verschiedener historischer Vorgehensweisen. Insbesondere der Frequenzbereich des 2,4 GHz-ISM-Bands war in Frankreich und Spanien wegen der militärischen Nutzung von Teilfrequenzen lange Zeit eingeschränkt. Seit Anfang 2000 steht nun auch in Frankreich und Spanien das gesamte Spektrum von 2400 bis 2483 MHz zur Verfügung. In Deutschland werden die nationalen Richtlinien von der dem Bundesministerium für Wirtschaft und Technologie unterstellten *Regulierungsbehörde für **T**elekommunikation und **P**ost* (RegTP) herausgegeben.
- Für den ebenfalls sehr wichtigen japanischen Markt nimmt das *Radio Equipment Inspection and Certification Institute* (MKK) die Funktion der Aufsichtsbehörde wahr.

Dabei können die Aufsichtsbehörden aufgrund der hoheitlichen Aufgaben unter Umständen sehr großen Einfluss auf die Wettbewerbsstellungen ausüben. Ein deutliches Beispiel ist die Erweiterung der Regeln für die Nutzung des 2,4 GHz-Bands für Frequenzsprung-Spread-Spectrum-Verfahren (FHSS)

durch die FCC im August 2000. Basierend auf dieser Erweiterung können HomeRF-Systeme der Version 2.0 Datenraten von 10 Mbps erreichen (FCC Part 15).

1.5.2 Standards und Standardisierungsgremien

Gemäß der ***I**nternational **S**tandards **O**rganisation* (ISO), die 1946 im Rahmen der UNESCO gegründet wurde und seitdem unter dem Dach der Vereinten Nationen tätig ist, ist ein

> *Standard eine technische Spezifikation oder ein anderes öffentlich verfügbares Dokument, das in Kooperation und Übereinstimmung oder mit allgemeiner Zustimmung aller betroffenen Interessengruppen erarbeitet wurde, auf den konsolidierten wissenschaftlichen, technologischen und experimentellen Ergebnissen beruht, auf die Verbreitung des optimalen Nutzens der Gemeinschaft ausgerichtet ist und von einem Gremium angenommen wurde, das auf nationaler, regionaler oder internationaler Ebene anerkannt ist (*zitiert nach: *Walke 2000).*

Drei zentrale Punkte sind in diesem Zusammenhang hervorzuheben:

- die Einbeziehung aller betroffenen Interessengruppen,
- die Verabschiedung durch ein anerkanntes Gremium und
- die öffentliche Verfügbarkeit.

Diese drei Forderungen sind bei den so genannten Firmenstandards nicht oder nur eingeschränkt erfüllt. Deswegen handelt es sich nicht um Standards im Sinne der Definition, sondern um so genannte *De-facto-Standards*.

Eine Übersicht über die im Bereich der Telekommunikation tätigen Standardisierungsgremien und deren zahlreiche Verflechtungen findet sich in [Walke 2000]. Folgende Gremien sind von besonderer Bedeutung:

- Die ***I**nternational **T**elecommunication **U**nion* (ITU) wurde bereits 1865 in Genf gegründet und gehört damit zu den ältesten internationalen Gremien überhaupt. Der Sektor für Radiokommunikation der ITU (ITU-R) nahm im März 1993 seine Arbeit auf.
- Das European Telecommunications Standards Institute (ETSI) (*http://www.etsi.org*) ist eine Non-Profit Organisation, die die Definition von langfristigen Standards im Bereich der Telekommunikation für Europa und darüber hinaus zum Ziel hat. Die ETSI hat knapp 800 Mitglieder aus 52 europäischen und außereuropäischen Ländern. Darunter befinden sich Hersteller, Netzwerkbetreiber, Anwender und staatliche Gremien. Die Interessen der Bundesrepublik Deutschland beispielsweise werden vom Bundesministerium für Wirtschaft wahrgenommen.
- Der Standardisierungsverband (***S**tandards **A**ssociation* – SA) (*http://standards.ieee.org*) des weltweit größten Berufsverbands, des Verbands für Elektrotechnik und Elektronik (***I**nstitute of **E**lectrical and **E**lectronic **E**ngi-*

neers, Inc. – IEEE) vereinigt internationale Mitglieder mit dem Ziel, Standards für verschiedenste technische Bereiche zu verabschieden und in den Markt einzuführen. Besonders bekannt ist der IEEE im Netzwerkbereich, in dem die Standards des IEEE802 lokale Netzwerke oder der IEEE1394 einen schnellen Firewire-Bus zur Kommunikation von Multimedia-Geräten beschreiben.

1.5.3 De-facto-Standards und Interessenvereinigungen

Es gibt verschiedene Gründe für Firmen oder Firmenvereinigungen, eigene De-facto- oder Firmenstandards zu entwickeln. Als die größten Nachteile bei den offiziellen Standardisierungsgremien erscheinen vor allem die folgenden Aspekte:

- sehr hoher Zeitaufwand,
- sehr viele Einflussfaktoren, die gegebenenfalls den eigenen Interessen widersprechen,
- Verpflichtung zur Offenlegung.

Dabei verliert der letzte Punkt allerdings an Bedeutung. Nicht nur im Bereich der Kommunikationstechnik hat sich in den letzten Jahren die Einsicht durchgesetzt, dass nur offene Standards, die von einer möglichst großen Anzahl von möglichst schlagkräftigen Firmen unterstützt werden, Aussicht auf Erfolg haben. Auf diese Weise können diese so genannten Firmenstandards entweder von den Standardisierungsgremien aufgenommen werden oder für lange Zeit eine ernste Konkurrenz für diese darstellen.

Als Beispiele für diese Firmenvereinigungen, die meist als ***N**on-**P**rofit-**O**rganizations* (NPO) organisiert sind, können genannt werden:

- ***B**luetooth **S**pecial **I**nterest **G**roup* (BSIG)
- ***Home R**adio **F**requency **W**orking **G**roup* (HomeRF WG)
- ***DECT M**ulti**m**edia **C**onsortium* (DECT-MMC)
- ***H**iperLAN/**2 G**lobal **F**orum* (H2GF)
- ***W**ireless **LAN A**ssociation* (WLANA) und ***W**ireless **E**thernet **C**ompatibility **A**lliance* (WECA)

2 Grundlagen

2.1 Geschichte der drahtlosen Nachrichtenübertragung

2.1.1 Drahtlos vs. drahtgebunden

In den meisten Fällen erscheint die drahtgebundene Übertragung als Vorläufer der drahtlosen Informationsübertragung. Zwei Beispiele können dies illustrieren. Die Verbreitung des drahtgebundenen Telefons begann bereits Anfang des vorigen Jahrhunderts, während die mobile, drahtlose Telefonie ihre jetzige Verbreitung erst mit dem Einsatz digitaler Technologien ab Beginn der 90er Jahre erreichen konnte. Auch im Bereich der lokalen Datennetze kamen zunächst drahtgebundene Technologien zum Einsatz, bevor seit Ende der 90er Jahre auch drahtlose Technologien im Sinne der hier vorgestellten Wireless-LAN-Systeme eine leistungsfähige Alternative darstellten.

Diese Betrachtung berücksichtigt allerdings nur die kommerziell eingesetzten Systeme in den jeweiligen Bereichen. Interessanterweise stellen die drahtlosen Systeme in beiden Fällen wichtige Vorläufer dar, die auch zentrale Eigenschaften der drahtgebundenen Systeme vorwegnehmen.

2.1.2 Optische Telegrafie

Bevor sich die drahtgebundene Telegrafie seit der Mitte des 19. Jahrhunderts verbreitete, wurde in besonders wichtigen Bereichen die optische Telegrafie eingesetzt. Dabei handelt es sich im weitesten Sinne auch um eine drahtlose Übertragung mit Hilfe elektromagnetischer Wellen.

Während die Wurzeln einer solchen Übertragung bis in die antike Welt zurückreichen, fanden die Systeme der optischen Telegrafie erst seit Anfang der 19. Jahrhunderts eine weitere Verbreitung. In einer ersten Anwendung der optischen Telegrafie wurde die Nachricht vom Fall Trojas im 12. Jahrhundert v. Chr. über eine Entfernung von 500 km von Kleinasien nach Argos auf den Peloponnes in nur einer Nacht mit Hilfe von Feuerzeichen übertragen [Kaiser 1999]. Auch wenn der Wahrheitsgehalt dieser Legende angezweifelt werden darf, ist der prinzipielle Einsatz einer optischen Signalverbindung mit Hilfe von Relaisstationen sowohl bei Griechen

als auch bei Römern bekannt. Im Frankreich des 19. Jahrhunderts wurden Nachrichten über ein landesweites Netz von Relaisstationen mit dem Zentrum Paris übertragen.

Ein wesentlicher Vorteil der optischen Telegrafie besteht in der einfachen Erzeugung der optischen Signale. Hinzu kommt, dass diese Signale auch in großer Entfernung mit dem menschlichen Auge zu beobachten sind. Einschränkend muss dabei allerdings berücksichtigt werden, dass der Übertragungskanal insbesondere am Tag oder bei Nebel unter Umständen von sehr schlechter Qualität war. Der ursprüngliche Vorteil des Sendens und Empfangens durch den Menschen und die damit verbundene geringe Datenrate gingen bei der drahtgebundenen elektrischen Telegrafie verloren.

Darüber hinaus entstanden in diesem Zusammenhang bereits wesentliche technische Entwicklungen im Bereich der Übertragungsprotokolle und der Kodierung, die dann bei der Nutzung späterer drahtgebundener Telegrafen eingesetzt werden konnten.

2.1.3 Die Nutzung elektromagnetischer Wellen

Die Entdeckung der elektromagnetischen Wellen geht auf die Mitte der 1880er Jahre durchgeführten Versuche von Heinrich Hertz (1857–1894) zurück, die über mehrere Umwege Guglielmo M. Marconi (1874–1937) dazu veranlassten, Mitte der 1890er Jahre entsprechende Versuche zu unternehmen, Nachrichten zu übermitteln. Bereits 1896 gelang über eine Entfernung von 3 km eine erfolgreiche Übertragung [Kaiser 1999]. Einsatz fand die Telegrafie mit Hilfe elektromagnetischer Wellen allerdings zunächst in Weitverkehrsnetzen.

2.1.4 Der drahtlose Vorläufer des Ethernet

Aber auch im Bereich der lokalen Netze findet man einen drahtlosen Vorläufer für den allgegenwärtigen Ethernet-Standard nach IEEE802.3. Prof. Norman Abramson, der nach seinem Wechsel von der Stanford University an die University of Hawaii Anschluss an das zu dieser Zeit auf dem amerikanischen Kontinent entstehende *Arpanet* finden wollte, dem Vorläufer des Internets, konnte dies kommerziell sinnvoll nur mit einer drahtlosen Datenübertragung erreichen. Ergebnis war das Aloha-Netz [Abramsson 1970]. Zentrale Eigenschaften des Aloha-Netzes sind:

- Alle Stationen verwenden einen gemeinsamen Übertragungskanal. Diese Eigenschaft bezeichnet man als ***M**ultiple **A**ccess* (MA). Sie setzt unbedingt eine Adressierung der Stationen voraus, da es sich um eine Kommunikation handelt, an der mehr als zwei Teilnehmer beteiligt sind.
- Jede Station verfolgt die Aktivität des Übertragungskanals. Wird der Kanal im Rahmen dieses ***C**arrier **S**ense* (CS) als frei erkannt, darf die Station ihre Übertragung beginnen. Zunächst durfte der Start einer Übertragung zu jedem beliebigen Zeitpunkt erfolgen (*Pure Aloha*). Durch die

Einführung von Zeitschlitzen, die alle Stationen gemeinsam nutzen, kann allerdings die Zeitdauer potenzieller Kollisionen deutlich verringert und somit die Nutzbarkeit des Kanals erheblich vergrößert werden. Entsprechend darf in der Weiterentwicklung des *Slotted Aloha* die Übertragung einer Station nur noch zu Beginn eines Zeitschlitzes erfolgen.

- Die Tatsache, dass Stationen im Falle eines freien Kanals die Übertragung beginnen dürfen, hat zur Folge, dass zwei Stationen gleichzeitig oder annähernd gleichzeitig eine Übertragung beginnen. Die Signale überlagern sich in dem gemeinsamen Übertragungskanal und die Empfänger sind nicht mehr in der Lage, die überlagerten Signale zu trennen. Um eine solche Kollision und den damit verbundenen Datenverlust auf dem Übertragungskanal erkennen zu können, ist jede Station verpflichtet, den erfolgreichen Empfang eines Datenpakets mit einer Bestätigung (***Ack****nowledgement* – ACK) zu quittieren. Die sendende Station darf das versendete Datenpaket erst dann aus dem Ausgangsspeicher löschen, wenn sie die Empfangsbestätigung erhalten hat. Empfängt sie innerhalb eines festgelegten Zeitraums keine Bestätigung, so beginnt sie eine erneute Übertragung des Pakets. Für die Wartezeit bis zum Beginn des zweiten Versuchs wird mit einem vergleichsweise aufwändigen, so genannten Backoff-Algorithmus versucht, die Wahrscheinlichkeit zu minimieren, dass zwei Stationen, deren Pakete bereits beim ersten Versuch kollidierten, sich auch bei den nachfolgenden Versuche stören (***C****ollision* ***A****voidance* - CA).

Die Eigenschaften des Aloha-Netzes insbesondere in Bezug auf den Backoff-Algorithmus wurden von Dr. Robert Metcalfe vom Xerox Palo Alto Parc übernommen, um mit Hilfe eines lokalen Netzwerks mehrere Alto Stations miteinander zu verbinden. Dabei handelte es sich um frühe Vorläufer des PCs mit einer grafischen Oberfläche, einer Mausbedienung und einem lokalen Druckeranschluss. Die erste Generation dieses Netzwerks, das mit einer Übertragungsgeschwindigkeit von 2,94 Mbps betrieben wurde (der Prozessor der Alto Station wurde mit 2,94 MHz getaktet), erhielt dann auch zunächst den Namen *Alto Aloha Network*. Kurze Zeit später erhielt die Technologie den marketing-fähigen Kunstnamen Ethernet, um deutlich zu machen, dass sich die Technologie nicht nur auf Xerox-Rechnern einsetzen lässt. Später verzichtete Xerox auch auf den Markennamen und die Technologie wurde beim IEEE als 802.3 standardisiert [Spurgeon 2000].

Der Bestätigungsmechanismus des Aloha-Netzes konnte bei der Entwicklung des Ethernet zu Gunsten einer Kollisionsdetektierung (***C****ollision* ***D****etection* – CD) aufgegeben werden. Da aber, wie in Abschnitt 2.10.2 gezeigt werden wird, eine solche Kollisionserkennung bei drahtlosen verteilten Systemen nicht möglich ist, kommt das Prinzip des Bestätigungsmechanismus auch bei den modernen drahtlosen LAN-Systemen wieder zum Einsatz.

2.1.5 Moderne Nutzung optischer Systeme

Neben der wachsenden Verbreitung drahtloser Übertragungssysteme auf der Grundlage elektromagnetischer Wellen konnten sich aber auch optische Systeme, die über Luft übertragen, bis in die Gegenwart behaupten:

- Für die Verschaltung mehrerer räumlich getrennter lokaler Netzwerke im Rahmen einer LAN-Kopplung werden Laser-Links eingesetzt.
- Für die Kopplung von Geräten im lokalen Umfeld im Sinne von Personal Area Networks wurde in den neunziger Jahren der IrDA-Standard verabschiedet, der vor allem Verbreitung zur infrarotgestützten Ankopplung von Mobiltelefonen und PDAs an den Notebook-PC fand.
- Neueste Entwicklungen zeigen, dass unter Einbeziehung einer leistungsfähigen digitalen Signalverarbeitung die Punkt-zu-Punkt-Kopplung von Stationen über Licht komfortabel erfolgen kann, wenn adaptive Verfahren, beispielsweise unter Einsatz mikromechanischer Spiegel, zum Einsatz kommen. Solche Technologien können eine interessante Ergänzung zu einem zukünftig anzubindenden Zugangspunkt der drahtlosen LANs mit diffuser Ausstrahlung elektromagnetischer Wellen darstellen, da hohe Datenraten unterstützt werden können [Texas Instruments]. Dabei lassen sich zum gegenwärtigen Zeitpunkt mit dem Mikrospiegel Positioniergenauigkeiten von 5 nm erreichen, mit deren Hilfe Entfernungen bis zu 50 m überbrückt werden.

2.2 Modelle und Klassifizierung der technischen Kommunikation

2.2.1 Referenzmodelle

Der erfolgreiche, effiziente und möglichst automatisierte Informationsaustausch zwischen Kommunikationspartnern setzt einen komplexen Vorgang voraus. Zur besseren Gliederung und zur Erstellung eines modularen Systems wird dieser Vorgang gemäß einem hierarchischen Schichtenmodell in funktionale Elemente aufgeteilt. Ausgehend von dem bereits in den siebziger Jahren von der ***I**nternational **S**tandardization **O**rganisation* (ISO) entwickelten ISO / OSI-Referenzmodell für die Verbindung offener digitaler Systeme (***O**pen **S**ystems **I**nterconnection* - OSI) unterscheidet man klassischerweise sieben Schichten, die in Abbildung 2.1 dargestellt sind.

Grundlage der Kommunikation sind Sender und Empfänger, die unter dem Begriff der *Station* zusammengefasst werden. Dabei versteht man unter einer Station ein beliebiges technisches System, das nach bestimmten Regeln Nachrichten senden oder empfangen kann.

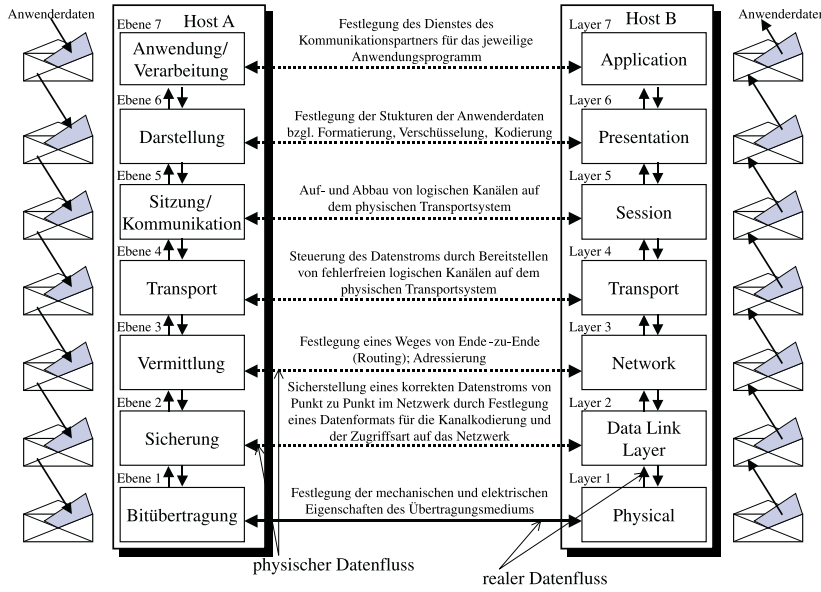


Abbildung 2.1: Das ISO-OSI-Referenzmodell für die Kommunikation technischer Systeme

In jeder Station bietet jede Schicht, mit Ausnahme der obersten, der nächsthöheren Schicht Dienste (*Services*) an. Um diese Dienste ausführen zu können, benötigt die Schicht Informationen, die bei der Instanziierung der jeweiligen Schicht übergeben werden. In den vielen Fällen einer Softwarebasierten Realisierung der Schichten kann man sich die Implementierung einer Schicht als eine Prozedur vorstellen, die aufgerufen wird und bei deren Aufruf ein Satz an Parametern übergeben wird.

Der wesentliche Vorteil des hierarchischen Modells besteht in der Abstraktion der Funktionalität. Die interne Realisierung einer Schicht ist für die aufrufende Schicht uninteressant. Auch dass die Schicht unter Umständen weitere Schichten zur Erbringung des Dienstes mit Hilfe des gleichen Mechanismus aktiviert, bleibt für die aufrufende Schicht unsichtbar. Diese Vorteile der Modularisierung und der Abstraktion müssen aber erkauft werden durch eine geringere Effizienz der Übertragung. Insbesondere ist zu beachten, dass jede an der Kommunikation beteiligte Ebene dem von der darüber liegenden Ebene übergebenen Datenpaket noch einen eigenen Rahmen mit Steuer- und Adressinformationen voranstellt (vgl. Abbildung 2.2). Realisiert ein Übertragungsprotokoll oder eine Protokollfamilie mehrere Schichten, so spricht man aufgrund des hierarchischen Aufbaus auch von einem Protokollstapel (*Protocol Stack*).

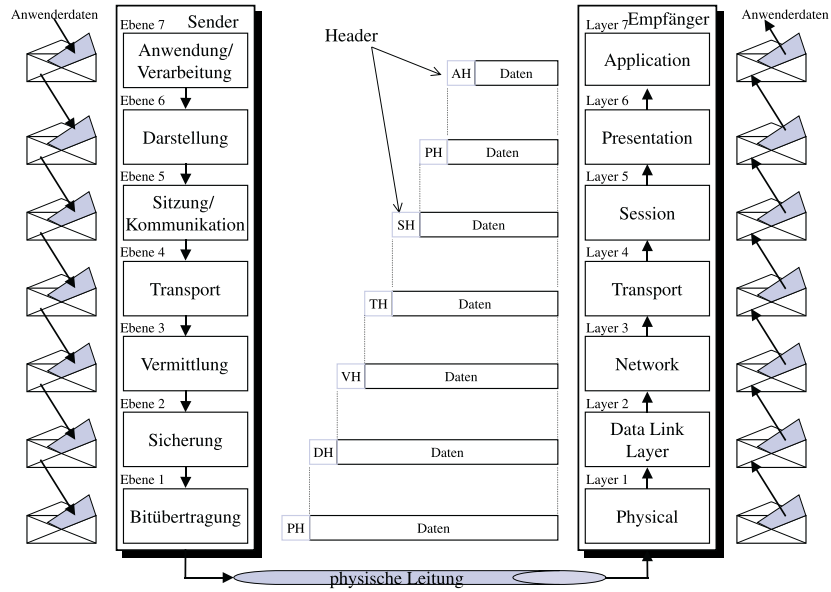


Abbildung 2.2: Jede Schicht fügt dem Datenpaket weitere Adress- oder Steuerinformationen hinzu. Dies erfolgt meist im Rahmen eines so genannten Headers und führt zu einer Vergrößerung der Datenmenge.

Für den Einsatz drahtloser Übertragungssysteme hat diese Hierarchisierung in der Praxis folgende Auswirkungen:

- Solange der Dienstzugangspunkt für die Funktion unverändert bleibt, kann eine drahtgebundene Übertragungsstrecke durch drahtlose Übertragung unmittelbar abgelöst werden. In diesem Fall bleibt der Austausch der Medien für die nächsthöheren Schichten komplett verborgen. Es muss lediglich ein spezieller Hardwaretreiber implementiert werden.
- Stellt die drahtlose Übertragung einen veränderten Dienstzugangspunkt zur Verfügung, in dem beispielsweise zusätzliche Parameter übergeben werden müssen, muss mindestens auch die den Dienstzugangspunkt aufrufende Schicht angepasst werden.
- Werden mit dem veränderten Medium auch noch zusätzliche Dienste verbunden, die nicht nur auf die unteren beiden Schichten beschränkt sind, so müssen die entsprechenden Applikationen unmittelbar angepasst werden. In den meisten Fällen erscheint eine Einbindung in das Betriebssystem und die Bereitstellung von ***A**pplication **P**rogram **I**nterfaces* (API) sinnvoll.

Mit der Verbreitung der Internet-Protokollfamilie und der Nutzung des TCP/IP-Protokollstapels in den vergangenen Jahren wurde das Modell auf vier Schichten reduziert. Dennoch bleibt die siebenschichtige Zählweise im allgemeinen Sprachgebrauch meist bestehen.

2.2.2 Klassifizierung des Kanalzugriffs

Eine der zentralen Aufgabenstellungen bei der organisatorischen Abwicklung von Kommunikation ist die Beantwortung der Frage, wer wann auf den Übertragungskanal zugreifen darf. Ebenso wie auf der Ebene der allgemeinen menschlichen Kommunikation haben sich in der technischen Realisierung verschiedenste Ansätze herausgebildet. Alle Realisierungen versuchen jedoch mit möglichst wenigen Regeln und möglichst ohne Behandlung von Ausnahmen auszukommen. Darüber hinaus ist zu berücksichtigen, dass jedes Aushandeln der Übertragungsparameter durch die Kommunikationsteilnehmer zusätzlichen Verkehr auf dem Medium verursacht.

Einige der möglichen Realisierungen wurden bereits in Abschnitt 2.1.4 beispielhaft vorgestellt.

Zentrale vs. dezentrale Zuteilung

Ein wesentliches Kriterium ist die Fragestellung, wer die Zugriffe verwaltet. Hier kann man zwischen zentraler und dezentraler Verwaltung unterscheiden. Während im zentralen Fall eine zentrale Station (*Master*) den anderen Stationen den Kanal zuteilt, fällt diese Aufgabe in der dezentralen Realisierung allen Stationen in gleichem Maße zu.

Deterministische vs. nicht-deterministische Zuteilung

Darüber hinaus ist von Bedeutung, in welcher Weise der Kanal zugeteilt wird. Im Rahmen einer deterministischen Zuteilung gibt es für jede Station eine definierte maximale Zeit bis zum nächsten Zugriff, während bei nicht-deterministischer Zuteilung kein solches Maximum definiert ist. Dieser Ansatz ist unabhängig von der zentralen oder dezentralen Zuteilung. Ein Beispiel für eine dezentrale deterministische Zuteilung ist das Token-Ring-Protokoll nach IEEE802.5, wohingegen Ethernet nach IEEE802.3 und auch Wireless-LAN nach IEEE802.11 Beispiele für die dezentrale nicht-deterministische Zuteilung sind.

Einführung von Zeitschlitzen

Bereits in Abschnitt 2.1.4 wurde dargelegt, dass im Rahmen eines zeitlich synchronisierten Zugriffs der unterschiedlichen Stationen die Wahrscheinlichkeit von Kollisionen verringert werden kann. Aus diesem Grund setzen praktisch alle modernen Übertragungsprotokolle so genannte Zeitschlitze (*time slots*) ein, die die grundlegende Zeiteinheit bei der Übertragung darstellen. Hierzu wird zusätzlich die Funktionalität der Synchronisation der Stationen benötigt.

2.2.3 Modell der physischen Kommunikation

Betrachtet man die physische Kommunikation auf einer allgemeinen Ebene, so lassen sich die drei Bestandteile Sender, Kanal und Empfänger unterscheiden. Bei der Implementierung von Sender und Empfänger spielen neben den logischen Schichten, die in Abschnitt 2.2.1 beschrieben wurden, die in Abbildung 2.3 gezeigten Bestandteile der physischen Schicht eine Rolle.

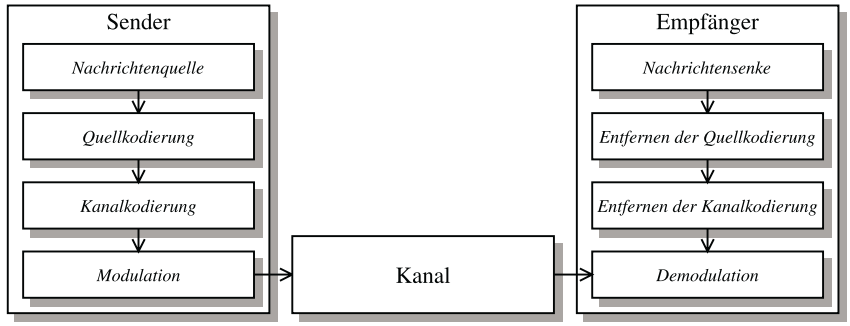


Abbildung 2.3: Kommunikationsmodell für die technische Realisierung auf der physischen Schicht

- Bei der Quellkodierung wird im Rahmen einer Redundanz- bzw. Irrelevanzminderung versucht, den Nachrichtenfluss der Quelle durch eine möglichst geringe digitale Symbolrate darzustellen. Die Quellkodierung wird in diesem Buch nicht näher erläutert.
- Die Kanalkodierung hat hingegen die Aufgabe, die aus der Quellkodierung erhaltenen Codewörter so umzugestalten, dass eine möglichst gute Anpassung an den Kanal erreicht wird. Üblicherweise wird gezielt Redundanz hinzugefügt, um beim Empfänger eine Erkennung oder möglicherweise auch eine Korrektur von Übertragungsfehlern zu ermöglichen. Da der drahtlose Übertragungskanal in hohem Maße störbehaftet ist (vgl. Abschnitt 2.4.3), findet die Kanalkodierung vielfach Anwendung. Häufig eingesetzte Verfahren sind ***F**orward **E**rror **C**orrection* (FEC) und ***C**yclic **R**edundancy **C**heck* (CRC).
- Analoge Signale wie Sprach-, Musik- oder Bildsignale befinden sich üblicherweise in der Basisbandlage, also im Tiefpassbereich. Praktische Übertragungskanäle haben hingegen in der überwiegenden Mehrzahl Bandpasscharakter, so dass das gesendete Signal spektral verschoben werden muss. Die klassische Lösung hierfür besteht in der Modulation eines sinusförmigen Trägers durch das Quellsignal. Hierbei werden die Parameter Amplitude, Frequenz oder Phase zeitlich verändert [Kammeyer 1992] (vgl. Abschnitt 2.5).

2.2.4 Klassifizierung von Kommunikation

Bei der Kommunikation über technische Netze unterscheidet man eine Reihe von grundsätzlich verschiedenen Realisierungsmöglichkeiten. Diese sollen im Folgenden kurz beschrieben werden, da sie unmittelbare Auswirkungen auf die Implementierung der drahtlosen Netze haben.

Leitungsvermittelte vs. paketvermittelte Kommunikation

Bei der Leitungsvermittlung (*Circuit Switching*) werden alle Netzteilstrecken physisch zu einer Ende-zu-Ende-Verbindung gekoppelt, wie dies in der oberen Hälfte der Abbildung 2.4 dargestellt ist. Auf diese Weise steht ein fester Übertragungskanal mit einer dezidierten Bandbreite zur Verfügung. Die Leitungsvermittlung ist historisch mit der Entwicklung der Sprachtelefonie verbunden, wobei in den frühen Systemen, die ausschließlich auf Kupferleitungen basierten, für jeden Übertragungskanal eine physische Verbindung geschaltet wurde.

Im Zeitalter digitaler Systeme findet die Leitungsvermittlung oft auch durch die periodische Reservierung von Zeitschlitzen im Sinne eines Zeitmultiplex statt, wie dies in der unteren Hälfte der Abbildung 2.4 dargestellt ist.

Vorteile	Nachteile
Garantierte Bandbreite	Die Leitung wird für eine Verbindung reserviert und steht für keine anderen Dienste oder Verbindungen zur Verfügung.
Sehr einfache und kostengünstige Realisierung der Geräte	Es können sinnvoll nur Punkt-zu-Punkt-Verbindungen aufgebaut werden.

Tab. 2.1: Vor- und Nachteile der Leitungsvermittlung

Bei der Paketvermittlung (*Packet Switching*) wird nur im Falle von Datenaufkommen ein Paket gebildet, das mit den notwendigen Adress- und Steuerinformationen versehen und in das Verbindungsnetz geschickt wird. Auf diese Weise können sich auch mehrere Stationen eine Verbindungsressource teilen. Dies ist in Abbildung 2.5 schematisch dargestellt.

Vorteile	Nachteile
Mehrfachzugang mehrerer Stationen auf eine Leitung ist möglich.	Die Gewährleistung von Dienstgüten ist problematisch.
Die Verteilung der Verkehrsströme auf mehrere Verbindungen ist möglich (Load Balancing).	Jedes Paket muss mit Steuerinformationen versehen werden. Dies verringert die nutzbare Bandbreite.

Tab. 2.2: Vor- und Nachteile der Paketvermittlung

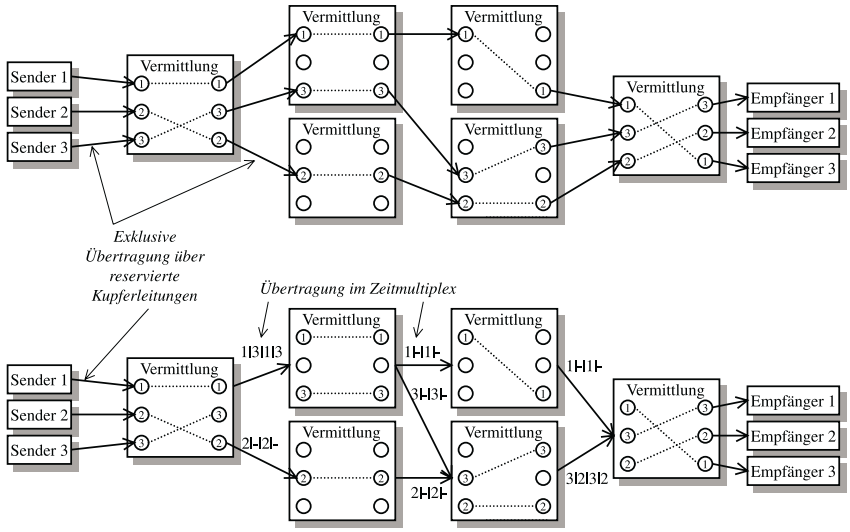


Abbildung 2.4: Schematische Darstellung der Leitungsvermittlung

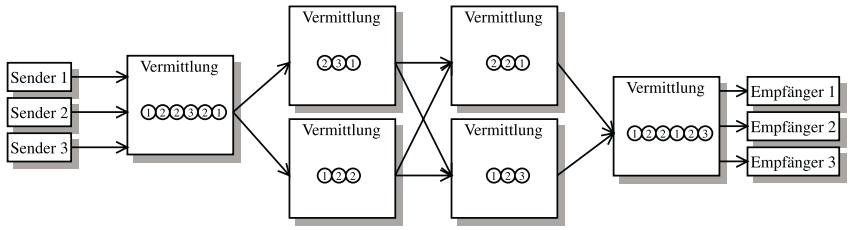


Abbildung 2.5: Schematische Darstellung der Paketvermittlung

Auf einen weiteren Aspekt bei der Abgrenzung zwischen Leitungs- und Paketvermittlung muss an dieser Stelle noch hingewiesen werden. Zunächst scheint die im Zeitbereich gemultiplexte Übertragung verschiedener leitungsvermittelter Systeme der Paketvermittlung zu entsprechen. Es bestehen aber zwei wesentliche Unterschiede:

- Bei der Leitungsvermittlung wird eine periodische Reservierung der Zeitschlitze vorgenommen. Diese werden auch dann den jeweiligen Übertragungsstrecken zugeteilt, wenn keine Informationen übertragen werden müssen. Dahingegen beanspruchen paketvermittelte Systeme nur dann Daten, wenn Informationen übertragen werden sollen.
- Bei der Paketvermittlung muss jedes Paket mit Adress- und Steuerinformationen versehen werden, um sein jeweiliges Ziel zu erreichen. Aufgrund der festen Zuordnung im Rahmen einer Kanalzuweisung können diese zusätzlichen Informationen in den Paketen entfallen.

Verbindungsorientierte vs. verbindungslose Kommunikation

Im Rahmen einer verbindungsorientierten Kommunikation (*Connection-Oriented Mode*) unterscheidet man grundsätzlich drei Phasen: Verbindungs-

aufbau, Datenübertragung und Verbindungsabbau. Dabei ist es unerheblich, ob es sich um eine Verbindung auf der physischen Ebene im Rahmen einer Leitungsvermittlung oder auf der logischen Ebene im Sinne einer Nachrichtenvermittlung handelt. Als typisches Beispiel unter Nutzung eines paketvermittelnden Netzes sei das ***T**ransport **C**ontrol **P**rotocol* (TCP) im Internet-Protokollstapel genannt. Dieses erlaubt die sequenzgerechte, fehlerfreie und vollständige Datenübertragung nach einem expliziten Verbindungsaufbau.

Dagegen verzichtet die verbindungslose Kommunikation (*Connectionless Mode*) ausdrücklich auf die Einrichtung physischer oder logischer Verbindungen. Informationsabschnitte werden ohne vorhergehende Kommunikation mit dem Empfänger in das Netzwerk gegeben. Verbindungslose Dienste basieren meist darauf, dass in den höheren Ebenen logische Verbindungen implementiert sind. Als Gegenstück zu TCP sei das ***U**ser **D**atagram **P**rotocol* (UDP) als verbindungsloses Protokoll genannt, das auf der Übertragung von einfachen Datagrammen basiert.

Zeitanforderungen

Unter einer synchronen Übertragung (griech: *syn* – mit; *chronos* – Zeit) versteht man in Zusammenhang mit der Kommunikation in Datennetzen entweder einen Datenstrom, der mit einem festen Takt übergeben wird, oder einen Ablauf, bei dem ein Prozess mit einem bestimmten Ereignis in einem anderen Prozess verbunden, d.h. synchronisiert wird.

Isochrone Übertragung (griech: *iso* – gleich) hingegen bezieht sich auf Prozesse, die gleichzeitig ablaufen müssen, um erfolgreich zu sein. Isochrone Übertragung ist zum Beispiel bei der Übertragung von Sprache oder Bewegtbildern erforderlich.

Asynchrone Übertragung (griech: *asyn* – nicht mit) als dritter Begriff lässt sich von den beiden anderen abgrenzen. Zum einen beschreibt die asynchrone Übertragung die Übermittlung von Daten unabhängig von anderen Signalen, z.B. einem Taktsignal. Zum anderen kann aber auch die Unabhängigkeit von Prozessen gemeint sein.

Symmetrische vs. asymmetrische Kommunikation

Symmetrische Kommunikation beschreibt den Austausch von Daten zwischen zwei gleichen Kommunikationspartnern. Hierzu wird im Allgemeinen die gleiche Transportcharakteristik in beiden Richtungen benötigt. Typische Beispiele sind die klassischen Telefonnetze, aber auch Verbindungen zwischen zwei Firmenniederlassungen zum Abgleich von Datenbanken.

Asymmetrische Kommunikation setzt ungleiches Verkehrsaufkommen zwischen den Kommunikationspartnern voraus. Als Beispiele seien hier typische Client-Server-Dienste genannt. So wird bei einem Zugriff auf einen Webserver (http-Server) vom Webclient (http-Client, Webbrowser) mit Hilfe eines meist geringen Datenvolumens der Dienst des Servers angefragt, der seinerseits mit einer umfangreichen Datensendung antwortet.

2.3 Anforderungen an Übertragungsnetze

2.3.1 Verkehrstypen

Neben der oben dargestellten Gliederung müssen die Anforderungen an ein Netzwerk noch nach den unterschiedlichen Verkehrstypen klassifiziert werden, wobei insbesondere die Übertragung von Sprache und von Daten unterschieden wird. Hier zeigt sich deutlich, dass den drahtlosen Netzen etwas zugemutet wird, was mit drahtgebundenen Netzwerken bislang nicht oder nur unzureichend umgesetzt werden kann, denn die Probleme der Sprachübertragung über ein Ethernet-IP-Netz sind allgemein bekannt.

Die Dienstgüte eines Netzwerks auf der Netzwerkebene bestimmt sich im Wesentlichen aus vier Parametern:

- Datenübertragungsrate (Bandbreite),
- Verzögerungszeit (Latenzzeit),
- Varianz der Verzögerungszeit (Jitter) und
- Verlustrate.

Dabei wird bei vielen Protokollen den besonderen Qualitätsanforderungen der unterschiedlichen Verkehrstypen bereits Rechnung getragen.

- Bei der Nutzung für reine Datenanwendungen (klassischer Datentransfer) werden für kurze und mittlere Zeiten hohe Datenraten benötigt. In Bezug auf eventuelle Verzögerungszeiten ist es jedoch lediglich wichtig, dass der gesamte Vorgang in einer akzeptablen Zeit abgeschlossen wird. Datenverluste sind keinesfalls hinnehmbar.
- Für die Übertragung von Sprache werden meist keine hohen Bandbreiten benötigt, es gelten jedoch besondere Anforderungen sowohl in Bezug auf die Latenzzeit der Übertragung als auch bezüglich der Varianz der Latenzzeit. Diese können im Allgemeinen nur durch die Reservierung von vorgegebenen Kanälen erfüllt werden. Andererseits leidet die Verständlichkeit nur wenig, wenn einzelne Bits während der Übertragung verloren gehen.
- Multimedia-Daten als Kombination von Bewegtbild und Ton, wie z.B. bei der Übertragung von Filmen, stellen wiederum eine veränderte Kombination der Anforderungen dar: Hohe Bandbreiten bei einer geringen Varianz der Latenzzeit. Die Größe der Latenzzeit hingegen erscheint zweitrangig. Die Verlustrate ist bis zu einem gewissen Grad unkritisch, da das menschliche Auge fehlende oder fehlerhafte Bildpunkte »ergänzt«.

2.3.2 Übertragungsgeschwindigkeit

Die Bandbreite eines Übertragungskanals wird üblicherweise mit Hilfe der Bitrate in Bit pro Sekunde angegeben. Werden jedoch mehrere Bit zu einem Zeichen oder Symbol zusammengefasst, wie dies bei einer mehrwertigen Übertragung der Fall ist (vgl. z.B. Abschnitt 2.5.3), so führt man die Symbolrate in Baud ein:

$$1\ Baud = 1\ Zeichen/s$$

Bei der Beschreibung der Leistungsfähigkeit von Übertragungsnetzen sollte man der Übertragungseffizienz im Sinne der Unterscheidung zwischen Brutto- und Nettodatenrate besondere Beachtung zukommen lassen.

Die Angabe einer Datenrate von 10 Mbps bedeutet zunächst einmal nicht mehr, als dass im zeitlichen Mittel alle 100 ns ein neues Bit auf den Kanal gegeben wird. In der Praxis stellt man jedoch fest, dass diese Bruttodatenrate bei weitem nicht erreicht wird. Die wesentlichen Gründe für die verringerte Nettodatenrate sind folgende:

- Zeitschlitze werden nicht genutzt.
  - Es kommt vor, dass zu verschiedenen Zeitpunkten keine Station auf den Kanal zugreifen will.
  - Ebenso können bei vielen Übertragungsprotokollen Kollisionen zwischen zwei Stationen auftreten, die zu einer Störung der Datenpakete führen und eine erneute Übertragung notwendig machen.
- Die Stationen müssen zusätzlich zu den reinen Nutzdaten Protokollaufwand betreiben.
  - Beispielsweise müssen in paketvermittelnden Netzen die Nutzdaten durch Adress- und Steuerinformationen ergänzt werden, damit die Pakete ihren Weg durch das Netz finden (vgl. Abbildung 2.5).
  - Die Stationen tauschen Informationen über ihre jeweilige Konfiguration aus. Diese Kommunikation findet über den normalen Übertragungskanal statt (*In-Channel Administration*). Entsprechend stehen diese Zeiten für den Nutzdatenverkehr nicht zur Verfügung.

2.4 Eigenschaften elektromagnetischer Wellen

2.4.1 Maxwellsche Gleichungen

In drahtlosen Systemen werden, anders als bei leitungsgebundenen Netzen, die elektromagnetischen Signale im freien Raum übertragen. Die hierbei eingesetzten elektromagnetischen Wellen lassen sich grundsätzlich mit den Gleichungen von James C. Maxwell (1831–1879) erklären, die die Entste-

hung elektromagnetischer Felder bei Vorhandensein beschleunigter elektrischer Ladung vorhersagen. Die Maxwellschen Gleichungen sind in Anhang A.1 angeführt.

2.4.2 Ausbreitung elektromagnetischer Wellen

Elektromagnetische Wellen können gemäß dieser Aussagen mit Hilfe von zeitlich veränderlichen Strömen in Leitern erzeugt werden. Ist die Länge des Leiters von der Größenordnung der Wellenlänge, dann können sich stehende Wellen ausbilden. Hierbei kommt es bei ausreichend großer Leistung zur so genannten Ablösung der elektromagnetischen Wellen vom Leiter.

Dabei ist sowohl die Charakterisierung des Nahfelds im Bereich des Ablösungsprozesses als auch des Fernfelds, das die Ausbreitung im freien Raum beschreibt, außerordentlich komplex. In Abhängigkeit von der Frequenz und der damit verbundenen Wellenlänge breiten sich elektromagnetische Wellen als Boden-, Oberflächen-, Raum- oder Direktwellen aus, wie dies in Abbildung 2.6 dargestellt ist. Die Berechnung mit Hilfe der Maxwellschen Gleichungen führt jedoch zu sehr komplizierten Rechnungen bzw. wird überhaupt nicht angewendet, wenn entweder die Geometrie oder die Materialeigenschaften nicht oder nur ungenau bekannt sind. Aus diesem Grund haben Modelle sehr weite Verbreitung gefunden, die lediglich die wesentlichen Eigenschaften der Funkkanäle berücksichtigen. Die Komplexität der Modelle hängt dabei in hohem Maße vom gewählten Abstraktionsgrad ab.

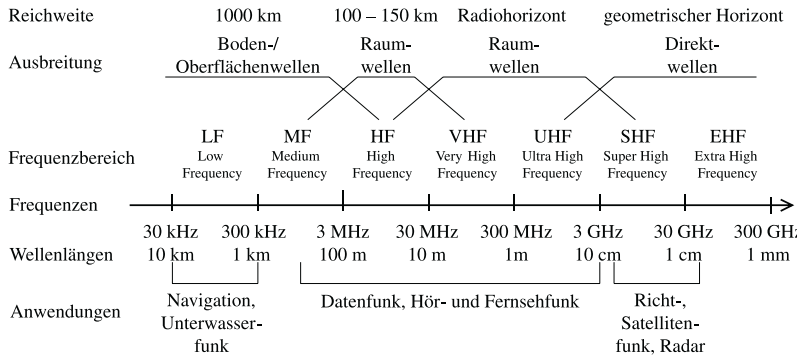


Abbildung 2.6: Ausbreitungseigenschaften elektromagnetischer Wellen in Abhängigkeit von ihrer Frequenz [Walke 2000]

Im Folgenden werden einige wesentliche Aussagen in Ergänzung zur Abbildung 2.6 aufgelistet:

- Allgemein gilt: Je höher die Frequenz der zu übertragenden Welle, desto geringer ist die Reichweite. Dies ist auf die Dämpfung der elektromagnetischen Wellen zurückzuführen, die in Abschnitt 2.4.3 näher erläutert wird.

- Wellen niedriger Frequenz breiten sich als Boden- oder Oberflächenwellen aus. Damit folgen sie auch der Erdkrümmung und erreichen sehr große Entfernungen.
- Bei höheren Frequenzen bilden sich hauptsächlich Raumwellen. Diese können Reichweiten von 100 bis 150 km erreichen, da die Wellen an der Troposphäre oder der Ionosphäre gebeugt oder reflektiert werden. Bei steigenden Frequenzen nimmt dieser Effekt und damit auch die überbrückbaren Entfernungen ab.
- Wellen oberhalb von 3 GHz breiten sich als Direktwellen aus und sind somit auf den geometrischen (optischen) Horizont beschränkt. Die Entfernung erreicht die als ***L**ine **o**f **S**ight* (LOS) bezeichnete Grenze. Dies gilt insbesondere für die elektromagnetischen Wellen mit Frequenzen im Terahertzbereich, das sichtbare Licht. Einige Aspekte der Ausbreitung von elektromagnetischen Wellen im Infrarotbereich werden in Abschnitt 2.4.4 erläutert.
- Die erreichbare Entfernung hängt zusätzlich von der pro Raumeinheit abgestrahlten Leistung ab. Die Effekte, die durch die Beschränkung der Raumwinkel erreicht werden können, werden in Abschnitt 2.9.1 näher erläutert.

2.4.3 Beeinträchtigung der Ausbreitung elektromagnetischer Wellen

Die räumliche Ausbreitung elektromagnetischer Wellen wird durch eine Vielzahl von Effekten beeinträchtigt. Hierzu zählen insbesondere Dämpfung, Streuung, Reflexion und Absorption.

Die Dämpfung reduziert die Feldstärke bei der wechselseitigen Erzeugung von elektrischem und magnetischem Wirbelfeld. Dabei ist die Dämpfung von vielen Faktoren abhängig:

- Nur im idealen Vakuum ist die Dämpfung Null.
- Bereits kleine Teilchen in allen Aggregatzuständen können eine Dämpfung der elektromagnetischen Wellen hervorrufen. Sowohl andere Gasmoleküle als auch flüssige Tropfen, wie z.B. Regen- oder Nebeltropfen, sowie feste Partikel oder Staub sind hier zu nennen.
- Die Dämpfung ist sehr stark von der Frequenz abhängig.
- Die Dämpfung durch größere Hindernisse kann sehr massiv sein. Einige Beispiele für den 2,4 GHz-Bereich sind in Tabelle 2.3 angegeben. Dabei handelt es sich um typische Werte, die nur für eine erste Einschätzung eingesetzt werden dürfen.

Tab. 2.3: Typische Dämpfungskoeffizienten im 2,4 GHz-Bereich

Hindernis	Typische Dämpfung	Quelle
Fenster in Ziegelsteinwänden	– 2 dB	[Compaq]
Ziegelwand neben einer Metalltür	– 3 dB	[Compaq]
Hölzerne Innentür	– 4 dB	[Andren 2001]
Leichtbauwand (Gipskarton), Bürowand	– 6 dB	[Andren 2001]
Metalltüren in Bürowand	– 6 dB	[Compaq]
Leichtbetonwand	– 12 dB	[Andren 2001]
Metalltüren in Ziegelsteinwand	– 12,4 dB	[Compaq]

Die Komplexität der Abhängigkeit der Dämpfung von Frequenz und Luftzusammensetzung zeigt beispielhaft Abbildung 2.7.

Streuung, Reflexion und Absorption führen in Gegenwart von Hindernissen zu einer Aufspaltung der ursprünglichen Welle. Dies hat zur Folge, dass eine Vielzahl von Signalen den Empfänger erreicht. Dabei können sich aufgrund von Laufzeitunterschieden und Frequenzverschiebungen starke Störungen ergeben. Ein Beispiel für die Mehrwegeausbreitung in einem geschlossenen Innenraum zeigt Abbildung 2.8. Dies ist offensichtlich besonders kritisch, wenn eine Antenne mit isotroper Abstrahlungscharakteristik (vgl. Abschnitt 2.9.1) eingesetzt wird.

Die beschriebenen Effekte sind insbesondere beim Aufbau und Betrieb von Funknetzen in Innenräumen zu berücksichtigen, da hier die Dichte von Hindernissen besonders groß ist. Ebenso wie bei der Auslegung von *Outdoor*-Mobilfunknetzen, bei denen die Geländetopologie berücksichtigt werden muss, arbeitet man auch bei der Planung von *Indoor*-Funknetzen mit der statistischen Beschreibung des Übertragungskanals [Walke 2000] und insbesondere mit empirischen Modellen. Typische Berechnungsbeispiele, die auch die Komplexität solcher Einschätzungen zeigen, finden sich in [Constantinou 1994]. Grundsätzlich sind die Reflexionseigenschaften abhängig vom Material und der Oberflächenbeschaffenheit des Hindernisses, von der Frequenz und der Polarisation der Welle und vom Einfallswinkel [Lebherz 1990].

Da die genaue Beschreibung der Umgebung jedoch sehr großen Aufwand erfordert, werden für die Qualifizierung der Systeme allgemeine Modelle eingesetzt. Drei Modelle finden dabei vor allem Anwendung [Halford 2000]:

- Beim Zweistrahlenmodell (2-Ray Model) werden ein direkter Strahl und ein reflektierter Strahl gleicher Intensität betrachtet. Die wichtigsten Kenngrößen für den reflektierten Strahl sind dann die mittlere und die maximale Verzögerungszeit sowie die Standardabweichung der Verzögerungszeit.

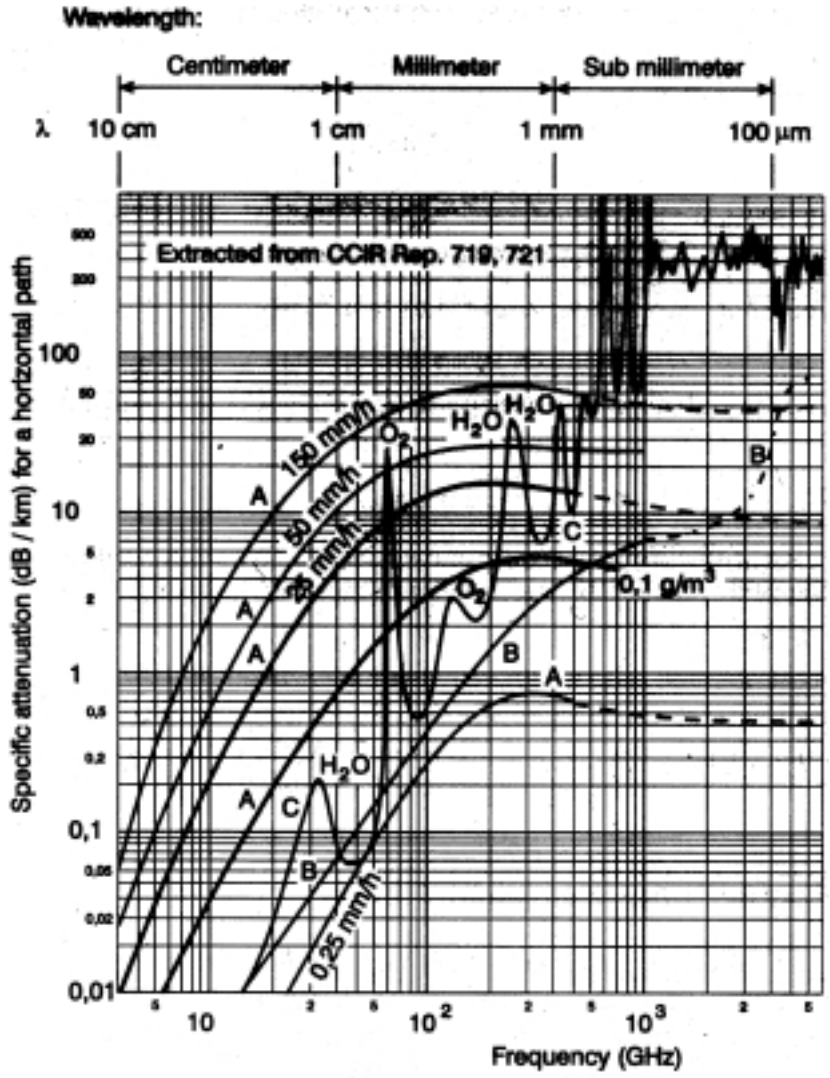


Abbildung 2.7: Dämpfung elektromagnetischer Wellen in Abhängigkeit von der Frequenz und der Luftzusammensetzung, aus der CCIR Rep. 719, 721, Abbildung aus [Walke 2000]

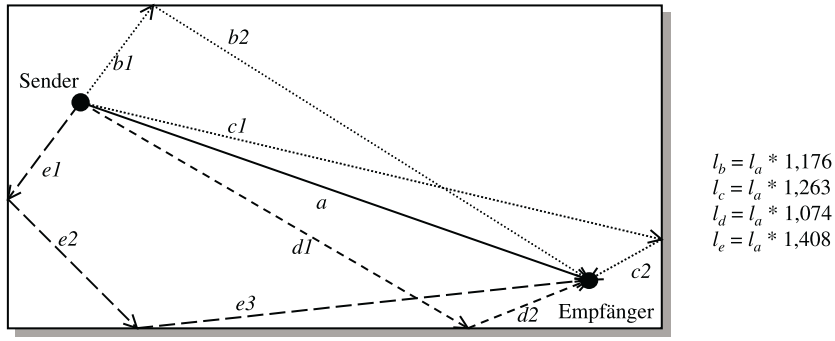


Abbildung 2.8: Die Abbildung zeigt beispielhaft einige Ausbreitungspfade in einem geschlossenen Innenraum.

Aufgrund der unterschiedlichen Längen der Ausbreitungspfade erreichen die Signale den Empfänger zu unterschiedlichen Zeitpunkten. Die relativen Längen zur geradlinigen Ausbreitung sind in der Übersicht angegeben.

- Die IEEE802.11-Spezifikation empfiehlt ein exponentielles Modell, das sich für eine Software-Modellierung sehr gut eignet. Dabei sind die Laufzeitpfade gleichverteilt, die Amplitude sinkt exponentiell ab.
- Als Kompromiss zwischen dem zu einfachen Zweistrahlenmodell und dem für viele Anwendungen zu komplizierten exponentiellen Modell finden in der Praxis die drei Szenarien des ***Joint-Standards-Committee***-Modells (JTC) Anwendung.

In diesem Zusammenhang muss noch der Begriff der Zelle definiert werden.

Unter eine Funkzelle versteht man die räumliche Region, innerhalb der Stationen kommunizieren können.

Da nun aber in einer Funkzelle auf mehreren physischen Kanälen übertragen werden kann, muss noch der Begriff einer logischen oder einer Kanalzelle eingeführt werden. Darunter versteht man die räumliche Region, innerhalb der Stationen auf einem Übertragungskanal kommunizieren können.

2.4.4 Einsatz von Licht zur Kommunikation

Wie bereits in Abschnitt 2.4.2 erwähnt, ist Licht als elektromagnetische Welle im Terahertzbereich in hohem Maße richtungsabhängig. Dies gilt in besonderem Maße für die im Kommunikationsbereich eingesetzten Laserquellen. Hieraus ergeben sich verschiedene Vor- und Nachteile:

- Für die Punkt-zu-Punkt-Verbindung zwischen zwei Stationen oder Netzwerken mit Sichtverbindung ist die geringe Streuung sehr positiv, da mit einer vergleichsweise geringen gesamten Ausgangsleistung am Sender immer noch eine hohe flächenbezogene Leistung am Sender erzielt werden kann.
- Die Herstellung von Laserdioden, wie sie für Verbindungen über kurze Entfernungen benötigt werden, ist sehr kostengünstig.

- Zwar können mit Hilfe einiger Vorkehrungen die Öffnungswinkel der Strahler vergrößert werden, dennoch muss in fast allen Fällen eine Ausrichtung der Stationen zueinander erfolgen. Dies ist unter anderem auch deswegen notwendig, weil die Strahlen nach der Reflexion an den meisten Hindernissen zu stark gedämpft sind, um noch vom Empfänger ausgewertet zu werden.
- Verbindungen zwischen mehreren Stationen im Sinne flexibler Netzwerke können nur sinnvoll durch die Kombination von Punkt-zu-Punkt-Verbindungen erreicht werden.

Aus diesen Gründen konnten sich Infrarotschnittstellen zur Kopplung von jeweils zwei Geräten im Rahmen des IrDA-Standards auf den verschiedenen Geschwindigkeitsstufen für eine gewisse Zeit und für eine Reihe von Anwendungen durchsetzen. Dennoch limitieren die mangelnden Netzwerkfähigkeiten und die unkomfortable Ausrichtung der Geräte zueinander viele Applikationen. Mit dem Vordringen der drahtlosen Netze, wie sie in diesem Buch vorgestellt werden, scheint die weitere Verbreitung der infrarotgestützten Kopplung gestoppt. Aus diesem Grund finden die entsprechenden Techniken und Standards in diesem Buch keine weitere Berücksichtigung.

Einige Anwendungen unter Nutzung von Licht sind in Abschnitt 2.1.5 genannt.

2.5 Digitale Modulationstechnik

2.5.1 Grundlegendes

Eine Übertragung digitaler Signale ist über die Luftschnittstelle im Basisband nicht möglich. Hierfür können zwei wesentliche Gründe angeführt werden:

- Das Frequenzspektrum eines solchen digitalen Signals ist sehr breit, im Normalfall sogar unbegrenzt. Bei der Berechnung des Frequenzspektrums eines periodischen Rechtecksignals mit Hilfe der Fourieranalyse erhält man das in Abbildung 2.9 beispielhaft gezeigte Ergebnis. Damit wäre eine Beschränkung eines Senders auf einen festen Frequenzbereich und damit das störungsfreie Nebeneinander unterschiedlichster Funksysteme nicht möglich.
- Darüber hinaus sind die Übertragungseigenschaften des Luftkanals in hohem Maße frequenzabhängig, wie in Abschnitt 2.4.2 dargestellt wurde. Auf diese Weise würde das Signal beim Empfänger nur mit einer sehr starken Verzerrung empfangen werden.

Aufgrund der Übertragungseigenschaften von elektromagnetischen Wellen in der Luft ist eine Übertragung der digitalen Signale im Basisband, wie sie

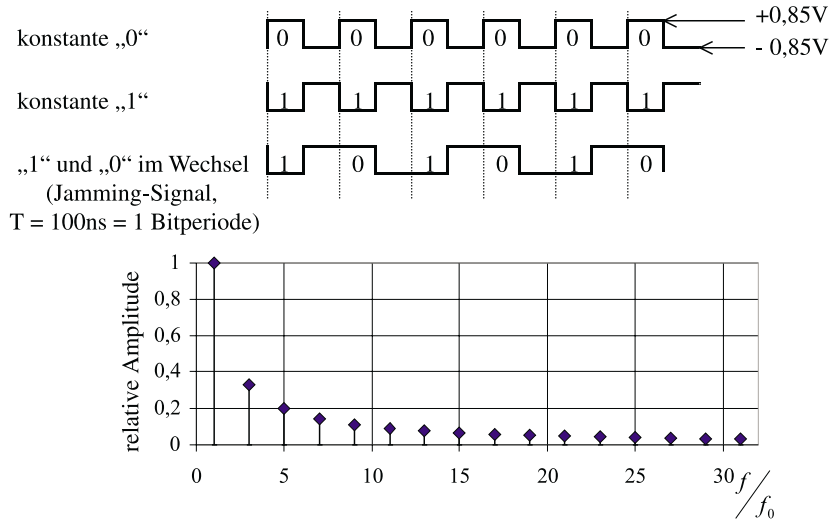


Abbildung 2.9: Frequenzspektrum einer periodischen Nullfolge in der Manchester-Kodierung des 10 Base-T Ethernet-Standards in der Basisbandübertragung

Bei der Manchester-Kodierung wird die Periode für die Übertragung eines Bits aufgeteilt. Die erste Hälfte enthält den komplementären Wert, die zweite Hälfte den darzustellenden Wert. Auf diese Weise werden gleichspannungsfreie Signale übertragen, bei denen die Taktrückgewinnung aus dem Datenstrom unabhängig von den übertragenen Informationen relativ einfach realisiert werden kann.

bei drahtgebundenen Netzwerken in vielen auch sehr leistungsfähigen Standards Einsatz findet, also nicht möglich. So werden beispielsweise die Signale in einem Ethernet zwar im Rahmen einer Kodierung umgesetzt und unter Umständen auch miteinander verbunden, so dass in einem Symbol mehrere Bits übertragen werden können. Es findet aber auf keiner Geschwindigkeitsstufe eine Modulation der Signale statt. Auch für das 10 Gb-Ethernet ist ein solcher Schritt nicht geplant.

Bei der Versendung analoger Signale mit Hilfe elektromagnetischer Wellen, wie z.B. bei herkömmlichen Radio- oder Fernsehsendern, werden die Audio- und Videosignale meist im Rahmen einer Amplituden- oder Frequenzmodulation übertragen. Bei der Übertragung digitaler Signale können die im Folgenden vorgestellten Technologien Einsatz finden. Dabei müssen bei lokalen Netzen insbesondere folgende Anforderungen berücksichtigt werden [Burkley 1994].

- Die spektrale Effizienz, die in Bit / MHz / Fläche angegeben wird, muss so groß wie möglich sein, um eine möglichst hohe Anzahl von Kanälen mit maximaler Bandbreite zu erreichen. Diese Forderung ist aufgrund des meist nur sehr beschränkt zur Verfügung stehenden Frequenzspektrums von zentraler Bedeutung. Es ist darauf hinzuweisen, dass dieser Aspekt auch als Forderung nach einer maximalen räumlichen Wiederholfrequenz formuliert werden kann. Dies ist notwendig, damit die Modula-

tionstechnik in zellularen Netzen eingesetzt werden kann, bei denen benachbarte Zellen die gleiche Modulationstechnik mit unterschiedlichen Parametern nutzen.

- Die Wahrscheinlichkeit von Übertragungsfehlern muss möglichst gering sein. Diese Forderung kann auch als Forderung nach einer minimalen Wahrscheinlichkeit von Bitfehlern (***B**it **E**rror **R**ate* – BER) gesehen werden.
- Der Implementierungsaufwand für die Modulationstechnik auf Sender- und Empfängerseite muss möglichst gering sein.

Die hier beschriebenen Anforderungen stehen im Wesentlichen in einem Zielkonflikt miteinander (vgl. Abbildung 2.10). Somit hängt das Optimum der Implementierung von der Wahl der Zielfunktion ab. Folgende Beispiele illustrieren dies:

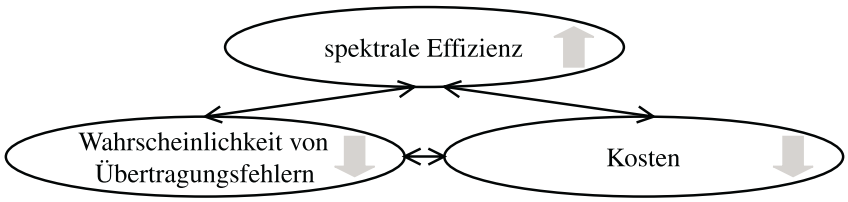


Abbildung 2.10: Zielkonflikte bei der Auswahl der Modulationsart

- Die spektrale Effizienz einer Modulationstechnik kann dadurch erhöht werden, dass mehrere Bits zu einem Symbol zusammengefasst werden, das mit Hilfe von mehr als zwei erlaubten Werten übermittelt wird. Hierdurch verringert sich aber unmittelbar der Signal-Rausch-Abstand (***S**ignal-To-**N**oise-**R**atio* - SNR). Entsprechend vergrößert sich die Wahrscheinlichkeit von Bitfehlern. Die Übertragung mit Hilfe mehrerer möglicher Werte (***M**ulti**l**evel **S**ignaling* – MLS) wird in den folgenden Abschnitten vorgestellt.
- Die Qualität des Empfängers kann in vielen Fällen durch zusätzlichen Aufwand vergrößert werden. Insbesondere adaptive Empfangsfilter, die auch die zeitlich variablen Eigenschaften des Kanals ausgleichen können, erreichen deutlich bessere Ergebnisse im Sinne verringerter BER. Auf der anderen Seite führt jeder zusätzliche Aufwand zu einer Erhöhung der Kosten – meist sowohl bei der Entwicklung als auch bei der Serienproduktion.

Die zunächst vorgestellten Modulationsverfahren beruhen darauf, dass man mit der Amplitude A(t), der Phasenlage φ(t) oder der Frequenz ω(t) einen der drei variablen Parameter aus Gleichung (2.1) in Abhängigkeit von der zu übertragenden Information verändert:

$$s(t) = A(t) * \cos(\omega(t) * t + \varphi(t)) \qquad (2.1)$$

Erst die Frequenzspreizverfahren stellen dann eine wesentliche Erweiterung dieses Ansatzes dar. Allerdings kann die technische Realisierung immer noch vergleichsweise ähnlich erfolgen.

Die Amplitudenmodulation hat aufgrund ihrer vergleichsweise hohen Störanfälligkeit sehr stark an Bedeutung verloren und findet bei digitalen Übertragungssystemen praktisch keine Anwendung. Sie wird deswegen hier nicht weiter berücksichtigt.

2.5.2 Phasenumtastverfahren

Das auch als ***P**hase **S**hift **K**eying* (PSK) bezeichnete Phasenumtastverfahren beruht darauf, dass bei unveränderter Frequenz und unveränderter Amplitude des übertragenen Signals die Phase des Signals verändert wird. Falls für die Übertragung binärer Signale nur zwei unterschiedliche Phasenlagen möglich sind, kann bei dieser ***B**inären **PSK**-Modulation* (BPSK) das Signal dargestellt werden als:

$$s(t) = b(t) * A * \cos(\omega t) \tag{2.2}$$

wobei b(t) = +1, wenn eine logische Eins übertragen wird und

b(t) = –1, wenn eine logische Null übertragen wird.

Auf der Empfängerseite kann die Demodulation mit einem ähnlichen Aufbau wie beim Sender erfolgen. Unter Berücksichtigung der Rauschsignale, die sich im Kanal zum Nutzsignal addieren, muss ein aufwändigeres Verfahren wie zum Beispiel die in Abbildung 2.11 gezeigte kohärente Demodulation Einsatz finden.

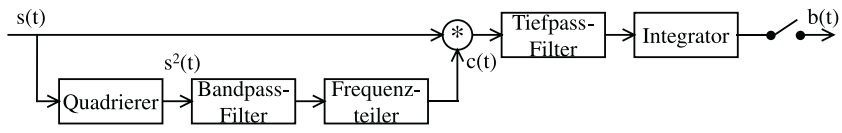


Abbildung 2.11: Grundsätzlicher Aufbau eines PSK-Demodulators

Ausgehend von dem empfangenen Signal

$$s(t) = \pm A * \cos(\omega t + \vartheta) \tag{2.3}$$

mit der Phasenverzögerung ϑ zwischen Sender und Empfänger wird das Signal quadriert und man erhält unabhängig vom Vorzeichen und damit unabhängig vom Zustand des übertragenen Bits

$$s^2(t) = A^2 * \cos^2(\omega t + \vartheta) = \frac{A^2}{2}(1 + \cos(2(\omega t + \vartheta))) \tag{2.4}$$

Wird dieses Signal nun auf einen Frequenz- und Amplitudenteiler gegeben, erhält man den Träger c(t). Wird dieser mit dem empfangenen Signal s(t) multipliziert, so ergibt sich:

$$s(t)*c(t)=\pm A*\cos(\omega t+\vartheta)*\cos(\omega t+\vartheta)=\pm\frac{A}{2}(1+\cos(2(\omega t+\vartheta))) \qquad (2.5)$$

Dieses Signal wird auf einen Integrator gegeben, der am Ende eines jeden Bitintervalls auf das Vorzeichen seines Inhalts ausgewertet wird.

Es können aber im Rahmen einer mehrwertigen Übertragung (***M**ulti**l**evel **S**ignaling* – MLS) auch mehr als zwei mögliche Zustände angenommen werden. Im Falle von vier möglichen Zuständen spricht man von QPSK (***Q**uarternary **PSK***). Stehen noch mehr Werte zur Verfügung, so bezeichnet man die Modulation als ***M**-wertiges **PSK*** (M-ary PSK). Die Lage der Phasen kann man dann durch die Darstellung in Diagrammen illustrieren, wie sie in Abbildung 2.12 für die Übertragung in Systemen nach IEEE802.11 gezeigt sind.

Vergleichsweise häufig wird auch die PSK- mit einer Amplitudenmodulation im Rahmen einer hybriden Modulation verbunden. Man erhält die so genannte ***Q**uadratur-**A**mplituden-**M**odulation* (QAM), bei der die Normal- und die Quadraturkomponente der Trägerschwingung durch unabhängige Datenfolgen moduliert werden.

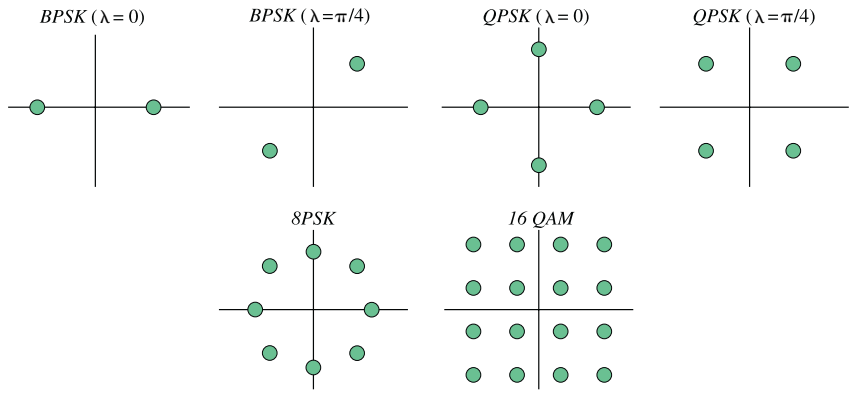


Abbildung 2.12: Phasendiagramme für die PSK- und die QAM-Modulation am Beispiel von IEEE802.11-Systemen

2.5.3 Frequenzumtastverfahren

Im auch als ***F**requency **S**hift **K**eying* (FSK) bezeichneten Frequenzumtastverfahren wird in Abhängigkeit von den binären Signalen die Trägerfrequenz verändert, so dass man im Sinne der Darstellung aus Gleichung (2.1) schreiben kann:

$$\omega(t)=\begin{cases}\omega_0 & \text{für "0"}\\ \omega_1 & \text{"1"}\end{cases} \qquad (2.6)$$

Bei der Auswahl der Frequenzen muss darauf geachtet werden, dass keine signifikante Erhöhung der Bandbreite erzeugt wird. Andererseits muss aber der Unterschied zwischen den Frequenzen ausreichend groß sein, um mit einem vertretbaren Aufwand eine Demodulation durchführen zu können. Dies ist insbesondere beim Aufbau eines nicht-kohärenten Empfängers wie in Abbildung 2.13 leicht einsehbar, da die Anforderungen an die Güte der Bandpassfilter mit abnehmendem Abstand zwischen den beiden Frequenzen steigen.

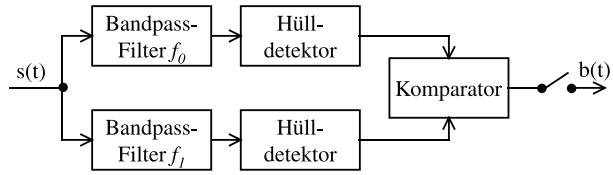


Abbildung 2.13: Grundsätzlicher Aufbau eines FSK-Demodulators

Darüber hinaus sollen möglichst keine Phasensprünge an den Signalübergängen auftreten, um einen möglichst einfachen Ausgangsverstärker einsetzen zu können. Diese Bedingung wird insbesondere vom ***M**inimum **S**hift **K**eying* (MSK) erfüllt. Dabei wird bei der Übertragung eines jeden Bits ein Phasenunterschied von 90° erreicht, so dass sprungfreie Signale resultieren.

Die spektrale Effizienz eines MSK-Systems kann durch die Filterung des digitalen Bitstroms verbessert werden. Oft wird ein Gauss'scher Filter mit

$$H(\omega) = e^{-0,45\omega/\omega_c}$$

eingesetzt. Weist dieser ein Bandbreiten-Zeit-Produkt (***B**andwidth **T**ime - BT*) größer als eins auf, dann erhält man weiterhin ein MSK-moduliertes Signal. Wird jedoch das BT-Produkt kleiner als eins (BT < 1) gewählt, tritt eine Überlagerung der Symbole auf (***Inter**symbol **I**nterference* - ISI). Diese erlaubt ein robusteres Verhalten bei Rauschen, benötigt allerdings einen aufwändigeren Demodulator.

2.6 Kanalzugriff

2.6.1 Überblick

Um mehrere Kanäle im Allgemeinen und mehrere drahtlose Systeme im Besonderen unabhängig voneinander betreiben zu können, muss der gemeinsam zur Verfügung gestellte Kanal aufgeteilt werden. Hier unterscheidet man im Wesentlichen vier Verfahren:

- das Zeitmultiplexverfahren (***T**ime **D**ivision **M**ultiple **A**ccess* – TDMA),
- das Frequenzmultiplexverfahren (***F**requency **D**ivision **M**ultiple **A**ccess* - FDMA),

- das Raummultiplexverfahren (***S**pace **D**ivision **M**ultiple **A**ccess* - SDMA) und
- die Codemultiplexverfahren (***C**ode **D**ivision **M**ultiple **A**ccess* - CDMA), die bei den Frequenzspreizverfahren (***S**pread **S**pectrum **T**echniques* - SST) in Abschnitt 2.7 vorgestellt werden.

Das auf dem FDMA-Verfahren aufbauende Orthogonale Frequenzmultiplexverfahren (***O**rthogonal **F**requency **D**ivision **M**ultiplex* – OFDM, vgl. Abschnitt 2.8) erlaubt die Nutzung mehrerer Unterfrequenzen für einen gebündelten Kanal.

2.6.2 Zeitmultiplexverfahren

Die Zeitmultiplexverfahren (***T**ime **D**ivision **M**ultiple **A**ccess* - TDMA) beruhen darauf, dass die Kommunikationsbestandteile verschiedener Kommunikationsteilnehmer zeitlich nacheinander über den Kanal übertragen werden. Wenn sich diese zeitliche Abfolge auf Hin- und Rückkanal zwischen zwei Kommunikationspartnern bezieht, spricht man auch von einem ***T**ime-**D**ivision-**D**uplex*-Verfahren (TDD). Das Zeitmultiplexverfahren nutzt hierzu einen hochbitratigen Übertragungskanal, der in der zeitlichen Abfolge auf mehrere Kanäle mit einer geringeren Datenrate verteilt wird. Das Zeitmultiplexverfahren zeichnet sich im Wesentlichen durch eine relativ einfache Realisierung der Zentralstation aus. Insbesondere kann der Frequenzmischer sehr einfach implementiert werden. Die Unterstützung von Handovers mit einem Wechsel der Basisstation erscheint ebenfalls recht einfach, da ohnehin die Übertragung eines Datenstroms zeitlich unterbrochen ist. Darüber hinaus kann durch eine Verlängerung der Zeitschlitze für einzelne Kommunikationsteilnehmer deren Datenrate vergrößert werden. Eine solche Bündelung von Zeitschlitzen erfolgt in der Praxis bei der paketorientierten Übertragung im Rahmen der ***G**eneral-**P**acket-**R**adio-**S**ervices*-Technik (GPRS) von ***G**lobal-**S**ystem-for-**M**obile-Communication*-Systemen (GSM) und bei der in Abschnitt 6.5.2 vorgestellten DPRS-Technik in DECT-Systemen für die Datenübertragung. Allerdings wird im Allgemeinen eine zentrale Verwaltung der Zeitschlitze für die verschiedenen Teilnehmer benötigt. Von Nachteil ist auch, dass ein TDMA-Kanal vergleichsweise hohe Bitraten aufweisen muss, um eine zeitliche Aufteilung noch sinnvoll zu erlauben. Darüber hinaus ist die Synchronisation zwischen Sender und Empfänger etwas aufwändiger, da die Übertragung zwischen den beiden Stationen ja immer wieder unterbrochen wird.

2.6.3 Frequenzmultiplexverfahren

Das Frequenzmultiplexverfahren (***F**requency **D**ivision **M**ultiple **A**ccess* - FDMA) stellt einem Kommunikationsstrom einen Frequenzbereich zur Verfügung, der unabhängig von den Frequenzbereichen der anderen Kommunikationsteilnehmer ist. Hierbei ist es neben einer zentralen Verwaltung vergleichsweise einfach möglich, dass eine kommunikationsbereite Station die

Frequenz selbstständig auswählt. Hierzu kann diese Station beispielsweise alle möglichen Übertragungsfrequenzen auf ihre Feldstärke hin überprüfen und annehmen, dass die Übertragungsfrequenz mit der geringsten Feldstärke frei ist.

2.6.4 Kombinierte Verfahren

Darüber hinaus sind Kombinationen der beiden Verfahren möglich. Auf diese Weise vergrößert sich die Anzahl der möglichen Nutzer. DECT-Systeme folgen beispielsweise einer Kombination von TDD-, TDMA- und FDMA-Verfahren mit zwanzig Zeitschlitzen, wobei jeweils zehn Zeitschlitze einer Übertragungsrichtung zugeordnet sind, und zwölf Frequenzen (vgl. Abbildung 6.1). Aber auch die bereits in Abschnitt 2.5.2 dargestellte QAM-Modulation stellt eine Kombination von Amplituden- und Phasenmodulation dar.

2.6.5 Raummultiplexverfahren

Bei Raummultiplexverfahren (***S**pace **D**ivision **M**ultiple **A**ccess* - SDMA) werden die zur Übertragung verwendeten Kanäle in geeigneten geometrischen Abständen im Rahmen einer so genannten Clusterbildung erneut verwendet. Man erreicht damit, dass trotz einer begrenzten Anzahl von Kanälen in einem unendlich ausgedehnten Raum unendlich viel Verkehr übertragen werden kann. Das Verfahren basiert auf der Tatsache, dass die Feldstärke eines Funksignals mit wachsendem Abstand vom Sender aufgrund der in Abschnitt 2.4.2 beschriebenen Dämpfung abnimmt. Bei einem ausreichend großen Abstand zweier Sender sind die jeweiligen Signale so schwach, dass die gegenseitigen Störungen vernachlässigt werden können.

2.7 Frequenzspreizverfahren

2.7.1 Grundlegendes

Die in Abschnitt 2.5 beschriebenen Verfahren haben – auch aus der historischen Entwicklung der technologischen Machbarkeit – einen großen Anteil bei den in der Praxis eingesetzten Systemen erlangt. Sie weisen jedoch mehrere Nachteile auf, die sich insbesondere beim Betrieb von mobilen Funknetzen bemerkbar machen und die mit den im Folgenden beschriebenen Frequenzspreizverfahren ausgeglichen werden können [Hatzold 2000].

Die herkömmlichen Verfahren zur Nachrichtenübertragung mit digital modulierten HF-Trägern sind vergleichsweise schmalbandig. Bei idealer Bandbegrenzung ist die Bandbreite gleich der Symbolrate, in der Praxis muss die Bandbreite aufgrund der Flankensteilheit (*Roll-Off*-Charakteristik) der eingesetzten Filter meist größer als die Symbolrate gewählt werden. Fre-

quenzspreizverfahren (***S**pread **S**pectrum **T**echniques* - SST) übertragen Signale mit einer größeren Bandbreite, als dies für die Symbolrate notwendig wäre.

- Es ergibt sich eine sehr große Anfälligkeit der Verfahren gegenüber Feldstärkeschwankungen durch Änderungen der Reflexionsbedingungen entlang des Ausbreitungsweges (*Fading*). Hierdurch kann sich eine starke Schwankung der empfangenen Leistung abhängig vom Standort der Empfangsantenne ergeben. Da die räumliche Charakteristik der sich ausbildenden stehenden Wellen von den Wellenlängen abhängig ist, kann durch die größere Bandbreite der Wellenlängen die lokale Schwankungsbreite der Feldstärke verringert werden.
- Nach Shannon berechnet sich die Übertragungskapazität *C* in Bit/s eines Nachrichtenkanals durch

  $$C = B * ld(1 + S/N) \qquad (2.7)$$

  Dabei ist B die Bandbreite des Kanals und S/N das Verhältnis von Signal- zu Störleistung (SNR).

  - Erhöht man demnach die Bandbreite, so steigt die Kanalkapazität linear an. Wird dieser Weg jedoch ohne weitere Vorkehrungen beschritten, läuft er der in Abschnitt 2.5.1 aufgestellten Forderung nach maximaler spektraler Effizienz zuwider.
  - Die Kanalkapazität steigt jedoch nur logarithmisch mit der Sendeleistung an.

Wichtige Voraussetzung für eine effiziente Nutzung, d.h. für eine möglichst große Übertragungskapazität eines limitierten Frequenzbereichs, ist, dass ein Verfahren gewählt wird, bei dem eine Überlagerung der Frequenzbänder unterschiedlicher Übertragungsstrecken störungsfrei möglich ist.

Darüber hinaus erreicht man mit Hilfe der Frequenzspreizverfahren eine sehr große Unempfindlichkeit gegen frequenzselektive Störungen. Hier ist auch die historische Herkunft der Verfahren zu sehen. Der ursprüngliche Anstoß für die Entwicklung der Frequenzspreizverfahren entstammt der Entwicklung militärischer Funksysteme, bei denen insbesondere die Stabilität gegenüber feindlichen Störsendern ein wichtiges Qualitätsmerkmal ist. Diese weisen im Allgemeinen eine hohe Signalstärke bei einer begrenzten Frequenzbandbreite auf. Aber auch der zeitgleiche Betrieb vieler autonomer Stationen in einer entsprechend störbehafteten Umgebung kann mit Hilfe von Frequenzspreizverfahren effizient ermöglicht werden, da gleichzeitig zwei Effekte erreicht werden:

- Zum einen lässt sich eine recht hohe Unempfindlichkeit gegenüber Störeinflüssen auf dem Übertragungskanal erzielen.
- Zum anderen ist auch der Einfluss einer Station, die nach einem Frequenzspreizverfahren arbeitet, auf ihre Umgebung vergleichsweise gering.

Aus diesem Grund eignen sich Frequenzspreizverfahren in besonderer Weise sowohl für den Einsatz in Umgebungen mit hohen Störeinflüssen als auch für eine hohe Dichte von autonomen Stationen. So ist beispielsweise die Nutzung des 2,4 GHz-ISM-Bandes an den Einsatz von Frequenzspreizverfahren mit bestimmten Rahmenbedingungen gebunden.

Man unterscheidet zwei grundsätzliche Verfahren: das Frequenzsprung-Spread-Spectrum-Verfahren (***F**requency **H**opping **S**pread **S**pectrum* - FHSS-Verfahren) und das Direct-Sequence-Spread-Spectrum-Verfahren (***D**irect-**S**equence **S**pread **S**pectrum* - DSSS), die in den Abschnitten 2.7.2 und 2.7.3 beschrieben werden. Weitere Kriterien zur Abgrenzung der beiden Technologien finden sich in Abschnitt 10.3.

2.7.2 Frequenzsprung-Spread-Spectrum-Verfahren

Das Prinzip des Frequenzsprung-Spread-Spectrum-Verfahrens besteht darin, dass sowohl Sender als auch Empfänger nach einer pseudozufälligen Abfolge (***P**seudo **R**andom **S**equence* - PRS) die Trägerfrequenz wechseln. Den Wechsel der Trägerfrequenz bezeichnet man als *Hop*. Das grundsätzliche Verfahren ist in Abbildung 2.14 dargestellt. Der Sender 1 hat z.B. mit seinem Empfänger die Frequenzfolge f_1, f_{76}, f_2, f_{78}, f_3, f_{75}, f_{76}, f_{77}, f_4, f_{79}, f_{78}, f_{77} ausgehandelt. Hierdurch sind eventuelle Störungen auf die Übertragung der Station 1 durch eine ununterbrochen auf einer Frequenz sendende Station 3, bei der es sich z.B. um einen Störsender handeln kann, oder durch eine andere FHSS-Station 2, die mit ihrem Kommunikationspartner eine andere Frequenzfolge festgelegt hat, auf kurze Zeitabschnitte begrenzt.

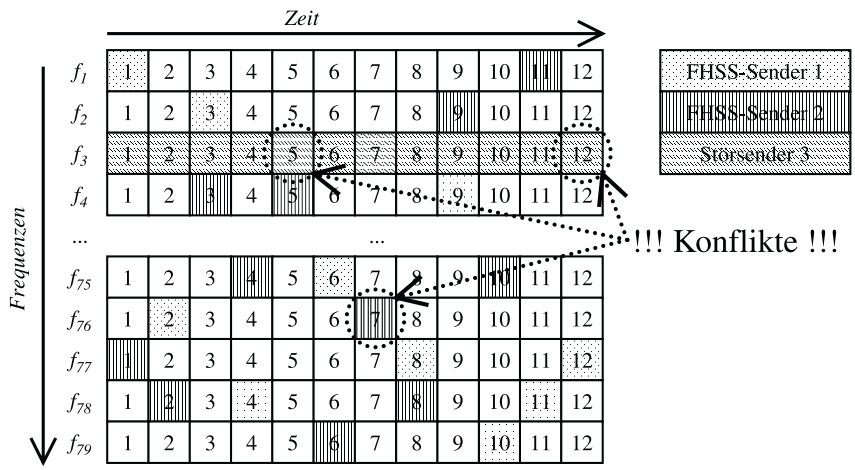


Abbildung 2.14: Funktionsweise des Frequenzsprungverfahrens

Man unterscheidet

- die schnelle FHSS-Übertragung, bei der zwischen zwei Frequenzsprüngen nur ein Symbol übertragen wird, und

- die langsame FHSS-Übertragung, die auf jeder der Sprungfrequenzen jeweils mehrere Symbole überträgt.

In Bezug auf die Systemarchitektur unterscheidet man

- asynchrone bzw. unkoordinierte FHSS-Systeme. Bei diesen werden die Frequenzsprünge auf den unterschiedlichen Übertragungsstrecken auch in überlappenden Funkbereichen unkoordiniert durchgeführt.
- synchrone bzw. koordinierte FHSS-Systeme, bei denen die Frequenzsprünge aller Stationen innerhalb einer Funkzelle gleichzeitig erfolgen.

Der wichtigste Vorteil des Frequenzsprung-Spread-Spectrum-Verfahrens besteht darin, dass sich die zugehörigen Systeme recht einfach und entsprechend kostengünstig realisieren lassen. Dabei erzielen sie meist auch einen geringen Energieverbrauch.

2.7.3 Direct-Sequence-Spread-Spectrum-Verfahren

Beim DSSS-Verfahren wird die Frequenzspreizung durch die logische Exklusiv-Oder-(XOR-)Verknüpfung der Daten mit einer Pseudozufallsfolge (***P**seudo-**R**andom **N**umerical **S**equence* - PRS oder auch PN-Sequenz) erreicht, die eine höhere Bitrate aufweist. Die einzelnen Signale innerhalb dieser PN-Sequenz werden als Chips bezeichnet. Der Aufbau dieser Operation auf der Senderseite ist in Abbildung 2.15 gezeigt. Auf der Senderseite erfolgt die inverse Verknüpfung. Diese wird in Anhang A.2 erläutert.

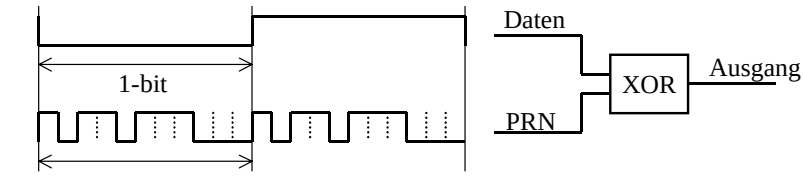


Abbildung 2.15: Grundsätzlicher Aufbau eines DSSS-Modulators (Zyren1)

Von grundlegendem Vorteil ist bei diesem Verfahren, dass die schmalbandige Störung der hohen Intensität I auf dem Kanal in ein breitbandiges Rauschen niedriger Intensität I_{PN} gespreizt wird (Abbildung 2.16). Auf diese Weise kann eine hohe Störunempfindlichkeit erreicht werden.

Das DSSS-Verfahren wird gerne mit der Party-Situation verglichen, wo einzelne Schlüsselwörter, wie zum Beispiel der eigene Name, auch aus einem sehr hohen allgemeinen Geräuschpegel herausgehört werden können.

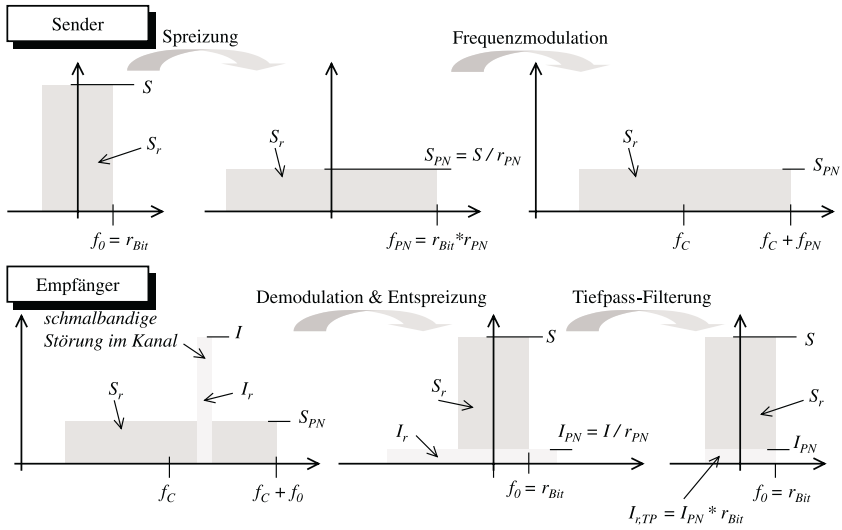


Abbildung 2.16: Veränderungen des Frequenzspektrums bei DSSS-Verfahren

Folgende Aspekte sind mit dem DSSS-Verfahren verbunden:

- Die Spektraleffizienz von DSSS-Verfahren ist sehr hoch, somit kann eine hohe Nutzerdichte bei begrenzter Bandbreite und hohen Datenraten erreicht werden.
- Durch die Verknüpfung der Nutzdaten mit dem höherbitratigen PN-Code erhöht sich die Übertragungsrate. Hierdurch erhöhen sich sowohl die Geschwindigkeitsanforderungen an den Senderbaustein als auch der Energieverbrauch.
- Auf der Empfangsseite werden mehrere Empfänger benötigt, die das Signal auswerten. Dies führt ebenfalls zu einer vergrößerten Komplexität der Empfängerbausteine und zu gestiegenem Energieverbrauch.

2.8 Orthogonale Frequenzmultiplexverfahren

Die orthogonalen Frequenzmultiplexverfahren (***O**rthogonal **F**requency **D**ivision **M**ultiplex* - OFDM) beruhen auf der parallelen Datenübertragung durch Frequenzmultiplexverfahren. Sie werden auch als *Multi-Carrier-* oder *Discrete-Multitone-*Verfahren bezeichnet. Sie erlauben hohe Datenraten bei vergleichsweise guter Störunempfindlichkeit insbesondere gegenüber schmalbandigen Störungen. Durch die Aufspaltung auf verschiedene Übertragungskanäle erreicht man, dass jeweils nur einige wenige Bits fehlerhaft übertragen werden, die jedoch durch eine geeignete Kodierung korrigiert werden können. Darüber hinaus lässt sich jede Unterfrequenz effizient auf die Eigenschaften des Übertragungskanals anpassen. Auf diese Weise kann insbesondere den

mit der Varianz der Signallaufzeiten (*Delay Spread*) über unterschiedliche Ausbreitungspfade (*Multipath*) verbundenen Schwierigkeiten begegnet werden, wie sie bei der drahtlosen Übertragung im Frequenzbereich von 5 GHz auftreten. OFDM findet neben den Wireless-LAN-Systemen auch im Bereich des digitalen Rundfunks (***D**igital **A**udio **B**roadcasting* - DAB) Anwendung. Aber auch bei drahtgebundenen Übertragungsprotokollen mit hoher spektraler Effizienz, wie z.B. ***A**symmetric **D**igital **S**ubscriber **L**ine* (ADSL), wird OFDM eingesetzt.

Der wesentliche Unterschied zu herkömmlichen Frequenzmultiplexverfahren, die relativ große Abstände zwischen den verschiedenen Kanälen aufweisen und deswegen das Frequenzspektrum nur mangelhaft ausnutzen, besteht darin, dass sich bei OFDM-Verfahren die Spektren der verschiedenen Kanäle überlappen dürfen. Um trotzdem Störungen der Kanäle zu vermeiden, nutzt OFDM Unterfrequenzen (*Subcarrier Frequencies*), die zueinander orthogonal sind. Dies bedeutet, dass die Signalrate T eines jeden Unterkanals gerade so gewählt wird, dass sie dem Frequenzabstand zwischen zwei benachbarten Unterkanälen entspricht.

In der Abbildung 2.17 ist mit der $si(f\text{-}f_n)$-Funktion die Fourier-Transformierte eines mit der Trägerfrequenz f_n multiplizierten Rechtecksignals der Dauer $T = 1 / f_0$ dargestellt. Diese Funktion besitzt Nullstellen an allen Frequenzen, für die gilt:

$$f_{Null} = f_n \pm N * f_0 \quad \text{mit} \quad N = -\infty,...,-2,-1,0,1,2,...,\infty \tag{2.8}$$

Werden nun jeweils um f_0 verschobene Trägerfrequenzen eingesetzt, dann können die Unterkanäle unabhängig voneinander empfangen werden. Unabhängig heißt in diesem Zusammenhang, dass keine Verzerrungen auftreten, die sich normalerweise bei der Überlagerung von Trägerfrequenzen durch die ***Inter**symbol **I**nterference* (ISI) ergeben. Technische Voraussetzung ist dabei eine sehr hohe Genauigkeit der Trägerfrequenzen.

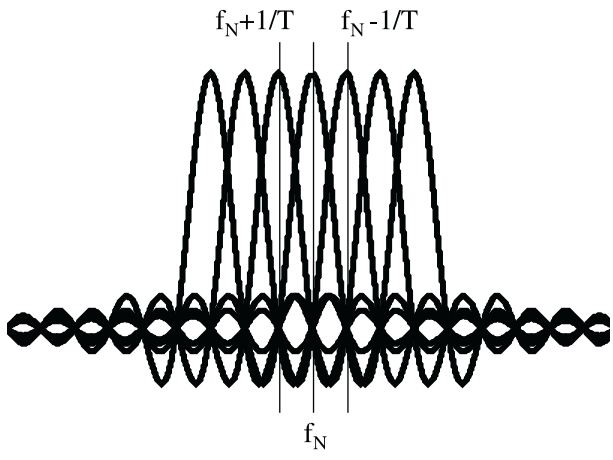


Abbildung 2.17: Darstellung von orthogonalen Unterfrequenzen in einer OFDM-Übertragung im Frequenzbereich. Am Maximum einer Unterfrequenz weisen die anderen Träger eine Nullstelle auf.

In Abbildung 2.18 sind drei Trägerfrequenzen beispielhaft dargestellt, die unabhängig voneinander demoduliert werden können.

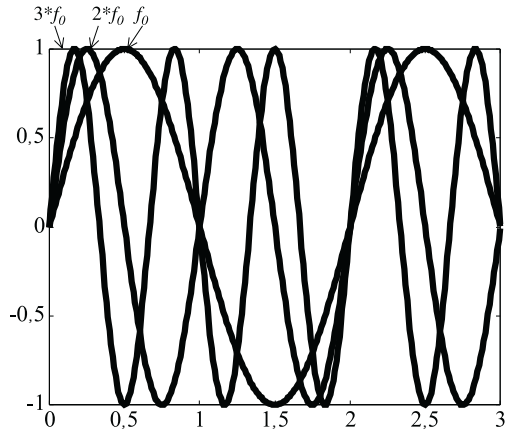


Abbildung 2.18: Beispielhafte Darstellung von drei orthogonalen Unterfrequenzen in einer OFDM-Übertragung im Zeitbereich. Zur Übersichtlichkeit weisen die drei Trägersignale die gleiche Amplitude und die gleiche Phasenlage auf.

Dennoch sind OFDM-Empfänger kostengünstig zu realisieren, da keine steilflankigen Filter oder Entzerrer (*Equalizer*) benötigt werden. Es müssen lediglich eine Schnelle Fourier-Transformation (***F**ast-**F**ourier **T**ransform* - FFT) bzw. deren Umkehrfunktion (***I**nverse **FFT*** - IFFT) durchgeführt werden [Walke 2000].

2.9 Antennen

2.9.1 Isotrope und anisotrope Antennen

Die Übertragung mit Hilfe elektromagnetischer Wellen setzt den Einsatz von Sende- bzw. Empfangsantennen voraus. Hierfür sind eine Vielzahl von Einflussfaktoren zu berücksichtigen, die die Leistungsfähigkeit der Systeme wesentlich beeinflussen können. Dabei sind in keinem der im weiteren Verlauf des Buches beschriebenen Standards Anforderungen an die Eigenschaften der Antennen vorgegeben.

Ein wesentlicher Parameter, der die in Abschnitt 2.4.2 erläuterte Reichweite elektromagnetischer Wellen bestimmt, ist deren Leistung. Die Feldstärke einer elektromagnetischen Welle nimmt im freien Raum umgekehrt proportional mit der Entfernung zum Sender ab. Die Eingangsleistung am Empfänger nimmt entsprechend mit dem Quadrat der Entfernung ab.

Geht man zunächst von der in Abbildung 2.19 gezeigten idealen punktförmigen Strahlungsquelle aus, die ihre Leistung P_S gleichverteilt in alle Richtungen, d.h. omnidirektional, aussendet, so breitet sich diese Leistung kugelförmig im Raum aus.

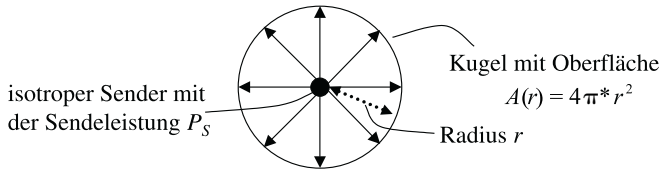


Abbildung 2.19: Abstrahlungscharakteristik einer isotropen Antenne

Die gesamte Leistung wird also im Abstand r vom Sender auf eine Kugelfläche mit $A(r)$ verteilt. Eine punktförmige Empfangsantenne, die sich auf der Kugeloberfläche befindet, erhält die Leistungsdichte

$$p = \frac{P_S}{4\pi * r^2} \quad \left[\frac{W}{m^2}\right] \tag{2.9}$$

In der Praxis werden Antennen eingesetzt, die ihre Leistung in bestimmte Vorzugsrichtungen bündeln. Diese werden in Anhang 11.3 näher dargestellt.

2.9.2 Diversizität

Die starke Empfindlichkeit der räumlichen Positionierung der Empfangsantenne kann durch den Einsatz von mehreren räumlich getrennten Antennen ausgeglichen werden. Um den Aufbau zu erleichtern, werden diese Antennen in einem Gehäuse ausgeliefert und decken typischerweise den Abstand von weniger als einer halben Wellenlänge ab. Auf diese Weise kann dann im Rahmen der *Antenna Diversity* (engl. *diversity* für: Mannigfaltigkeit, Verschiedenheit, Vielfalt, Unterschiedlichkeit) diejenige Antenne ausgewählt werden, die im Bereich der größten Feldstärke liegt. Darüber hinaus lässt sich auch eine Richtungsbündelung durch die Interferenzeffekte der Sektoren der Antennen erreichen. Je nach elektronischer Beschaltung kann auf diese Weise auch ein adaptives Ausrichten einer Empfangsantenne auf die Richtung des stärksten Empfangssignals unterstützt werden.

2.9.3 Polarisation

Darüber hinaus spielt auch die Polarisationsrichtung der elektromagnetischen Welle eine Rolle. Insbesondere im Falle einer stabförmigen Sendeantenne erfolgt die Abstrahlung mit einer Vorzugspolarisationsrichtung, die von einer stabförmigen Empfangsantenne ebenfalls erwartet wird, um eine möglichst gute Anregung der Ladungsträger in der Antenne zu erreichen. Dabei ist die Wahl der Polarisationsrichtung in vielen Fällen vom Standort und von der Bauform vorgegeben. Der Einsatz von Leiterplattenantennen in PC-Karten für den Einsatz in Notebook-Computern bedingt eine horizontale Polarisation, die am besten auch von den beteiligten Kommunikationspartnern übernommen wird [Andren 2001].

2.9.4 Standort

Störend ist dagegen die Richtcharakteristik bei vielen mobilen Anwendungen. Hier ist eine möglichst gleichmäßige, d.h. isotrope, Ausstrahlung in alle Richtungen anzustreben. Zwar kann die Richtungsunabhängigkeit der Antennen zumindest in größeren Entfernungen recht gut erreicht werden, in der Praxis ist aber die Abschattung durch Hindernisse zu berücksichtigen. Aus diesem Grund ist der Standort der Antennen von zentraler Bedeutung. Dabei sind die Ausmaße der Antennen recht gering, so dass verschiedene Einbauarten Verbreitung gefunden haben. Eine Antenne mit der Länge einer Wellenlänge misst im 2,4 GHz-Band etwa 12,5 cm. Entsprechend kann eine $\lambda/4$-Antenne auf etwas mehr als 3 cm untergebracht werden. Im Wesentlichen lassen sich zwei Einbauarten unterscheiden:

- Im Gerät integriert. Hier gibt es zahlreiche verschiedene Bauformen:
  - In der PC-Karte des Notebook-Computers ohne externes Ansatzstück. Dabei ist die direkte Abstrahlungsrichtung auf einen Kegel aus dem PC-Kartenschacht beschränkt.
  - In der PC-Karte des Notebook-Computers ohne externes Ansatzstück. Der direkte Abstrahlungskegel kann hierdurch vergrößert werden. Dennoch verbleibt ein starker Funkschatten auf der Seite, auf der die Signale erst den Rechner durchqueren müssen.
  - Im Deckel des Notebook. Diese Technik bietet die besten Ergebnisse bei größtmöglichem Komfort, solange der Deckel keine weiteren Metallteile enthält. Sie setzt allerdings im Allgemeinen die Installation durch den Notebook-Hersteller voraus und ist somit auf absehbare Zeit den Geräten der höheren Preisklasse vorbehalten.
  - Im Desktop-PC. Diese Bauform wird aufgrund des meist ungünstigen Standorts des Desk»tops« »unter« einem abschattenden Schreibtisch (vielleicht mit Metallgerüst) selten gewählt.
- Mit Hilfe einer externen Antenne. Dieser Anschluss bringt zwar ein weiteres Peripheriegerät in das Kabelgewirr auf dem Schreibtisch und ist besonders lästig bei Geräten mit hoher Mobilität, führt aber für vorwiegend stationär betriebene Geräte zu den besten Ergebnissen, da selbst eine geringe Verschiebung des Notebooks zu einer wesentlichen Verschlechterung des Funkergebnisses führen kann. Insbesondere scheint sich die unkomplizierte Anschlussmöglichkeit über USB durchzusetzen.

2.9.5 Auswahl

Antennen werden in zahllosen Varianten angeboten. Da die Antennen unabhängig vom verwendeten Protokoll und vom Hersteller der aktiven Geräte sind, wird in Abbildung 2.20 eine Übersicht über die wesentlichen Parameter mit jeweils einigen Beispielen gegeben, die bei der Auswahl der Anten-

nen zu berücksichtigen sind. Zu beachten ist bei der Installation unbedingt die Dämpfung der Antennenleitung, da die Übertragung bereits im RF-Bereich erfolgt. Die Dämpfung beträgt mindestens 0,2 dB / m.

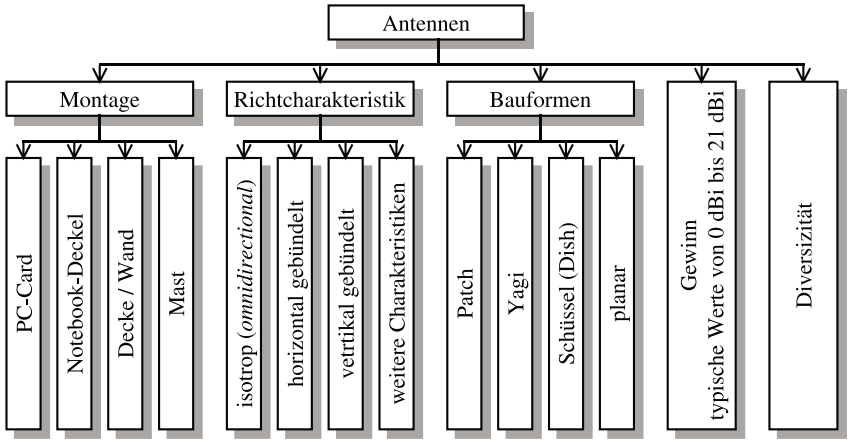


Abbildung 2.20: Übersicht über die wichtigsten technischen Parameter bei der Antennenauswahl

2.10 Besonderheiten drahtloser Netze

2.10.1 Drahtlose Netze nutzen ein allgemeines Medium

Die drahtlose Übertragung von Informationen weist eine Reihe von Besonderheiten auf, die bei drahtgebundenen Systemen nicht oder nur sehr eingeschränkt zu berücksichtigen sind. Die wesentliche Aussage ist, dass die Übertragung durch die Luft ein allgemeines Medium nutzt. Dies gilt in doppelter Hinsicht:

- Die unterschiedlichen Stationen greifen auf das gleiche Medium zu, so dass wechselseitige Beeinflussungen auftreten. Bei Nutzung des gleichen Übertragungskanals sind unbedingt Regeln für den Zugriff auf das Medium anzuwenden.
- Die Regeln für die Nutzung der Luftschnittstelle werden von hoheitlichen Aufsichtsbehörden vorgegeben, um übergreifende gesellschaftliche Interessen zu wahren.

2.10.2 Räumliche Charakteristik

Die Anordnung von Sendern und Empfängern im Raum führt zu verschiedenen Effekten, die bei der Konzeption drahtloser Netze eine wichtige Rolle spielen:

- Aufgrund der räumlichen Verteilung des Signals ist eine Kanalüberwachung an einem Ort nicht möglich. Insbesondere kann die Kollisionserkennung beim Sender, wie sie beim klassischen Ethernet unterstützt wird, nicht umgesetzt werden. Diese Problematik bezeichnet man als *Near-Far-* oder *Hidden-Station-Problem*.
- Die Ausbreitung des Signals ist räumlich nicht beschränkt. Allerdings nimmt die Stärke des Signals nach den Gesetzmäßigkeiten der Dämpfung ab, wie sie in Abschnitt 2.4.2 besprochen werden. Dies hat insbesondere drei Auswirkungen:
  - Nur innerhalb einer bestimmten Entfernung zwischen Sender und Empfänger ist das Verhältnis der Leistungen von Nutzsignal und Störeinflüssen (***S**ignal-to-**N**oise-**R**atio* – SNR) groß genug für eine ausreichende Empfangsqualität.
  - Werden mehrere Funkzellen betrieben, so kann die Situation eintreten, dass ein Gerät die Signale von mehreren Funkzellen gleichzeitig empfängt. Dann muss eine Entscheidung getroffen werden, welche Funkzelle die jeweils aktive ist.
  - Es ist nicht auszuschließen, dass innerhalb des Funkbereichs die gesendeten Signale auch von nicht autorisierten Stationen empfangen werden können. Um ein unerlaubtes Abhören zu verhindern, bedarf es entsprechender Sicherheitsvorkehrungen.
  - Die räumliche Charakteristik des Übertragungskanals ist zeitlich veränderlich. Aus diesem Grund kann keine Anpassung des Kanals erfolgen, wie sie beispielsweise bei drahtgebundenen Medien zur Unterdrückung von Reflexionen an Leitungsenden erfolgt. Entsprechend können übertragene Nachrichten nicht nur durch die Überlagerung von zwei unterschiedlichen Nachrichtenpaketen gestört werden, sondern auch durch die Überlagerung der originalen mit den reflektierten Signalen.

2.11 Frequenzzuweisungen

Bei den in diesem Buch vorgestellten Technologien sind in Bezug auf die Frequenzzuweisungen drei Fälle zu unterscheiden:

- Es handelt sich um einen Frequenzbereich, der für die Nutzung durch eine definierte Funktechnologie reserviert ist. Als Beispiel kann der Bereich von 1880 MHz bis 1900 MHz dienen, der im Geltungsbereich der ETSI für die DECT-Technologie (vgl. Kapitel 6) reserviert ist.
- Es handelt sich um einen Frequenzbereich, der für die Nutzung von Funktechnologien unter Einhaltung bestimmter Regeln reserviert ist. Das US-amerikanische ***U**nlicensed **N**ational **I**nformation **I**nfrastructure* (UNII)-Band oder das europäische *License-Exempt-Frequenzband* im 5 GHz-Bereich ist hier als Beispiel zu nennen.

- Es handelt sich um einen Frequenzbereich, der unter Einhaltung bestimmter Regeln für verschiedenste Anwendungen reserviert ist, die elektromagnetische Wellen abstrahlen. Hierbei besitzen die lizenzierungsfreien ISM-Bänder besondere Bedeutung, die weltweit für industrielle, wissenschaftliche und medizinische Zwecke (***I**ndustrial*, ***S**cientific*, ***M**edical* – ISM) freigegeben sind. Insbesondere die Frequenzen im 2,4 GHz-Bereich werden von zahlreichen Kommunikationsprotokollen genutzt, so z.B. von IEEE802.11, Bluetooth, HomeRF und eventuell von Upbanded DECT. In diesem Bereich liegen aber auch andere Sender, wie z.B. Mikrowellenherde. Diese sind übrigens der hauptsächliche Grund, dass dieser Frequenzbereich freigegeben wurde, da er für andere lizenzierungs- und kostenpflichtige Übertragungsverfahren ein zu hohes Aufkommen an Störern aufweist.

  In diesem Zusammenhang muss allerdings darauf hingewiesen werden, dass dieses 2,4 GHz-Band nicht in allen Nationen vollständig freigegeben wird. Dies führt dann zu einer geringeren Anzahl von Kanälen. Von diesen Einschränkungen sind insbesondere Japan, Frankreich und Spanien betroffen. Allerdings steht seit Anfang 2000 nun auch in Frankreich und Spanien das gesamte Spektrum von 2400 bis 2483 MHz zur Verfügung. Auch die weiteren Spezifikationen, wie z.B. die erlaubte abgestrahlte Leistung und die Modulationsverfahren, unterscheiden sich zum Teil deutlich.

  Für die Nutzung des 2,4 GHz-ISM-Frequenzbereichs ist in Nordamerika und in Europa der Einsatz eines Frequenzspreizverfahrens vorgeschrieben.

  Für den Fall, dass ein FHSS-Verfahren eingesetzt wird, darf ein Kanal eine Frequenz höchstens 400 ms benutzen. Zwei aufeinander folgende Frequenzen müssen mindestens einen Abstand von 6 MHz aufweisen.

  Für den Fall, dass ein DSSS-Verfahren eingesetzt wird, war ursprünglich in den Nutzungsrichtlinien die Verwendung eines PN-Codes mit einer Länge von mindestens 11 Bit vorgesehen.

Eine Übersicht über die Frequenzzuweisungen für den europäischen Raum zeigt Abbildung 2.21.

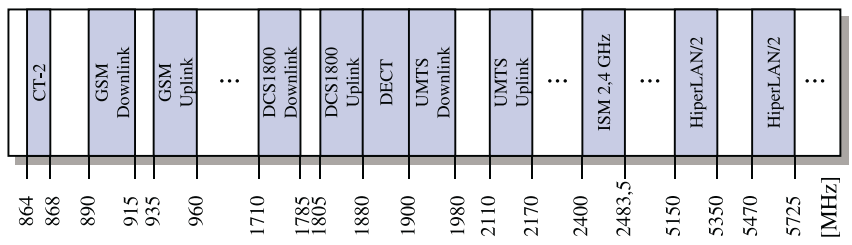


Abbildung 2.21: Übersicht über die Frequenzzuweisungen für den europäischen Raum. Regionale Abweichungen werden in den jeweiligen Abschnitten besprochen.

3 Anwendungen, Geräte und Standards

3.1 Anwendungsszenarien

Die drahtlose Übertragung von Informationen ersetzt das Kabel zunächst lediglich auf der Bitübertragungsschicht im ISO-OSI-Referenzmodell. Diese grundlegende Aussage hat jedoch noch zwei Aspekte:

- Die wesentlichen Netzwerkarchitekturen, wie sie sich während des jahrzehntelangen Einsatzes drahtgebundener Netzwerke etabliert haben, werden auch von den drahtlosen Netzen übernommen. Entsprechend findet sich eine große Übereinstimmung zwischen der Gliederung der üblichen Netzwerkanwendungen und der in den folgenden Abschnitten dargestellten Anwendungsszenarien.
- Durch die verschiedenen Mobilitätsaspekte, die sich durch den Einsatz der drahtlosen Netze ergeben, kann die Integration von intelligenten Mehrwertdiensten attraktiv erscheinen. Werden diese Dienste auf den höheren Ebenen mit dem physischem Übertragungsprotokoll der untersten Ebene verbunden – wie dies bei Bluetooth der Fall ist –, dann ist ein drahtloses Netz doch mehr als nur ein Kabelersatz.

3.1.1 Personal Area Networks

Unter dem vergleichsweise neuen Begriff des ***P**ersonal **A**rea **N**etwork* (PAN) fasst man die Kommunikation von Geräten eines oder einiger weniger Nutzer im Umkreis von etwa 10 m zusammen. Hierbei sind im Wesentlichen drei Szenarien zu unterscheiden:

- Die Kopplung von Peripheriegeräten, wie Drucker, Mobiltelefon, ***P**ersonal **D**igital **A**ssistant* (PDA), Digitalkamera mit einem PC zur Datenübertragung bzw. zum Datenabgleich.
- Die Kopplung von externen Bediengeräten mit der Dienstplattform. Typisches Beispiel ist das von Ericsson als Gehäuse bereits sehr früh vorgestellte Headset für Mobiltelefone auf Bluetooth-Basis.
- Die Kopplung von mehreren PCs zur Datenübertragung. Diese Architektur stellt einen unmittelbaren Grenzfall zu den klassischen LANs dar.

Ausgehend von den Anwendungen kann man annehmen, dass sich die kommunizierenden Geräte meist im gleichen Raum oder zumindest in der unmittelbaren Nähe befinden. Dabei lassen sich die meisten Anwendungen mit moderaten Bandbreiten zufrieden stellen.

Für diese PAN-Anwendungen ist von essentieller Bedeutung, dass die Funkmodule mit möglichst geringen Kosten implementiert werden können, da die Funktionalität auch in vergleichsweise einfachen und kostengünstigen Geräten implementiert werden muss, um die nötige Akzeptanz zu erreichen.

Von zentraler Bedeutung dabei ist, dass mehr als eine Punkt-zu-Punkt-Verbindung unterstützt wird und dass Datenraten erreicht werden, die eine sinnvolle Kopplung verschiedener leistungsfähiger Geräte ermöglicht. Deswegen werden die Funkmäuse und Funktastaturen, wie sie von verschiedenen Herstellern zum Betrieb im 27 MHz-Band angeboten werden [Gieselmann 2001], nicht zu den PANs gezählt. Vielmehr ist sehr wahrscheinlich, dass die PAN-Technologien diese proprietären Systeme ablösen werden.

3.1.2 Local Area Networks

Unter einem lokalen Netz (***L**ocal **A**rea **N**etwork* - LAN) versteht man die Kopplung von mehreren Geräten in einem Gebäudebereich. Ein typisches Szenario besteht in der Verknüpfung von Client-PCs, Servern und Peripheriegeräten wie Druckern in einem Bürogebäude. Die typischen Entfernungen zwischen den Stationen betragen entsprechend einige zehn bis einige hundert Meter. Die Bandbreitenanforderungen sind deutlich höher als bei einem PAN, da ein Austausch auch größerer Dateien und auch der Betrieb von Applikationen über das Netzwerk möglich sein muss. Bei den in der Realität installierten Netzwerken sind drei typische Anwendungsklassen zu unterscheiden.

3.1.3 SoHo-LAN

Viele Haushalte und kleinere Büros (***S**mall **O**ffices and **H**ome **O**ffices - SoHo*) verfügen über einige wenige Rechner, die miteinander vernetzt werden und gemeinsam auf Ressourcen wie Drucker oder Modem zugreifen sollen. Für drahtlose Systeme bedeutet dieses Szenario insbesondere:

- Die Anforderungen an die Leistungsfähigkeit der Systeme ist moderat, da meist mit nur geringen Datenmengen hantiert wird und die Anzahl der Stationen im Netz recht limitiert ist. Meist reicht eine Funkzelle aus, um die unterschiedlichen Rechner zu versorgen.
- Die Kosten spielen eine recht wichtige Rolle, da die Investitionen in den meisten Fällen aus der Privatschatulle bezahlt werden müssen. Andererseits ist aber der Preisdruck nicht so hoch wie bei den PANs, da die Anzahl der benötigten Module meist recht gering und die Komplexität der ausgestatteten Systeme vergleichsweise hoch ist
- Die Anzahl der Benutzer und Stationen ist beschränkt. Somit werden keine oder nur rudimentäre Werkzeuge zur Netzwerkadministration benötigt. Deren Bedienung muss aber möglichst intuitiv sein, damit auch Laien diese Systeme einrichten und verwalten können.

Der SoHo-Markt stellt für die Hersteller von WLAN-Systemen einen wichtigen Aspekt bei der Marktdurchdringung dar, da zum einen zunehmend große Stückzahlen in diesem Marktsegment erreicht werden können, so dass man bereits von Skalierungseffekten profitieren kann, zum anderen aber die technischen Anforderungen meist nicht so hoch angesiedelt sind wie in größeren Büroumgebungen, so dass auf diese Weise die Lernkurve leichter durchschritten werden kann [Frost 1999].

3.1.4 Büro-LAN

Dahingegen stellt die Kopplung von Rechnern in größeren Büroeinheiten immer höhere Anforderungen an die Netze. Die Verbindung von Hunderten bis zu mehreren tausend Rechnern an einem Standort stellt keine Seltenheit mehr dar.

Bei der Verwendung drahtloser Systeme sind aber folgende Gesichtspunkte zu berücksichtigen:

- Die Anforderungen an die Leistungsfähigkeit der Systeme sind deutlich höher. Es werden vielfach größere Datenmengen ausgetauscht, die Anzahl der Stationen im Netz kann recht hoch werden. In vielen Fällen reicht eine Funkzelle nicht aus, um die räumliche Ausdehnung oder die benötigte Anzahl von Kanälen zu erreichen.
- Die Kosten spielen eine wichtige Rolle, da die Anzahl der benötigten Module meist vergleichsweise hoch ist.
- Die Anzahl der Benutzer und Stationen kann sehr hoch sein. Deswegen werden leistungsfähige Werkzeuge zur Netzwerkadministration benötigt, deren Bedienung im Allgemeinen Fachleuten überlassen wird.

3.1.5 Kopplung von Netzwerken

Darüber hinaus muss die Kopplung von Netzwerken betrachtet werden, da hier vielfach drahtlose Netze Einsatz finden:

- *LAN-LAN-Kopplung:* Als Grenzfall für ein lokales Netzwerk gilt, dass sich die Geräte nicht nur in einem Gebäude, sondern in verteilten Lokationen befinden. Dann bietet es sich in vielen Fällen an, die Netzwerke unmittelbar miteinander zu koppeln, ohne den expliziten Schritt über ein Weitverkehrsnetz zu gehen. Allerdings ist die für den Nutzer transparente Verschaltung von LANs auch über ein Weitverkehrsnetz mit Hilfe eines virtuellen Netzes möglich.
- *LAN-WAN-Kopplung:* Ein weiterer Grenzfall ist die Ankopplung von lokalen Netzen an Weitverkehrsnetze in dem Sinne, dass die physische Anbindung im lokalen Bereich mit Hilfe einer LAN-Technologie erfolgt. Im Bereich der drahtlosen Übertragungssysteme spricht man dabei von ***W**ireless **L**ocal **L**oop* (WLL).

3.2 Gerätetypen

Zur Erfüllung dieser Aufgaben müssen verschiedene Geräte zur Verfügung gestellt werden. Man unterscheidet insbesondere:

- Netzwerkadapter, die die Verbindung der Endgeräte ermöglichen. Hierbei kann man noch einmal fünf Kategorien beobachten:
  - PC-Cards zum Einsatz in Notebooks
  - PCI-Karten zum Einsatz in Desktop-Computern. Da die Anbindung von stationären Desktop-PCs weniger Marktbedeutung aufweist als die drahtlose Vernetzung von portablen Notebooks, basieren die PCI-Lösungen nicht selten auf den PC-Cards. Die Kompatibilität wird dann mit Hilfe zusätzlicher Schaltkreise hergestellt.
  - USB-Stationen zum flexiblen Einsatz an Desktop- und Notebook-Computern. Allerdings muss die Unterstützung sowohl durch die PC-Hardware als auch durch das Betriebssystem gegeben sein. Insbesondere für ältere PCs, aber auch für Rechner, die unter Microsoft-Windows-NT4.0 betrieben werden, ist dies nicht gegeben.
  - Integrierte WLAN-Adapter, die vom Hersteller fest in das Notebook eingebaut werden
  - Netzwerkkarten zur Ankopplung von Embedded Systemen. Hierbei handelt es sich bislang oft noch um anwendungs- oder kundenspezifische Lösungen.
- Zugangspunkte, die die Kopplung zwischen den drahtlosen Netzsegmenten und den verdrahteten Segmenten herstellen.
- Brücken zur Realisierung einer LAN-LAN oder LAN-WAN-Kopplung.

3.3 Standards

Von den am Markt verfügbaren Produkten erscheinen zum Zeitpunkt der Drucklegung folgende Kandidaten von Bedeutung:

- IEEE802.11
- Bluetooth
- DECT
- HomeRF und
- HiperLAN/2

Diese werden in den Kapiteln 4 bis 8 im Detail besprochen. Abbildung 3.1 zeigt eine Übersicht, in der die zwei wichtigsten Kenngrößen aufgetragen sind. Diese Darstellung bedarf allerdings aus zwei bereits erwähnten Gründen der Kommentierung.

- Bei der Bandbreite handelt es sich um die Brutto-Bandbreite. Die tatsächlich erreichbare Netto-Datenrate liegt oft deutlich darunter. Die Unterschiede ergeben sich durch nicht genutzte Zeitschlitze, durch Kollisionen sowie durch das Protokoll in dem Sinne, dass zum einen Header zur Adressierung und Qualifizierung an die Pakete angehängt werden müssen und zum anderen die Stationen untereinander auch noch Informationen zur Verkehrssteuerung austauschen. Diese Anteile unterscheiden sich zwischen den Systemen unter Umständen sehr stark, andererseits sind die Werte aber auch in hohem Maße abhängig von dem jeweiligen Verkehrsaufkommen.
- Die Reichweite bezieht sich auf die ungehinderte Ausbreitung unter der Voraussetzung, dass eine direkte Sichtverbindung (***L**ine **o**f **S**ight* - LOS) besteht. Die großen Bereiche, die in dem Diagramm angegeben sind, ergeben sich beim Einsatz von Antennen mit Richtcharakteristik, die bei unveränderter Ausgangsleistung die Reichweite im Vergleich zu einer isotropen Antenne wesentlich vergrößern können. Dieser Aspekt ist aber im Wesentlichen unabhängig vom Protokoll.
- Im praktischen Einsatz ist aber oft keine Sichtverbindung vorhanden. Zusätzliche Hindernisse vergrößern die Dämpfung. Dies führt entweder zu einer Verringerung der Reichweite oder der erreichbaren Bandbreite.

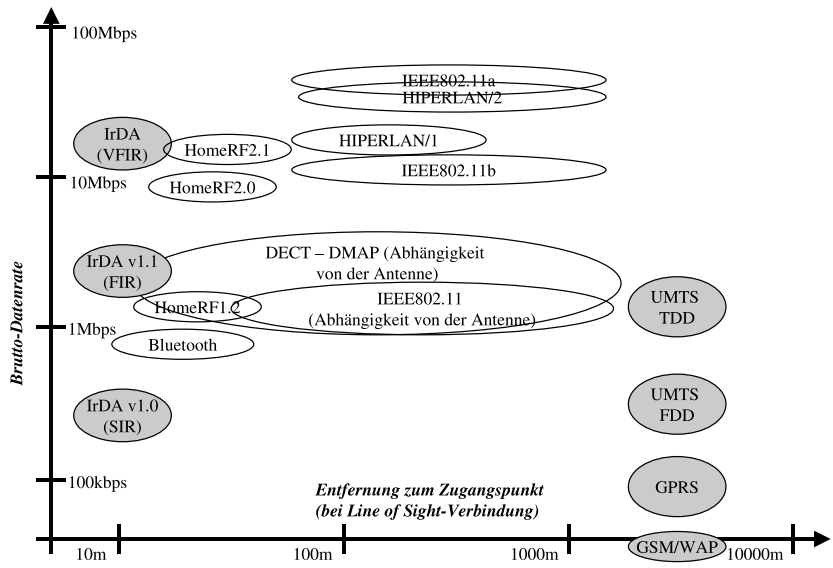


Abbildung 3.1: Überblick über die WLAN-Technologien. Zum Vergleich sind auch die IrDA-Infrarot-Technologien und die Zugangstechnologien über Mobilfunknetze aufgeführt.

4 IEEE802.11

4.1 Standard

4.1.1 Positionierung

Die Familie des 802.x des IEEE (vgl. Abschnitt 1.5) bildet eine allgegenwärtige Plattform im Bereich der lokalen Netzen (***L**ocal **A**rea **N**etworks* – LAN). Insbesondere gehören die Ethernet-Standards nach 802.3 in den unterschiedlichen Geschwindigkeitsklassen von 10 Mbps bis zu den gegenwärtig in der Spezifikation befindlichen 10 Gbps zu dieser Familie. Abbildung 4.1 zeigt die wichtigsten Standards und ihre wechselseitigen Beziehungen im Überblick.

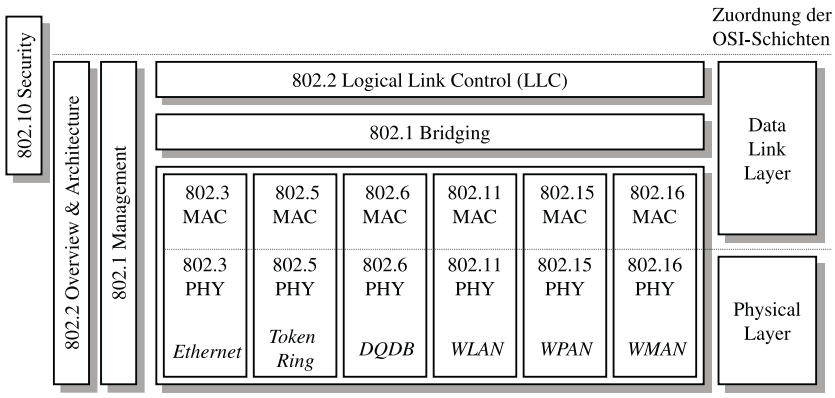


Abbildung 4.1: Die wichtigsten Standards der IEEE802-Familie und ihre wechselseitigen Beziehungen im Überblick

Für drahtlose lokale Netze hat die Standardisierungsvereinigung (***S**tandards **A**ssociation* – SA) des IEEE im Jahr 1997 nach einer etwa sieben Jahre langen Erstellungs- und Genehmigungsphase mit dem 802.11 den ersten herstellerunabhängigen Standard für Übertragungsprotokolle verabschiedet. Deswegen trifft man für den ursprünglich verabschiedeten Standard auch manchmal auf die Schreibweise IEEE802.11-1997. Seit April 2001 steht der Standard in der Ausgabe von 1999 zum Download bereit (*http://standards.ieee.org/getieee802/*). Ein allgemeiner Überblick über die IEEE802.11-Technologien findet sich in [Sikora 2001 (1)].

Im Umfeld des IEEE802.11-Standards haben sich weitere Gremien gebildet, die helfen sollen, den Markterfolg und die Interoperabilität der Geräte zu gewährleisten:

- Die ***W**ireless **LAN A**ssociation* (WLANA) (*http://www.wlana.com*) soll die Verbreitung des Standards durch Marketing- und Informationsaktivitäten unterstützen.
- Die im August 1999 gegründete ***W**ireless **E**thernet **C**ompatibility **A**lliance* (WECA) (*http://www.wi-fi.com*) zertifiziert die Interoperabilität der 802.11-kompatiblen Geräte. In diesem Zusammenhang werden die Geräte nach IEEE802.11 auch unter dem Markennamen Wi-Fi™ (***Wi**reless **Fi**delity*) vermarktet. Bis dahin hatte das im März 1996 gegründete ***W**ireless **LAN I**nteroperability **F**orum* (WLIF) eine ähnliche Zielrichtung verfolgt und auch die im April 1997 veröffentliche Spezifikation zur Interoperabilitätsprüfung erarbeitet.

4.1.2 Aufbau

Die Familie der 802-Standards beschreibt mit der Bitübertragungsschicht (*Physical Layer*) und der Sicherungsschicht (*Data Link Layer*) die unteren zwei Schichten des ISO / OSI-Referenzmodells (vgl. Abschnitt 2.2.1). Dabei wird die Verbindungsschicht noch einmal unterteilt: Die Zugriffssteuerung übernimmt das ***M**edium **A**ccess **C**ontrol* (MAC), die logische Steuerung der Verbindungen ist Sache des ***L**ogical **L**ink **C**ontrol* (LLC), das für alle Standards nach IEEE802 identisch ist. Auf diese Weise können Protokolle der darüber liegenden Schichten unabhängig vom Zugriffsmechanismus und der physikalischen Realisierung auf die Kommunikationsdienste zugreifen. Insbesondere bedeutet dies, dass die drahtlosen Protokolle nach 802.11 von Protokollen wie TCP / IP (Schichten 4 und 3) in prinzipiell der gleichen Weise genutzt werden können wie herkömmliche drahtgebundene Protokolle nach 802.3. Einschränkungen im Sinne einer reduzierten Datenrate können sich dennoch durch die mehrfache Implementierung von Algorithmen zur Fehlerkorrektur oder Verkehrssteuerung ergeben, wie sie in Abschnitt 10.5 erläutert werden.

Der IEEE802.11-1997-Standard spezifiziert Datenraten von 1 und 2 Mbps. Der Standard unterteilt sich in die Beschreibung eines MAC-Protokolls und drei alternativer PHY-Protokolle. Mit einem Frequenzsprung- (FHSS) und einem Direct-Sequence-Spread-Spectrum-Verfahren (DSSS) werden zwei Frequenzspreizverfahren auf der Grundlage elektromagnetischer Wellen im 2,4 GHz-ISM-Band beschrieben. Darüber hinaus wird auch eine Infrarot-Technologie vorgeschlagen, die allerdings nie praktische Anwendung gefunden hat und deswegen in diesem Buch nicht weiter dargestellt wird.

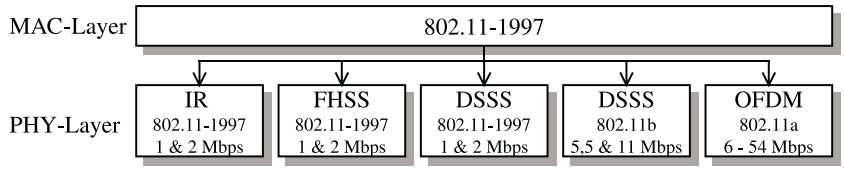


Abbildung 4.2: Zuordnung der Schichten zu den Standards des IEEE802.11

4.1.3 Erweiterungen

Im Jahr 1999 sind mit dem IEEE802.11a und dem IEEE802.11b zwei weitere Bestandteile hinzugefügt worden, die insbesondere das Ziel haben, höhere Bandbreiten zu erreichen. Dabei beschreiten beide grundsätzlich unterschiedliche Wege. Während der 802.11a einen weiteren Frequenzbereich im 5 GHz-Bereich nutzt, in dem größere Bandbreiten zur Verfügung stehen, nutzt der 802.11b weiterhin das 2,4 GHz-ISM-Band. Der 802.11b in der gegenwärtigen Fassung erreicht eine Bruttodatenrate von 11 Mbps und greift auf das DSSS-Verfahren zurück. Damit ist eine Einbeziehung des 802.11-DSSS-PHY verbunden, so dass auch Systeme nach 802.11-1997 mit Datenraten von 1 oder 2 Mbps angesprochen werden. WLAN-Systeme nach 802.11, die das FHSS-Verfahren einsetzen, können jedoch nicht eingebunden werden. Die Erweiterungen werden in Abschnitt 4.7 vorgestellt.

Beide Erweiterungen basieren auf dem gleichen MAC-Protokoll und ermöglichen somit auch identische Systemarchitekturen.

4.2 Architekturen

4.2.1 Systemarchitekturen

Der 802.11-Standard beschreibt die folgenden Betriebsarten, deren Hierarchie und Aufbau in Abbildung 4.3 und Abbildung 4.4 dargestellt sind.

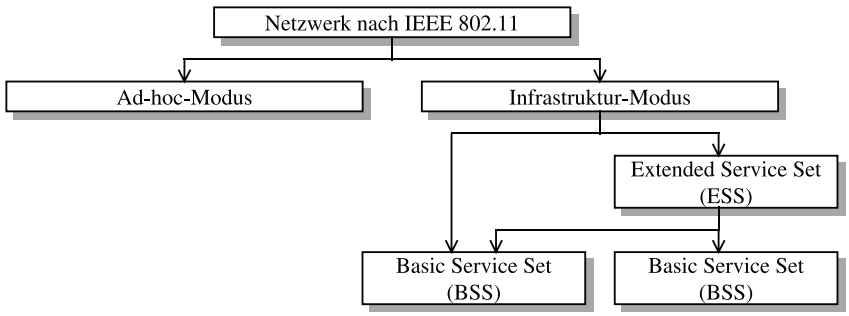
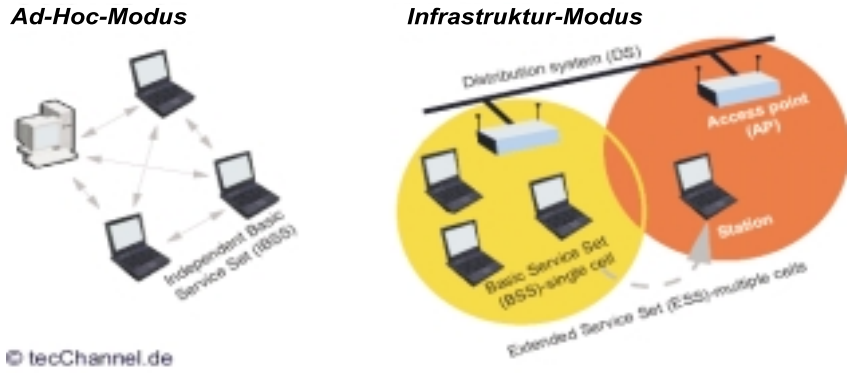


Abbildung 4.3: Gliederung der Betriebsarten im IEEE802.11

Abbildung 4.4: Architekturen der Betriebsarten im IEEE802.11



- Im *Ad-hoc-Modus* können Endgeräte in einem *Peer-to-Peer*-Netzwerk unmittelbar miteinander kommunizieren. In diesem ***I**ndependent **B**asic **S**ervice **S**et* (IBSS) können schnell, einfach und kostengünstig Netzwerke über meist kurze Entfernungen und mit einer begrenzten Anzahl von Teilnehmern ohne Integration in eine größere Netzwerkstruktur aufgebaut werden.
- Im *Infrastruktur-Modus* findet die Kommunikation grundsätzlich über einen Zugangspunkt statt. In dieser Betriebsart können auch Stationen außerhalb der direkten Reichweite kommunizieren. Die Anbindung an ein externes Netzwerk kann mit Hilfe eines Portals oder Gateways erfolgen.
  - In der einfachsten Version besteht ein solches Netzwerk aus einem Zugangspunkt und einer Gruppe von drahtlosen 802.11-Stationen im Funkbereich des Zugangspunkts. Ein solches Netzwerk wird als ***B**asic **S**ervice **S**et* (BSS) bezeichnet.
  - Werden zwei oder mehrere BSS in einem gemeinsamen Netzwerk betrieben, indem die Zugangspunkte über ein dahinter liegendes Netzwerk gekoppelt werden, so spricht man von einem ***E**xtended **S**ervice **S**et* (ESS). Das koppelnde Netzwerk bezeichnet der Standard als Verteilungssystem (***D**istribution **S**ystem* – DS). Dieses kann drahtgebunden oder auch mit Hilfe von Richtfunkstrecken implementiert werden. Im ESS-Modus muss insbesondere die Lokalisierung der Stationen in einem BSS und ein Wechsel der Stationen von einem BSS zu einem anderen unterstützt werden. Einen solchen Wechsel bezeichnet man als *Roaming*. Die hierzu notwendige Kommunikation der Zugangspunkte über das Verteilungsnetzwerk ist noch nicht Bestandteil des IEEE802.11-Standards (vgl. Abschnitt 4.7).

Im Infrastruktur-Modus müssen sich die Stationen beim Zugangspunkt anmelden (vgl. Abschnitt 4.3.7). Sie übertragen dann auf dem Kanal, der von dem Zugangspunkt verwendet und ihnen vorgegeben wird. Drei Hinweise erscheinen an dieser Stelle angebracht:

- Die Zuordnung kann vom Systemadministrator vorgegeben werden, um Zugriffsrechte zu verwalten und Benutzergruppen physisch zusammenzufassen.
- Es besteht aber auch die Möglichkeit einer Zuordnung. Insbesondere existieren dabei verschiedene herstellerspezifische Verfahren eines Load Balancing (vgl. Abschnitt 9.4.3). Auch kann im Rahmen des *Roaming* eine neue Zuordnung zum Beispiel durch die räumliche Veränderung der mobilen Station erfolgen, die zu einer Veränderung der Kanaleigenschaften führt.
- Die Bezeichnung des Ad-hoc-Modus im Rahmen des IEEE802.11-Standards unterscheidet sich von der in Abschnitt 1.3.10 gegebenen Definition von Ad-hoc-Networking. Denn auch im Infrastrukturmodus müssen die Zugangspunkte und die mobilen Stationen selbsttätig Informationen austauschen und den Anmeldevorgang durchführen. Also: Ad-hoc-Networking betreiben die IEEE802.11-Netze sowohl im Ad-hoc- als auch im Infrastrukturmodus.

4.2.2 Protokollarchitektur

Bei der Betrachtung der Protokollarchitektur des IEEE802.11 ist neben der auch in anderen Protokollen üblichen Aufteilung einer Ebene in einen *Sublayer* und einen *Management Layer* die weitere Aufteilung der Bitübertragungsschicht (*PHY-Layer*) hervorzuheben. In dieser Aufteilung übernimmt das ***P**hysical-**M**edium-**D**ependent*-Sublayer (PMD) die Modulation und Kodierung, während das ***P**hysical **L**ayer **C**onvergence **P**rotocol* (PLCP) medienunabhängig eine übliche PHY-Schnittstelle zur Verfügung stellt. Insbesondere liefert das PLCP auch das ***C**lear-**C**hannel-**A**ssignment*-Signal (CCA), das den aktuellen Zustand des Mediums anzeigt. Dieses CCA-Signal dient neben der Beobachtung der Signale, die von anderen Kommunikationsteilnehmern ausgesendet werden, auch der Vermeidung von Kollisionen mit Störungen durch Mikrowellenherde. Diese senden bei 50 Hz-Netzen und einer Aktivität von 50% Störsignale mit einer Dauer von 10 ms und einer Pause von 10 ms aus. Selbst wenn das Störsignal des Mikrowellenherds während der aktiven Phase sehr stark ist, stehen immer noch die 10 ms Pausenzeit für eine Übertragung des WLAN zur Verfügung [Solectek (2)].

Die Dienstzugangspunkte (***S**ervice **A**ccess **P**oints* - SAP) für den Signalfluss sind in Abbildung 4.5 dargestellt.

- Der MAC-SAP ist identisch mit den Dienstzugangspunkten der anderen Standards nach IEEE802.x, insbesondere auch mit dem Ethernet-Standard 802.3.
- Der PHY-SAP ist unabhängig von der Realisierung der physischen Übertragung.

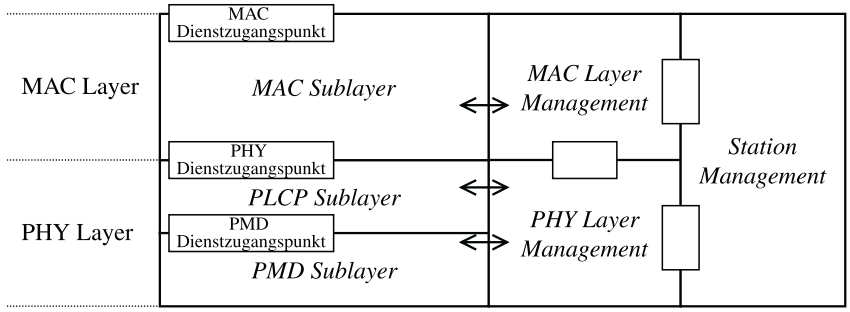


Abbildung 4.5: Die Dienstzugangspunkte der MAC- und PHY-Schichten im IEEE802.11

Eine weitere Besonderheit ergibt sich dadurch, dass auf beiden Ebenen die von den höheren Ebenen erhaltenen Daten mit einem zusätzlichen Rahmen verpackt werden. Die Rahmenformate werden in Abschnitt 4.3.6 besprochen.

4.3 Kanalzugriff

4.3.1 Einordnung

Die im 802.11-Standard beschriebene Kanalzugriffsschicht (MAC-Layer) ist recht eng mit den Vorgaben aus dem Ethernet-Standard 802.3 verwandt. Allerdings muss der drahtlose Standard auf die Besonderheiten der Übertragungsstrecke Rücksicht nehmen. Dabei ist insbesondere zu beachten, dass eine Überwachung einer Kollision, wie sie auf dem drahtgebundenen Übertragungsmedium durchgeführt werden kann, bei einer drahtlosen Übertragung nicht möglich ist (*Near/Far-Problem* – vgl. Abschnitt 2.10.2).

Der Zugriff erfolgt mit Hilfe von zwei Zugriffsmechanismen, der ***D**istributed **C**oordination **F**unction* (DCF) und der ***P**oint **C**oordination **F**unction* (PCF). Dabei greift die PCF auf die DCF zu, wie dies in Abbildung 4.6 gezeigt ist. Vor einer Erläuterung des Zusammenhangs zwischen diesen beiden Funktionen werden die beiden Algorithmen zunächst einzeln beschrieben.

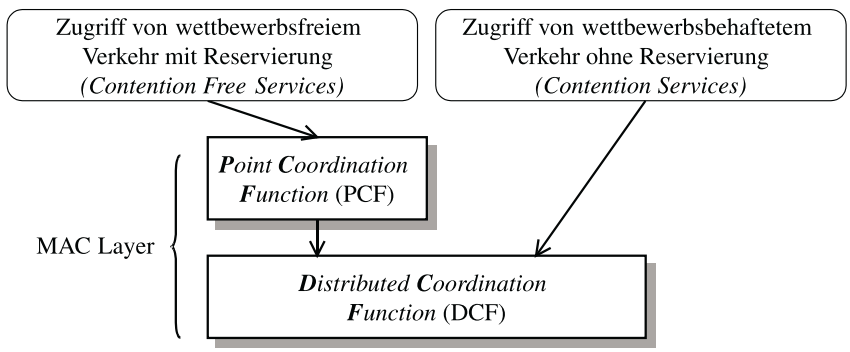


Abbildung 4.6: Zugriffe und Einordnung von PCF und DCF

4.3.2 Distributed Coordination Function

CSMA/CA

Die ***D**istributed **C**oordination **F**unction* (DCF) beschreibt die grundlegende Zugriffsmethode des IEEE802.11-Standards auf den Übertragungskanal. Sie folgt dem CSMA /CA-Algorithmus:

- ***M**ultiple **A**ccess* (MA) bedeutet, dass mehrere Kommunikationsteilnehmer einen gemeinsamen Übertragungskanal nutzen (*Shared Medium*).
- ***C**arrier **S**ense* (CS) bedeutet, dass jeder Kommunikationsteilnehmer den gemeinsamen Kanal überwacht und seine eigene Tätigkeit an den Zustand des Kanals anpasst. Insbesondere darf keine Station mit einer Übertragung beginnen, wenn der Kanal als belegt erkannt wird. Dabei unterscheidet man beim IEEE802.11-Standard ein physisches Abhören (*Physical Sensing*), bei dem anhand der gemessenen Feldstärke die Aktivität eines Kanals beurteilt wird, und ein virtuelles Abhören (*Virtual Sensing*). Hierbei kann eine Station im Rahmen spezieller Protokolle den Kanal für ein bestimmtes Zeitintervall reservieren, wie dies in den Abschnitten 4.3.3 und 4.3.5 erläutert wird.
- ***C**ollision **A**voidance* (CA) beschreibt die Algorithmen, die Kollisionen auf dem Kanal vermeiden sollen.

  In diesem Zusammenhang muss deutlich darauf hingewiesen werden, dass Vermeidung nicht gleichbedeutend ist mit einer Garantie, dass keine Kollisionen mehr auftreten. Denn es können gleichwohl bei 802.11-Netzen Kollisionen auftreten, die auch zu Datenverlust auf dem Übertragungskanal führen können. Analog zu dem Vorgehen bei drahtgebundenen Übertragungsmechanismen sind aber die Übertragungseinrichtungen dafür verantwortlich, die Daten so lange zu speichern, bis eine Übertragung erfolgreich durchgeführt wurde.

  Entsprechend können die Algorithmen am besten so verstanden werden, dass sie die Wahrscheinlichkeit von Kollisionen auf dem Kanal so weit wie möglich verringern sollen. Dennoch sollte dem Anwender klar sein, dass – ebenso wie im drahtgebundenen Ethernet – im normalen Betrieb Kollisionen durchaus häufig auftreten und keine Ausnahme darstellen.

Ein Kommunikationsteilnehmer muss also zunächst das Medium abhören, bevor er eine Übertragung beginnt (***L**isten **B**efore **T**alk* - LBT). Dabei sind zwei Fälle zu unterscheiden:

- Wenn das Medium während einer festgelegten Zeitdauer als frei erkannt wird, darf die Übertragung gestartet werden. Die Zeitdauer, die das Medium physisch abgehört wird, bezeichnet man als DIFS-Zeit. Die Bedeutung dieser Zeit wird im Folgenden dargestellt.
- Wird das Medium hingegen als belegt erkannt, weil gerade eine andere Station sendet, wird die Übertragung zurückgestellt und im Rahmen

eines Backoff-Prozesses um eine bestimmte Wartezeit verzögert, innerhalb der kein neuer Übertragungsversuch unternommen wird.

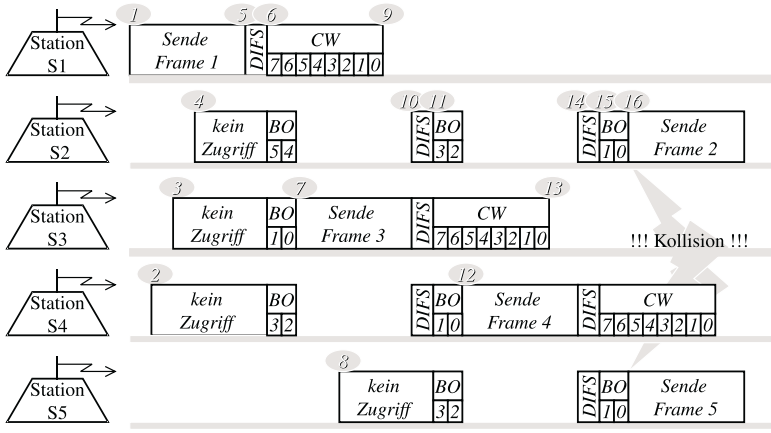
Diese Vorgehensweise stellt eine Abweichung vom Vorgehen des drahtgebundenen Ethernets dar, bei dem der Backoff-Algorithmus nur nach einer detektierten Kollision gestartet wird.

Backoff-Prozess

Die Bestimmung der Wartezeit erfolgt innerhalb des so genannten Backoff-Prozesses (engl. *to back off*: zurückdrehen). Hierzu wird zunächst eine gleichförmig zwischen Null und einem Maximum verteilte Pseudo-Zufallszahl bestimmt. Dieses Maximum bezeichnet man als ***C**ontention **W**indow* (CW) (engl. *contention*: 1. Streit, Zank 2. Streitpunkt 3. Behauptung, in diesem Zusammenhang jedoch vielleicht am besten mit Wettbewerb übertragbar, vgl. Abschnitt 4.3.5). Die Zufallszahl wird mit einer Zeitschlitzdauer multipliziert und bestimmt so die Dauer des Backoff-Zeitgebers. Die Dauer der Zeitschlitze ist abhängig von der Auswahl des physischen Übertragungsprotokolls. Die Basiswerte sind in Tabelle 4.5 und Tabelle 4.7 angegeben. Eine Besonderheit besteht darin, dass die verbleibende Wartezeit nicht reduziert wird, solange das Medium als belegt erkannt wird. Wenn das Medium frei wird, wartet der Kommunikationsteilnehmer eine DIFS-Zeit und erniedrigt dann periodisch den Backoff-Zeitgeber. Der volle Wert CW wird herabgezählt, nachdem eine Übertragung erfolgreich abgeschlossen wurde.

Dieser Backoff-Algorithmus soll vermeiden, dass nach der Beendigung der Übertragung durch eine Station mehrere andere wartende Stationen gleichzeitig die Übertragung beginnen. Dass aber dennoch eine Kollision auftreten kann, ist in Abbildung 4.7 dargestellt.

Der Wert von CW wird zunächst auf einen Ausgangswert CW_{Min} und bei jedem erfolglosen Übertragungsversuch auf den nächstgrößeren Wert in einer vorgegebenen Folge gesetzt. Kann eine Übertragung erfolgreich abgewickelt werden, wird der CW wieder auf CW_{Min} zurückgesetzt. Erreicht CW einen maximalen Wert CW_{Max}, verbleibt er dort so lange, bis er wieder zurückgesetzt wird. CW berechnet sich durch 2^n-1, wobei der Startwert von *n* von der Auswahl des physischen Übertragungsprotokolls abhängt (vgl. Abbildung 4.8)..



Darstellung ohne Berücksichtigung der Laufzeiten und ohne Empfangsbestätigungen (ACK)

Abbildung 4.7: Grundlegender Zugriff auf den Kanal bei der DCF im IEEE802.11

Erläuterung zu Abbildung 4.7

1. Station S1 beginnt mit der Übertragung eines ersten Rahmens *Frame 1*.
2. Die räumlich entfernte Station S4 detektiert zu einem späteren Zeitpunkt, dass der Kanal belegt ist, und verschiebt den eigenen Zugriff.
3. Die räumlich entfernte Station S3 detektiert zu einem späteren Zeitpunkt, dass der Kanal belegt ist, und verschiebt den eigenen Zugriff.
4. Die räumlich entfernte Station S2 detektiert zu einem späteren Zeitpunkt, dass der Kanal belegt ist, und verschiebt den eigenen Zugriff.
5. Nach dem erfolgreichen Abschluss der Übertragung von Frame 1 warten alle Stationen eine DIFS-Zeit ab.
6. Station S1 beginnt ein *Contention Window*; die anderen Stationen, die alle auf den Kanal zugreifen wollen, gehen in den *Backoff*-Modus. Die Startzahl des Backoff-Zählers wird innerhalb des Intervalls als Zufallszahl gewählt.
7. Der Backoff-Zähler von Station S3 erreicht als erster die 0 und beginnt mit der Übertragung seines Rahmens *Frame 3*.
8. Die räumlich entfernte Station S5 detektiert zu einem späteren Zeitpunkt, dass der Kanal belegt ist, und verschiebt den eigenen Zugriff.
9. Das *Contention Window* von Station S1 erreicht die 0. Da keine weiteren Daten zur Übertragung anstehen, hat dies keine Auswirkungen.
10. Nach dem erfolgreichen Abschluss der Übertragung von *Frame 3* warten alle aktiven Stationen eine DIFS-Zeit ab.
11. Station S3 beginnt ein *Contention Window*; die anderen Stationen, die alle auf den Kanal zugreifen wollen, gehen in den *Backoff*-Modus.
12. Der Backoff-Zähler von Station S4 erreicht als erster die 0 und beginnt mit der Übertragung seines Rahmens *Frame 4*.
13. Das *Contention Window* von Station S3 erreicht die 0. Da keine weiteren Daten zur Übertragung anstehen, hat dies keine Auswirkungen.
14. Nach dem erfolgreichen Abschluss der Übertragung von *Frame 4* warten alle aktiven Stationen eine DIFS-Zeit ab.
15. Station S4 beginnt ein *Contention Window*; die anderen Stationen, die alle auf den Kanal zugreifen wollen, gehen in den *Backoff*-Modus.
16. Die Backoff-Zähler der Stationen S2 und S5 erreichen gleichzeitig die 0 und beginnen mit der Übertragung der Rahmen *Frame 2* und *Frame 5*. Die elektromagnetischen Wellen überlagern sich – es tritt eine Kollision auf.

Übertragungsversuch	1	2	3	4	5	6	7
n	3	4	5	6	7	8	8
CW	7	15	31	63	127	255	255

CW_{min} CW_{max}

*Abbildung 4.8: Auswahl der Länge des **C**ontention **W**indow (CW) in Abhängigkeit von der Anzahl der bisher fehlgeschlagenen Übertragungsversuche*

Bestätigungsmechanismus

Es wird deutlich, dass dieser Algorithmus auf die Eigenschaften einer drahtlosen Übertragung abgestimmt ist.

- Zum einen können durchaus Kollisionen auftreten, die die Datenpakete beider sendenden Kommunikationsteilnehmer zerstören, wie das Szenario in Abbildung 4.9 zeigt.
- Zum anderen besteht in drahtlosen Übertragungssystemen keine Möglichkeit der Kollisionserkennung. Somit ist ein CSMA/CD-Algorithmus (*Carrier Sense Multiple Access - Collision Detection*) wie beim Ethernet nach 802.3 nicht möglich.

Deswegen wird bei der drahtlosen Übertragung nach 802.11 der ordnungsgemäße Empfang eines Rahmens quittiert. Die Versendung der Quittung (*Acknowledgement* – ACK) erfolgt nach einer Wartezeit, die man als *Short Interframe Space* (SIFS) bezeichnet.

Nun bleibt noch der Fall übrig, dass die Station S1 die Quittung nicht innerhalb eines festgelegten Zeitintervalls empfängt. Dies kann (mindestens) zwei Ursachen haben:

- Zum einen kann eine Kollision zweier Datenpakete aufgetreten sein, wie sie in Abbildung 4.7 beschrieben wurde.
- Zum anderen ist es auch nicht ausgeschlossen, dass der ACK-Rahmen zerstört wurde. Hierfür kann eine Kollision von zwei Paketen verantwortlich sein, die insbesondere dann auftreten kann, wenn die Summe aus SIFS und der maximalen Ausbreitungszeit in Hin- und Rückrichtung größer ist als die DIFS einer sendebereiten Station. Es ist aber ebenso eine Störung eines Pakets durch Reflexion möglich (vgl. Abschnitt 2.4.3).

Für den Fall, dass eine Station den Quittungsrahmen nicht rechtzeitig zurückerhält, bereitet sie eine erneute Übertragung vor, indem sie in den Backoff-Zustand übergeht. Bei der erneuten Übertragung wird mit Hilfe des *Retry*-Bits im Steuerfeld des Datenrahmens signalisiert, dass es sich um einen wiederholten Sendeversuch handelt (vgl. Abschnitt 4.3.6).

Abbildung 4.9 illustriert den Ablauf:

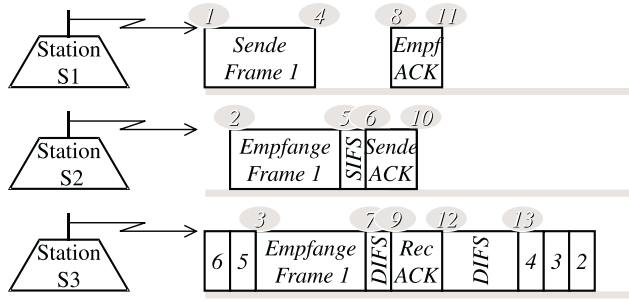


Abbildung 4.9: Ablauf eines erfolgreichen Kanalzugriffs mit Acknowledgement

Erläuterung zu Abbildung 4.9

1. Station 1 beginnt zu einem Zeitpunkt die Übertragung eines Rahmens *Frame 1*, der an Station S2 adressiert ist. Zu diesem Zeitpunkt befindet sich die Station S3 im Backoff-Prozess.
2. Station S2 beginnt mit dem ordnungsgemäßen Empfang von *Frame 1*.
3. Station S3 empfängt ebenfalls den Rahmen. Sobald das Medium als belegt erkannt wird, wird das Herunterzählen des Backoff-Zählers angehalten.
4. Station S1 beendet die Übertragung ihres Rahmens.
5. Station S2 erkennt das Medium wieder als frei. Da die Übertragung ordnungsgemäß abgeschlossen werden konnte, wird ein SIFS-Warteintervall begonnen, um eine Quittung zu versenden.
6. Nach Ablauf von SIFS versendet Station S2 den ACK-Rahmen.
7. Station S3 erkennt das Medium wieder als frei und beginnt ein DIFS-Warteintervall.
8. Station S1 empfängt den ACK-Rahmen.
9. Station S3 empfängt den ACK-Rahmen und stellt fest, dass das Medium belegt ist. Das noch nicht beendete DIFS-Warteintervall wird abgebrochen.
10. Station S2 beendet die Übertragung des ACK-Rahmens.
11. Station S1 beendet den Empfang des ACK-Rahmens.
12. Station S1 beendet den Empfang des ACK-Rahmens und beginnt ein neues DIFS-Warteintervall.
13. Nach dessen vollständigem Ablauf kann der Backoff-Zähler von Station S1 weiter dekrementiert werden.

Interframe Spaces

Eine zentrale Rolle bei der Funktionsweise des Zugriffsmechanismus spielt die Zeit zwischen zwei Rahmen, die als ***I**nter**f**rame **S**pace* (IFS) bezeichnet wird. Um die Belegung des Mediums zu ermitteln, muss ein Kommunikationsteilnehmer für die IFS-Zeit das Medium abhören. Dabei sind im Standard vier verschiedene IFS-Zeiten definiert, die drei unterschiedliche

Prioritätsstufen für den Kanalzugriff widerspiegeln. Dabei gilt: Je kürzer die IFS-Zeit ist, desto höher ist die Priorität.

So ist SIFS kürzer als DIFS, so dass die Bestätigung nicht die Wartezeiten der normalen Datenübermittlung einhalten muss. Die Quittungsrahmen erlangen durch die kürzere Wartezeit SIFS eine höhere Priorität als die normalen Datenpakete, die die längere DIFS-Zeit warten müssen.

Man unterscheidet vier Typen von IFS, die in Tabelle 4.1 dargestellt sind:

*Tab. 4.1: Die unterschiedlichen Längen der **I**nter**f**rame **S**paces (IFS) regeln die Priorität des Kanalzugriffs.*

		Funktion	Dauer
SIFS	Short IFS	ACK-Rahmen, CTS-Rahmen, PCF-Polling	abhängig von PHY-Auswahl
PIFS	PCF IFS	Wenn eine Station in der PCF zu Beginn der CFP mit Priorität Zugang zum Medium erhalten will	SIFS + SlotTime
DIFS	DCF IFS	Wartezeit im Rahmen der DCF	SIFS + 2 * SlotTime
EIFS	Extended IFS	verschiedene Funktionen	SIFS + DIFS + ACK-ControlFrame

4.3.3 RTS-CTS-Mechanismus

Das in den vorangegangenen Abschnitten beschriebene Verfahren funktioniert zuverlässig, solange alle Stationen mit jeweils allen anderen Stationen in Funkkontakt stehen. Ist dies jedoch nicht der Fall, dann kann eine der Stationen das Medium als frei erkennen, obwohl dies für die andere Station nicht zutrifft. Ein mögliches Szenario unter Berücksichtigung von solchen so genannten versteckten Stationen zeigt Abbildung 4.10. Station S1 kann von zwei anderen Stationen S2 und S3 Daten empfangen. Ein unmittelbarer Funkkontakt zwischen den Station S2 und S3 ist aber nicht möglich. Wenn Station S3 eine Nachricht an Station S2 sendet, erscheint das Medium für Station S2 als frei. Würde S1 nun ein Datenpaket an S2 übertragen, so würde S2 dieses nicht fehlerfrei empfangen können.

Zur Vermeidung solcher Situationen beinhaltet das 802.11-Protokoll den so genannten RTS-CTS-Mechanismus. Ein ***R**equest-**T**o-**S**end*-Rahmen (RTS) wird von der sendewilligen Station an den Empfänger geschickt und von diesem mit einem ***C**lear-**T**o-**S**end*-Rahmen (CTS) beantwortet. Falls der Sender den CTS-Rahmen erfolgreich empfängt, werden nach einer SIFS-Zeit die Daten übertragen. Für den Fall, dass der CTS-Rahmen nicht innerhalb einer festgelegten Zeitdauer empfangen wird, muss der RTS-Rahmen nach der Ausführung eines normalen *Backoff*-Zyklus erneut übertragen werden. Die Verwendung der SIFS-Zeit sichert der CTS-Antwort eine höhere Priorität gegenüber der normalen Datenübertragung.

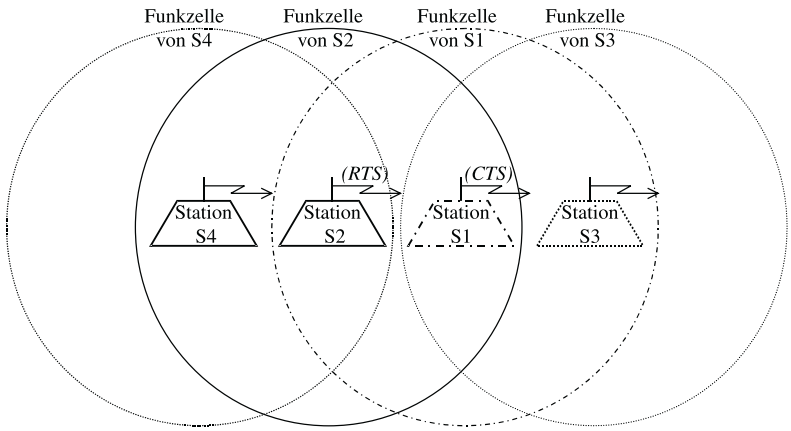


Abbildung 4.10: Die Konstellation von versteckten Stationen. Die Funkzellen der Stationen S3 und S4 überlappen nicht.

Auf zwei Sachverhalte muss in Zusammenhang mit dem RTS-CTS-Mechanismus hingewiesen werden:

- Die Implementierung des RTS-Mechanismus ist optional. Nichtsdestoweniger muss jedes Gerät nach 802.11 in der Lage sein, einen RTS-Rahmen innerhalb der geforderten Zeit mit dem zugehörigen CTS-Rahmen zu beantworten.
- Die RTS- und CTS-Rahmen enthalten ein Feld, das die Dauer für die Übertragung des Datenrahmens angibt. Diese Information wird von allen Stationen ausgewertet, die den RTS- oder den CTS-Rahmen empfangen können. In diesen Stationen wird ein Zeitgeber (***N**et **A**llocation **V**ector* - NAV) aktiviert, der im Gegensatz zum Backoff-Zähler unabhängig vom Zustand des Übertragungsmediums dekrementiert wird. Während der NAV-Zeit beginnen die jeweiligen Stationen keinen Übertragungsvorgang, um auf diese Weise die Wahrscheinlichkeit von Kollisionen wesentlich zu verringern. Man bezeichnet diese logische Blockierung des Kanalzugriffs auch als virtuelles Abhören (*Virtual Sensing*), weil gleichsam der NAV-Zähler abgehört wird.

  An dieser Stelle muss noch darauf hingewiesen werden, dass der NAV-Zähler nicht nur beim RTS-CTS-Mechanismus gesetzt wird, sondern durch das *Length*-Feld eines jeden Rahmens (vgl. Abschnitt 4.3.6).

In der Abbildung 4.10 kann die Station S4 den RTS-Rahmen und die Station S3 den CTS-Rahmen auswerten. Abbildung 4.11 zeigt das zugehörige Zeitdiagramm ohne Berücksichtigung der Signallaufzeiten auf dem Medium.

Der Mechanismus schützt also offensichtlich vor Kollisionen, nachdem die RTS- und CTS-Pakete störungsfrei übertragen wurden. Dieser Schutz muss aber mit zusätzlichem Protokollverkehr auf dem Kanal erkauft werden. Insbesondere bei kurzen Datenpaketen dieser Aufwand störend, so dass zur Optimierung des Ablaufs eine Länge des Datenpakets eingeführt wird, oberhalb der mit dem RTS-CTS-Mechanismus übertragen wird (*RTS threshold*).

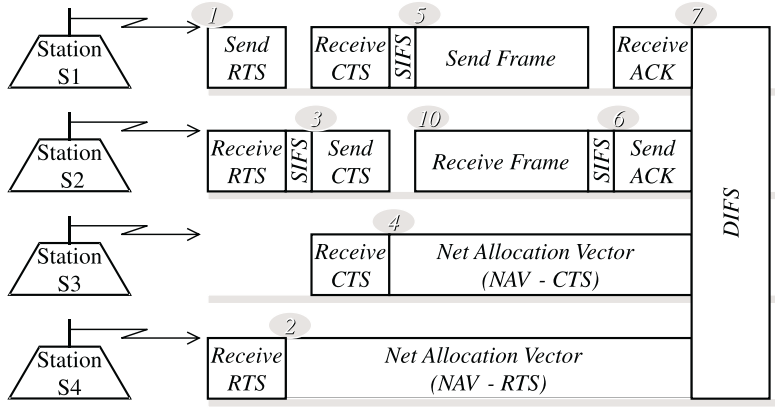


Abbildung 4.11: Ablauf eines Kanalzugriffs unter Nutzung des RTS-CTS-Mechanismus

Erläuterung zu Abbildung 4.11

1. Station 1 beginnt zu einem Zeitpunkt die Übertragung eines RTS-Rahmens, der an Station S2 adresssiert ist. Dieser Rahmen kann von Station S2 und S4 empfangen werden.
2. Nach Abschluss des ordnungsgemäßen Empfangs des RTS-Rahmens setzt Station S4 den NAV-Zeitgeber und »verhält sich ruhig«. Der NAV von Station S4 enthält die benötigte Zeit für CTS-, Daten- und ACK-Rahmen zuzüglich der jeweiligen SIFS-Intervalle.
3. Ein SIFS-Zeitintervall später sendet Station S2 den CTS-Rahmen. Dieser kann von den Stationen S1 und S3 empfangen werden.
4. Station S3 setzt ihren NAV-Zeitgeber auf die für die Übertragung des Daten- und des ACK-Rahmens benötigte Zeit, zuzüglich der dazwischen liegenden SIFS-Zeit, und »verhält sich ruhig«.
5. Station S1 überträgt nach dem erfolgreichen Empfang des CTS-Rahmens und eines SIFS-Intervalls den Datenrahmen.
6. Station S2 bestätigt den erfolgreichen Empfang nach einem SIFS-Intervall mit einem ACK-Rahmen.
7. Die Datenübertragung ist erfolgreich abgeschlossen, die NAV-Zeitgeber der beiden an der Kommunikation nicht beteiligten Stationen sind abgelaufen und nach Ablauf einer DIFS-Zeit kann eine neue Datenübertragung beginnen.

Der RTS-CTS-Mechanismus bewährt sich auch beim Betrieb überlappender BSS und IBSS.

4.3.4 Fragmentierung von langen Nachrichten

Längere Mitteilungen lassen sich in Fragmente zerlegen, um hierdurch die Wahrscheinlichkeit der fehlerfreien Übertragung jedes einzelnen Fragments zu erhöhen.

Dabei werden die zu einer Nachricht gehörenden Fragmente mit Hilfe des Sequenzkontrollfelds gekennzeichnet, das im Steuerrahmen übermittelt wird (vgl. Abschnitt 4.3.6). Zum einen wird eine Identifikationsnummer der Nachricht angegeben, zum anderen werden die einzelnen Rahmen durchnummeriert. Bei jedem Rahmen wird außerdem das *More Frag*-Bit gesetzt. Lediglich beim letzten Rahmen wird diese Kennzeichnung nicht vorgenommen. Der Ablauf ist in Abbildung 4.12 dargestellt.

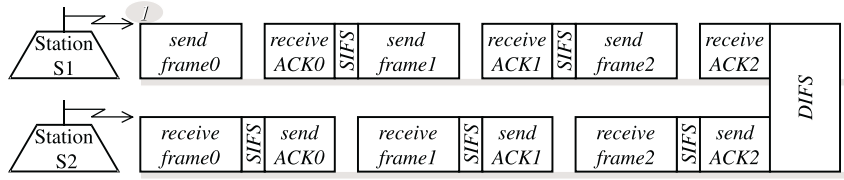


Abbildung 4.12: Fragmentierung von langen Nachrichten

Wenn es sich bei der Nachricht um keine Broadcast-Nachricht handelt, so sendet die empfangende Station eine Empfangsbestätigung zurück. Bevor andere Stationen nach dem Ablauf der DIFS auf den Kanal zugreifen können, darf die sendende Station bereits nach SIFS das folgende Fragment verschicken. Somit wird der fortlaufende Zugriff des Senders gewährleistet.

Für den Fall, dass die Übertragung entweder durch das Datenpaket oder die Empfangsbestätigung gestört wird, erhält die sendende Station keine Empfangsbestätigung. Dann wiederholt die sendende Station – wie in dem Basisprotokoll – die Übertragung, setzt allerdings das Bit *Retry* im Steuerrahmen (vgl. Abschnitt 4.3.6).

Auch die Reservierung des Kanals für fragmentierte Nachrichten ist möglich (vgl. Abbildung 4.13). Hierzu teilt die sendende Station in ihrem RTS-Paket die Dauer der Übertragung für das erste Fragment *Frame 0* mit, das in dem CTS-Paket der empfangenden Station repliziert wird. In dem *Frame 0* der sendenden Station wird nunmehr im Duration / ID Field des Headers die Verlängerung des NAV-Vektors für das folgende Fragment übertragen. Ebenso enthält das Duration / ID Field die Empfangsbestätigung für dieses Fragment, so dass alle Stationen im Empfangsbereich ihre Übertragungen auch für das nächste Fragment zurückstellen. Die Daten- und Bestätigungspakete können als virtuelle RTS- / CTS-Pakete angesehen werden. Beim letzten Fragment *Frame 2* enthält die Reservierung nur noch die Zeit für ein SIFS und Acknowledgement.

Der Wert *RTSthreshold*, ab dem ein Paket fragmentiert werden soll, kann vom Systemadministrator eingestellt werden. Dabei muss einerseits berücksichtigt werden, dass lange Pakete mit einer höheren Wahrscheinlichkeit von Bitfehlern während der Übertragung belastet sind, wobei im Fehlerfall die Übertragung wiederholt werden muss. Andererseits erhöht sich aber durch die Fragmentierung der Protokollaufwand, so dass hier für die jeweiligen Gegebenheiten des Funknetzes ein Optimum gefunden werden muss. Dies geschieht meist experimentell.

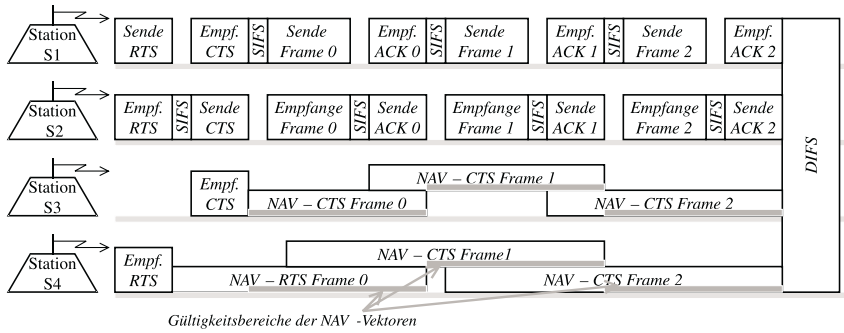


Abbildung 4.13: Fragmentierung von langen Nachrichten unter Nutzung des RTS-CTS-Algorithmus

4.3.5 Point Coordination Function

Um zeitkritische Dienste unterstützen zu können, wird die PCF definiert, um einem ***P**oint **C**oordinator* (PC) den priorisierten Zugriff auf das Übertragungsmedium zu ermöglichen. Normalerweise agiert ein AP mit einem Festnetzzugang als PC.

Obwohl PCF optional ist, müssen alle Stationen in der Lage sein, den Medienzugriffsregeln der PCF Folge zu leisten, da diese erstens auf der DCF basiert und zweitens das Prinzip sonst keine Wirkung zeigen würde. Stationen, die auf Anfragen des PC antworten können, werden *CF-Pollable* genannt. Nur diese Stationen können Daten entsprechend der PCF neben dem AP übertragen. Dabei ist zu berücksichtigen, dass in den meisten gegenwärtig am Markt verfügbaren Geräten die PCF aus Kostengründen nicht implementiert wird.

Die PCF steuert die Übertragung der Rahmen während einer wettbewerbsfreien Zeit (***C**ontention **F**ree **P**eriod* - CFP), die sich mit der durch die DCF gesteuerten Wettbewerbsperiode abwechselt (***C**ontention **P**eriod* - CP). Die CFP wird in regelmäßigen Zeitabständen mit der CFP-Rate wiederholt und startet mit der Übertragung eines Beacon-Rahmens (vgl. Abschnitt 4.3.6), der die maximale Dauer der CFP enthält. Alle Stationen im BSS mit Ausnahme des PC setzen ihren NAV auf diesen Wert, wie dies in Abbildung 4.14 dargestellt ist.

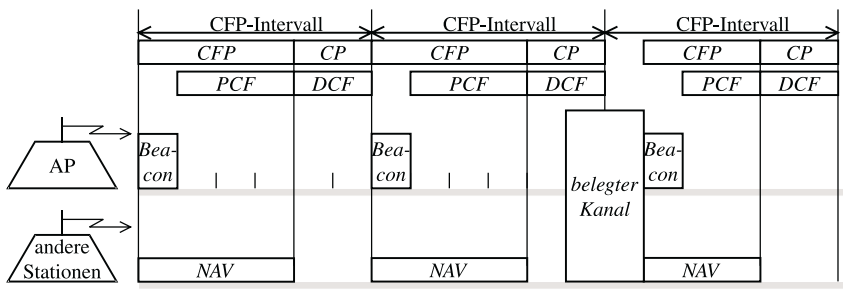


Abbildung 4.14: Reservierung des Kanals mit Hilfe der Point Coordination Function

Der PC übernimmt die Steuerung zu Beginn der CFP nach Ablauf der PCF IFS (PIFS), nachdem das Übertragungsmedium als frei erkannt wurde. Die PIFS ist länger als die SIFS, aber kürzer als die DIFS.

Dies bedeutet, dass die PCF eine höhere Priorität aufweist als die normale Übertragung, jedoch eine Quittierung, die nach SIFS übertragen wurde, abwarten muss. Der PC bleibt während der gesamten CFP steuernd tätig, er führt eine so genannte Polling List und fragt in der CFP alle Stationen auf dieser Liste der Reihe nach ab, ob sie eine Übertragung wünschen. Mit Hilfe dieser zentralen Zuteilung der Zugriffsrechte auf den Übertragungskanal können Kollisionen ausgeschlossen werden. Der PC identifiziert die Stationen dabei über einen *Association Identifier* (AID). Die Stationen können sich während der Anmeldung bei dem Zugangspunkt für die Polling-Liste eintragen lassen.

Einen möglichen Ablauf einer CFP zeigt Abbildung 4.14. Der PC darf dabei folgende Pakettypen in beliebigen Kombination an die CF-Pollable-Stationen senden:

- Daten an eine Station S_x. Wenn keine Daten für die Station vorliegen, kann dieser Bestandteil auch weggelassen werden.
- CF-Aufruf (CF-Poll) an eine Station S_x. Wenn die Station nicht aufgerufen werden soll, darf dieser Bestandteil auch weggelassen werden.
- CF-Bestätigung (CF-ACK) für die vorangehende Datenübertragung von der Station S_{x-1} an den PC. Wenn die Station S_{x-1} im vorangegangenen Zeitschlitz keine Daten übertragen hat, sendet der PC auch keine Empfangsbestätigung.
- Darüber hinaus dürfen auch Steuerrahmen versendet werden. Einer dieser Steuerrahmen ist das Signal CF-END, das den Abschluss der CFP signalisiert und bei den anderen beteiligten Stationen den NAV-Vektor zurücksetzt. Durch dieses vorzeitige Beenden der CFP kann die Reservierung des Kanals für die CP ohne Zeitverzug aufgehoben werden. CF-END darf mit CF-ACK kombiniert werden.

Die beteiligten Stationen dürfen im Wesentlichen zwei Pakettypen versenden, nachdem sie vom PC aufgerufen wurden:

- Daten an den PC.
- CF-Bestätigungen (CF-ACK) für die vom PC zusammen mit dem Aufruf erhaltenen Daten.
- Für den Fall, dass eine aufgerufene Station weder Daten vom PC erhält, noch Daten an den PC senden will, bestätigt sie den Aufruf mit einem Null-Rahmen.

Wenn eine Station auf einen Aufruf nicht antwortet, setzt der PC den Polling-Vorgang nach der PCF-IFS-Zeit mit der nächsten Station fort.

Problematisch erscheint die Abwicklung von PCF insbesondere in der Situation, wenn benachbarte Zugangspunkte, die auf dem gleichen Kanal arbeiten, ähnliche CFP-Intervalle besitzen. Um das Risiko von sich regelmäßig wiederholenden Kollisionen zu vermeiden, werden die Backoff-Zeiten des PC mit Hilfe von speziellen Zufallsalgorithmen eingestellt. Darüber hinaus kann der Beginn einer CFP verzögert werden, wenn eine andere Übertragung noch nicht abgeschlossen ist.

Die PCF bietet eine einfache und vergleichsweise effiziente Grundlage für die Implementierung von Protokollen für zeitkritische Dienste. Hierbei wird auch noch einmal die Beschränkung des 802.11-Standards auf die unteren beiden OSI-Layer deutlich, da die Gewährleistung einer Dienstgüte auf der dritten Ebene erfolgt.

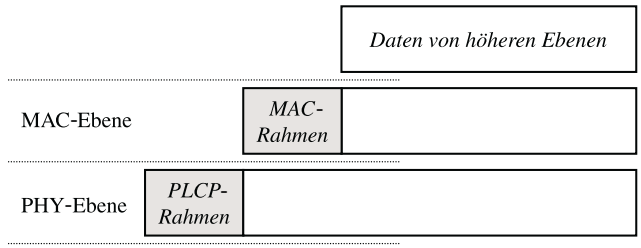
Einschränkend muss jedoch vermerkt werden, dass die konkrete Ausgestaltung der PCF im Standard offen bleibt. Insbesondere die Regeln, nach denen eine Polling-Liste abgearbeitet wird, oder das Verhalten nach einer Kollision während der CFP werden nicht beschrieben. Auch dass die Länge der CFP aufgrund vorangehender Übertragungen nicht unter allen Umständen eingehalten werden kann, stellt eine wesentliche Einschränkung für die zuverlässige Bereitstellung der Kanalkapazität für eine Anwendung dar.

4.3.6 Rahmenformate auf der MAC-Ebene

Allgemeine Rahmenformate

Bevor die Rahmenformate auf der MAC-Ebene besprochen werden, sei noch einmal auf die hierarchische Organisation eines Kommunikationsablaufs hingewiesen. Dies bedeutet für den Einsatz von IEEE802.11-konformen Geräten, dass sowohl auf der MAC- als auch auf der PHY-Ebene Rahmeninformationen hinzugefügt werden (vgl. Abbildung 4.15). Die MAC-Rahmen sind Gegenstand dieses Abschnitts. Die so genannten PLCP-Rahmen der PHY-Ebene werden in den Abschnitten 4.4.2 und 4.4.3 vorgestellt.

Abbildung 4.15: Hierarchischer Aufbau der Rahmen im IEEE802



Bei der Organisation des Kanalzugriffs werden drei unterschiedliche Rahmentypen eingesetzt: Daten-, Steuer- und Management-Rahmen. Das allgemeine Format eines Rahmens auf der MAC-Ebene, das auch dem Format des Datenrahmens entspricht, zeigt Abbildung 4.16 (1).

(1)

MAC Header							Daten	Prüf-summe
Steuer	Länge	Adresse 1	Adresse 2	Adresse 3	Sequenz-steuerung	Adresse 4		
2 Bytes	2 Bytes	6 Bytes	6 Bytes	2 Bytes	2 Bytes	6 Bytes	0 .. 2312 Bytes	4 Bytes

(2)

Version	Typ	Subtyp	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order
2 Bits	2 Bits	4 Bits	1 Bits	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit

(3)

00	01	10	11
Management-Rahmen	Steuer-Rahmen	Daten-Rahmen	reserviert
zur Verwaltung der Zellen	zur Regelung des Zugriffs auf das Medium und zur Sicherstellung einer zuverlässigen Übertragung (z.B. ACK-Rahmen)	zur Übertragung der Nutzdaten	

Abbildung 4.16: (1) Format des allgemeinen MAC-Rahmens; (2) Format des Steuerfelds eines Datenrahmens; (3) Mögliche Rahmentypen und ihre Kodierung

An dieser Stelle sei hervorgehoben, dass

- *Length:* die Länge des Rahmens angibt, um auf diese Weise den Kanal mit Hilfe der NAV-Vektoren zu reservieren.
- *Sequence:* die Nummerierung fragmentierter Nachrichten übernimmt.

Dabei weist das Steuerfeld im Falle eines Datenrahmens den in Abbildung 4.16 (2) angegebenen Aufbau auf. Die einzelnen Felder besitzen dabei folgende Bedeutung:

- *Version:* gibt die Version des IEEE802.11-Protokolls an. Gegenwärtig ist hier nur der Wert »00« erlaubt.
- *Typ:* gibt den Typ des Rahmens anhand der Kodierung aus Abbildung 4.16 (3) an.
- *Subtyp:* beschreibt die Bedeutung des Rahmens anhand der Kodierung aus Abbildung 4.17 in Abhängigkeit vom Typ des Rahmens.
- *To DS, From DS:* beschreibt den Übergang von Datenrahmen zwischen einer Zelle und dem Verteilungssystem (***D**istribution **S**ystem* – DS) in Zusammenhang mit den Adressfeldern, wie dies in Abbildung 4.18 dargestellt ist. Dabei entspricht die Adresse der Zelle der MAC-Adresse der Funkseite des Zugangspunkts
- *More Frag:* wird auf »1« gesetzt, wenn bei fragmentierten Nachrichten noch weitere Rahmen folgen, die zur selben Nachricht gehören. Handelt es sich um den letzten Rahmen einer fragmentierten Nachricht oder um den einzigen Rahmen einer nicht fragmentierten Nachricht, dann trägt das Bit den Wert »0«.
- *Retry:* wird auf »1« gesetzt, wenn ein Rahmen erneut gesendet wird.

Abbildung 4.17: Mögliche Subtypen und ihre Kodierung

Sub-typ-Wert	Daten-Rahmen	Steuer-Rahmen	Management-Rahmen
0000	Daten		Association Request
0001	Daten + CF-ACK		Association Response
0010	Daten + CF-Poll		Reassociation Request
0011	Daten + CF-Ack + CF-Poll		Reassociation Response
0100	Null		Probe Request
0101	CF-Ack		Probe Response
0110	CF-Poll		
0111	CF-Ack + CF-Poll		
1000			Beacon
1001			ATIM (Power Save)
1010		Power Save (PS) Poll	Deassociation
1011		RTS (Request-To-Send)	Authentification
1100		CTS (Clear-To-Send)	De-Authentification
1101		ACK (Acknowledgement)	
1110		CF-End	
1111		CF-End + CF-Ack	

- *Pwr Mgmt, More Data:* werden zur Verwaltung der Stromsparmodi eingesetzt.
- *WEP:* Wenn das WEP-Bit auf »1« gesetzt wird, wird der Datenteil des Rahmens mittels des Wired-Equivalent-Privacy-Algorithmus verschlüsselt übertragen (siehe Abschnitt 4.6).
- *Order:* Dieses Bit gibt die optionale Funktionalität an, dass der Rahmen in der richtigen Reihenfolge von Nachrichten an die oberen Schichten weitergereicht werden soll..

Abbildung 4.18: Mögliche Übergänge zwischen Zelle und Verteilungssystem und ihre Kodierung

To DS	0	0	1	1
From DS	0	1	0	1
Adresse 1	Empfänger	Empfänger	Zelle des Senders	Zelle des Empfängers
Adresse 2	Sender	Zelle des Empfängers	Sender	Zelle des Senders
Adresse 3	Zelle	Sender	Empfänger	Empfänger
Adresse 4	-	-	-	Sender
Erläuterung	Der Rahmen wird nur innerhalb einer Zelle versendet. Dies gilt für alle Steuer- und Management-Rahmen.	Der Rahmen wird von dem Zugangspunkt aus dem Verteilungssystem an eine Station in der Zelle geschickt.	Der Rahmen wird von einer Station aus einer Zelle an den Zugangspunkt zur Weiterleitung in das Verteilungssystem versendet.	Der Rahmen wird von einer Station in einer Zelle über den eigenen Zugangspunkt an eine Station in einer anderen Zelle versendet.

Datenrahmen

Das Format von Datenrahmen folgt den oben genannten allgemeinen Angaben.

Steuerrahmen

Die Untertypen für die Steuerrahmen sind ebenfalls in Abbildung 4.17 angegeben. Das Rahmenformat von Steuerrahmen ist abhängig vom jeweiligen Untertypen. Jedoch haben alle Steuerrahmen den gleichen Aufbau des Steuerfeldes im Header (vgl. Abbildung 4.19). Steuerrahmen werden nur innerhalb einer Zelle verschickt und sie werden nicht verschlüsselt.

Version	Steuer-rahmen	Subtyp	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order
Version	Typ	Subtyp	0	0	0	0	Pwr Mgmt	0	0	0
2 Bits	2 Bits	4 Bits	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit

Abbildung 4.19: Format des Steuerfelds von Steuerrahmen

Managementrahmen

Das in Abbildung 4.20 gezeigte Rahmenformat der Managementrahmen ist unabhängig vom Subtypen, der in Abbildung 4.17 angegeben ist. Insbesondere gehören die Beacon-Rahmen (engl. *Beacon*: Leuchtfeuer, Signalfeuer) zu den Managementrahmen.

MAC Header						Daten	Prüf-summe
Steuer	Länge	Emp-fänger	Sender	Zelle	Sequenz-steuerung		
2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	0 .. 2312 Bytes	4 Bytes

Abbildung 4.20: Format von Management-rahmen

Abschließend sei angemerkt, dass die hier beschriebenen Steuerinformationen

- nur einen Teil der gesamten im Standard vorgegebenen Konfigurationen umfassen.
- durch zahlreiche weitere proprietäre Erweiterungen ergänzt werden, die in den meisten Fällen auch nicht offengelegt sind.

4.3.7 Verwaltung von Stationen

In diesem Abschnitt finden insbesondere zwei Aspekte Berücksichtigung:

- Die Zuordnung der mobilen Stationen zur Zelle eines Zugangspunkts. Dabei muss noch darauf hingewiesen werden, dass im IEEE802.11-Standard der Begriff der Zelle in der Bedeutung der in Abschnitt 2.4.3 definierten Kanalzelle verwendet wird.
- Der Aufbau von Ad-hoc-Netzwerken.

Die Verwaltung von Stationen im Sinne des in Abschnitt 1.3.10 beschriebenen Ad-hoc-Networking umfasst die folgenden drei Schritte:

- Identifikation von Stationen,
- Authentifizierung und
- Anmeldung.

Die Verwaltung von Stationen im Sinne ihrer Adressierung und Identifizierung findet sich in Abschnitt 4.3.8.

Beacon-Rahmen

Die Beacon-Rahmen stellen Management-Rahmen dar (vgl. Abschnitt 4.3.6), die in einer Zelle in periodischen Zeitintervallen per Broadcast an alle Teilnehmer einer Zelle versendet werden und grundlegende Informationen über die Zelle enthalten. Diese sind in Abbildung 4.21 aufgeführt.

Abbildung 4.21: Format von Beacon-Rahmen

Information	*Länge*	*Bedeutung*		
Timestamp	*8 Bytes*	*Uhrzeit des Senders zur Synchronisation der Uhren aller Stationen in einer Zelle*		
Beacon-Intervall	*2 Bytes*	*Die Zeitdauer zwischen zwei Beacons. Zusammen mit der Uhrzeit kann jede Station den Startzeitpunkt des nächsten Beacon errechnen, den man als Target Beacon Transmission Time (TBTT) bezeichnet. Auf diese Weise kann eine Station auch das Ausbleiben eines Beacon erkennen.*		
Capability	*8 Bytes*	*Informationen zur Zelle: Adhoc oder Infrastruktur, CFP -unterstützt, Verschlüsselung*		
Address	*6 Bytes*	*Adresse der Zelle: In einem Infrastruktur-Netzwerk entspricht die Adresse der Zelle der MAC-Adresse des Zugangspunkts*		
Data Rate	*3 - 8 Bytes*			
FH Parameter	*7 Bytes*	*DS Parameter*	*7 Bytes*	*Alternative Übermittlung der Eigenschaften der PHY-Ebene: Kanalwahl*
CF Parameter	*8 Bytes*	*Falls der Zugangspunkt die PCF implementiert, dann werden hier Angaben wie die Startzeit der nächsten CFP, die maximale Dauer d er CFP, die Restdauer der laufenden CFP übermittelt.*		
TIM	*4 Bytes*	*Transmission Indication Map zur Steuerung der Stromsparmodi*		

Beacon-Rahmen werden in Infrastruktur-Netzwerken von den Zugangspunkten versendet. In Ad-hoc-Netzwerken kann jede Station zur nächsten TBTT (***T**arget **B**eacon **T**ransmission **T**ime*) einen Beacon-Rahmen versenden.

Damit dies nicht mehrere Stationen gleichzeitig tun, wird wieder ein Algorithmus zur Kollisionsvermeidung eingesetzt, indem jede Station zur nächsten TBTT einen Timer mit einer Zufallszahl lädt und den Beacon-Rahmen nur dann sendet, wenn der Timer abgelaufen ist und bis zu diesem Zeitpunkt noch kein Beacon-Rahmen von einer anderen Station empfangen wurde.

Wird ein Zugangspunkt eingeschaltet, so beginnt er mit der Versendung von Beacon-Rahmen in den festgesetzten Zeitabständen. Eine Station, die kein AP ist, kann also durch die Überwachung aller physischen Kanäle herausfinden,

von welchen Zellen sie Signale empfangen kann. Diesen Vorgang bezeichnet man als *Passives Scanning*. Dabei kann eine Station durchaus Beacon-Rahmen von mehreren Zugangspunkten erhalten, wenn sie sich im Bereich überlappender Zellen befindet. Die Station kann aufgrund der Signalstärke des Beacons entscheiden, bei welcher Zelle sie sich anmelden möchte. Ist die Station so konfiguriert, dass sie sich nur bei einer bestimmten Zelle anmelden darf, so schränkt dies natürlich die Auswahl der Funkzelle ein.

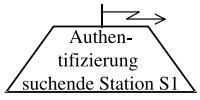
Darüber hinaus kann eine Station auch so konfiguriert werden (vgl. Abschnitt 9.2.3), dass sie eine neue Zelle als Ad-hoc-Netzwerk startet, nachdem sie eine bestimmte, einstellbare Zeit auf den Empfang eines Beacon-Rahmens für ein Ad-hoc-Netzwerk gewartet hat.

Stationen können aber auch *Aktives Scanning* betreiben. Hierzu werden Management-Rahmen per Broadcast mit dem Subtype *Probe Request* versendet. Im Datenteil des Rahmens ist entweder lediglich angegeben, dass die Station eine beliebige Zelle sucht, oder es ist die Adresse der gesuchten Zelle hinterlegt. Empfängt ein AP einen solchen Rahmen, antwortet es mit einem Management-Rahmen – mit dem Subtype *Probe Response* mit den Informationen über seine Zelle. In einem Ad-hoc-Netzwerk antwortet diejenige Station, die als Letzte für die Zelle einen Beacon-Rahmen erzeugt hat.

Authentifizierung

Unter Authentifizierung versteht man den Identitätsnachweis einer Station gegenüber einer anderen Station. Der IEEE802.11-Standard unterscheidet zwei Arten von Authentifizierung:

- Die offene Authentifizierung folgt einem sehr einfachen Algorithmus, der die Authentifizierung nur formal erfüllt. Die in Abbildung 4.22 dargestellte offene Authentifizierung ist das standardmäßig implementierte Verfahren.



Rahmen 1	
Message-Type	*Management*
Message-Subtype	*Authentication*
Information	*Authentication Algorithm Identification = „Open System“*
	Station Identify Assertion (in SA field of header)
	Authentication Transaction Sequence Number = „1“
	Authentication Algorithm Dependant Information = None



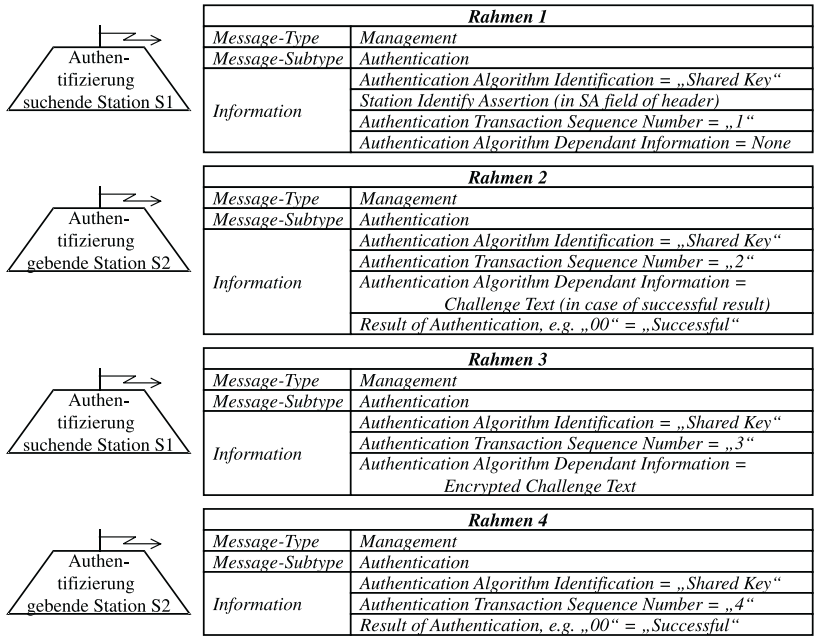
Rahmen 2	
Message-Type	*Management*
Message-Subtype	*Authentication*
Information	*Authentication Algorithm Identification = „Open System“*
	Authentication Transaction Sequence Number = „2“
	Authentication Algorithm Dependant Information = None
	Result of Authentication, e.g. „00“ = „Successful“

Abbildung 4.22: Offene Authentifizierung von Stationen

- Die Authentifizierung durch gemeinsame Schlüssel (*Shared Key Authentication*) setzt auf der verschlüsselten Kommunikation mit Hilfe des WEP-Algorithmus auf. Er beruht auf der Überprüfung, ob die beiden beteiligten Stationen denselben geheimen Schlüssel aufweisen.

Dies wird dadurch erreicht, dass die Authentifizierung gebende Station S2 der Authentifizierung suchenden Station S1 einen Text übergibt (*Challenge Text*), den diese verschlüsselt zurücksendet. Nur wenn die Verschlüsselung korrekt war, erhält diese die Nachricht der erfolgreichen Authentifizierung zurück (vgl. Abbildung 4.23).

Abbildung 4.23: Authentifizierung von Stationen durch gemeinsame Schlüssel



Anmeldung

Grundlegend für die Funktionsweise von Infrastrukturnetzen ist die Zuordnung der Stationen zu den jeweiligen Zellen. Dabei muss für jede Station eine eindeutige Entscheidung möglich sein, zu welcher Zelle sie gehört, um Daten in das Verteilungssystem zu schicken. Eine solche Zuordnung kann mit Hilfe der ESSID erfolgen. In vielen Fällen werden aber auch herstellerspezifische Steuerinformationen eingesetzt.

Auf der anderen Seite muss einem Zugangspunkt bekannt sein, welche Stationen sich als zu seiner Zelle gehörend betrachten. Diese Zuordnung erfolgt über eine explizite Anmeldung (*Association*), wie sie in Abbildung 4.24 dargestellt ist.

Anmeldung und Authentifizierung bilden zusammen ein zweistufiges Zuordnungssystem:

- Eine Station kann sich nur anmelden, wenn sie authentifiziert ist.
- Eine Station kann das Verteilungssystem nur dann nutzen, wenn sie bei einer Zelle angemeldet ist.

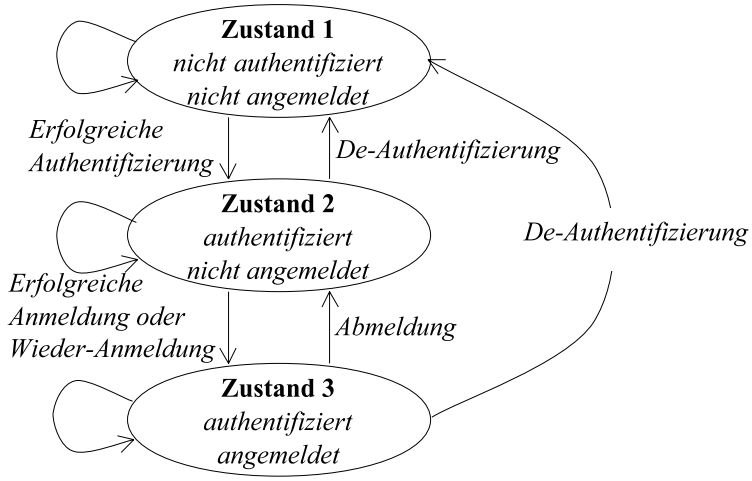


Abbildung 4.24: Algorithmus einer expliziten Anmeldung

Zusätzlich schreibt der IEEE802.11-Standard anhand der in Abbildung 4.25 gezeigten Klassifizierung vor, welche Rahmen in welchem der drei Zustände von den Stationen gesendet oder empfangen werden dürfen, um auf diese Weise den zweistufigen Aufbau umzusetzen. Zu beachten ist dabei, dass im nicht authentifizierten und nicht angemeldeten Zustand 1 Datenrahmen innerhalb einer Zelle gesendet und auch empfangen werden dürfen.

Klasse	Daten-Rahmen	Steuer-Rahmen	Management-Rahmen	Zustand 1	Zustand 2	Zustand 3
1	alle innerhalb der Zelle (ToDS = FromDS = 0)	alle außer PS-Poll	alle außer •Association Request/Response •Re-Association Request/Response, •Disassociation	erlaubt	erlaubt	erlaubt
2	-	-	alle übrigen, also •Association Request/Response •Re-Association Request/Response, •Disassociation	nicht erlaubt	erlaubt	erlaubt
3	alle Daten-Rahmen, bei denen die Bits ToDS oder FromDS gesetzt sind	PS-Poll	-	nicht erlaubt	nicht erlaubt	erlaubt

Abbildung 4.25: Klassifizierung der Rechte in Abhängigkeit vom Anmeldezustand

4.3.8 Adressierung von Stationen

Bei der Adressierung im Rahmen von IEEE802.11-Netzwerken sind mit der Adressierung auf MAC-Ebene und der Identifizierung auf Netzwerkebene zwei Aspekte zu unterscheiden, die jedoch auch miteinander verbunden sind.

Auf der MAC-Ebene verwendet IEEE802.11 Adressen, die den MAC-Adressen des IEEE802.3-Ethernet-Standards entsprechen. Auch aus diesem Grund ist die Einbindung in die bestehenden Betriebssysteme vergleichsweise einfach. Allerdings muss noch auf einen Aspekt hingewiesen werden, der von Zeit zu Zeit zu Verwirrung führt. Die Stationen in Funknetzen, die Brückenfunktionen erfüllen, weisen mindestens zwei Netzwerkanschlüsse auf. Dies gilt beispielsweise für die Zugangspunkte. Diese sind auf der einen Seite an das drahtgebundene Verteilungssystem (*Distribution System*) angeschlossen sind und verfügen dort über eine MAC-Adresse für das IEEE802.3-Netzwerk. Auf der anderen Seite wird auch dem Funkmodul eine MAC-Adresse zugewiesen. Wenn in Abbildung 4.17 die Adressen von Zugangspunkten aufgeführt sind, so handelt es sich hierbei grundsätzlich um die Adressen der Funkmodule.

Auf der Netzwerkebene wird zusätzlich eine Identifikation durchgeführt. Dabei sind zwei Identifikationsebenen zu unterscheiden:

- Für die Identifikation eines ***B**asic **S**ervice **S**et* (BSS) wird eine BSSID eindeutig zugewiesen. Bei einem drahtgebundenen BSS wird die MAC-Adresse des Zugangspunkts gewählt, der den Dienst für das BSS erbringt. Für ein unabhängiges BSS (***I**ndependent **BSS*** - IBSS) wird die BSSID zufällig gebildet.
- Auf der zweiten Ebene wird vom Systemadministrator eine ***E**lectronic **Sys**tem **ID*** (SSID oder ESSID) in allen mobilen Teilnehmern und allen Zugangspunkten eingetragen, die zu einer Domäne gehören sollen. Diese SSID bildet auch ein Element der Zugangsbeschränkung (vgl. Abschnitt 4.6).

4.4 Bitübertragung

4.4.1 Einordnung

Auf der Bitübertragungsschicht ergeben sich naturgemäß die größten Unterschiede zur drahtgebundenen Kommunikation, da ja nunmehr auf elektromagnetische Wellen als Übertragungsmedium über die Luftschnittstelle zurückgegriffen wird. Bei der Spezifikation des physischen Übertragungsprotokolls müssen die Eigenschaften der Übertragung über die Luftschnittstelle – und hierbei insbesondere Störungen – berücksichtigt werden.

Während in den frühen IEEE802.11-kompatiblen Produkten vorwiegend das FHSS-Verfahren Anwendung gefunden hat, setzt sich das DSSS-Verfahren zunehmend durch. Die maßgebliche Begründung hierfür besteht darin, dass die Erweiterung IEEE802.11b und die damit erreichbare Datenrate von 11 Mbps nur mit dem DSSS-Verfahren erreicht wird. Dabei bleiben die Systeme auf eine einfache Weise abwärtskompatibel zu den langsamen Geschwindigkeiten.

4.4.2 Frequency Hopping Spread Spectrum

In dem FHSS-Standard nach IEEE802.11 sind bis zu 79 nichtüberlappende Frequenzbereiche mit einer Bandbreite von jeweils 1 MHz vorgesehen, wobei 3 Gruppen mit je 26 Mustern zusammengefasst werden. Die Abfolge der Frequenzen wird aus einer Basisfolge berechnet, die einer Pseudozufallskette im Intervall von 0 bis 78 entspricht.

Die Basisfolge b(i) wird beispielsweise für Nordamerika und Europa durch die in Tabelle 4.2 gezeigten Werte vorgegeben:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
b(i)	0	23	62	8	43	16	71	47	19	61	76	29	59	22	52	63	26	77	31	2
i	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
b(i)	18	11	36	71	54	69	21	3	37	10	34	66	7	68	75	4	60	27	12	25
i	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
b(i)	14	57	41	74	32	70	9	58	78	45	20	73	64	39	13	33	65	50	56	42
i	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	-
b(i)	48	15	5	17	6	67	49	40	1	28	55	35	53	24	44	51	38	30	46	-

Tab. 4.2: Basisfolgen für FHSS nach 802.11 in Nordamerika und Europa

Die Übertragungsfrequenz des mit Hilfe der Berechnungsvorschrift aus Tabelle 4.3 aus dieser Basisfolge abgeleiteten Musters berechnet sich zu:

$F_x(i) = 2400 + f_x(i)$ [GHz]

Region	freigegebenes Frequenzband	Sprung-frequenzen	Kanäle	Berechnung der Kanalnummer
USA	2,4000 - 2,4835 GHz	2,402 - 2,480 GHz	2 .. 80	[b(i) + x] mod 79 + 2
Europa	2,4000 - 2,4835 GHz	2,402 - 2,480 GHz	2 .. 80	[b(i) + x] mod 79 + 2
Japan	2,4710 - 2,4970 GHz	2,473 - 2,495 GHz	73 .. 95	[(i - 1) * x] mod 23 + 73
Spanien	2,4465 - 2,4835 GHz	2,447 - 2,473 GHz	47 .. 73	[b(i) + x] mod 27 + 47
Frankreich	2,4450 - 2,4750 GHz	2,448 - 2,482 GHz	48 .. 82	[b(i) + x] mod 35 + 48

Tab. 4.3: Zuordnung der Frequenzsprung-sequenzen

Hierzu wird zusätzlich der Offset *x* des Kanalmusters benötigt, der für Nordamerika und Europa in die in Tabelle 4.4 aufgeführten drei Gruppen aufgeteilt ist:

Tab. 4.4: Zuordnung der Kanalmuster für Nordamerika und Europa

Set 1	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75
Set 2	1	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61	64	67	70	73	76
Set 3	2	5	8	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77

In den Regionen mit eingeschränkter Breite des ISM-Bands wird die Anzahl der Frequenzbereiche reduziert (vgl. Tabelle 4.3), wodurch sich die mögliche Dichte von Geräten verringert. Für die Berechnung der Basisfolgen und der Kanalmuster stehen entsprechend reduzierte Vorlagen zur Verfügung.

*Abbildung 4.26: Rahmenformat des **P**hysical **L**ayer **C**onvergence **P**rocedure-Rahmens (PLCP) für das FHSS-Verfahren im IEEE802.11*

PPDU					
PLCP Protocol Data Unit					
PLCP-Präambel		***PLCP Header***			***MPDU***
Synchronisation	*Start Frame Delimiter*	*MPDU Length Word*	*PLCP Signaling Field*	*Header Error Check*	*MAC Protocol Data Unit*
SYNC	***SFD***	***PLW***	***PSF***	***HEC***	*0 .. 4095 Bytes*
80 Bits	*16 Bits*	*12 Bits*	*4 Bits*	*16 Bits*	
besteht aus abwechselnden Nullen und Einsen; dient dem Empfänger der Erkennung eines ankommenden Signals und der Synchronisation	*feststehendes Bitmuster, das den Anfang des eigentlichen Frames kennzeichnet*	*spezifiziert die Länge des MPDU in Byte; maximale Länge: 2^{12}-1 = 4095 Bytes*	*spezifiziert die Datenrate, mit der das MPDU gesendet wird*	*Fehlerüberprüfung für den PLCP Header mittels 16b CRC*	*Nutzdaten*

Das Rahmenformat der FHSS-Übertragungsstrecke ist in Abbildung 4.26 gezeigt. Es ist hervorzuheben, dass Präambel und Header grundsätzlich mit einer Datenrate von 1 Mbps übertragen werden, während die Datenpakete mit 1 oder 2 Mbps gesendet werden können. Dabei ist die Betriebsart mit 1 Mbps für alle Geräte im ursprünglichen 802.11-Standard von 1997 vorgeschrieben. Die Übertragung mit 2 Mbps ist eine spätere Erweiterung und optional. Die Erhöhung der Datenrate wird durch ein *Multilevel-Signaling* der GFSK-Modulation (***G**aussian **P**hase **S**hift **K**eying*) erreicht, wobei die Symbolgeschwindigkeit mit 1 MBaud konstant gehalten wird.

Bei der Übertragung mit 1 Mbps wird ein Bit pro Symbol übertragen, während bei der Übertragung mit 2 Mbps zwei Bits in einem Symbol zusammengefasst werden (siehe Abbildung 4.27).

Als grundlegende Parameter wurden für den FHSS-Standard die in Tabelle 4.5 genannten Größen festgelegt.

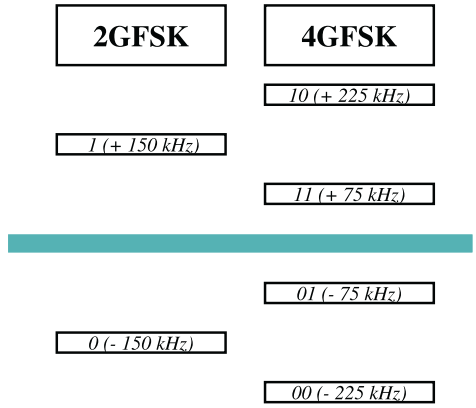


Abbildung 4.27: 2GFSK-Modulation bei IEEE802.11-FHSS

Größe	Wert
AslotTime	50 μs
ASIFSTime	28 μs
AMPDUMaxLength	4095 Byte

Tab. 4.5: Grundlegende Parameter der FHSS-Übertragung im 802.11-Standard

4.4.3 Direct Sequence Spread Spectrum

Beim DSSS-Verfahren findet eine Frequenzspreizung durch die logische Verknüpfung mit einer höherbitratigen Pseudo-Noise-(PN-)Sequenz statt. Für DSSS-Systeme nach dem 802.11-Standard für Datenraten von 1 und 2 Mbps wird der 1-Chip lange Barker-Code genutzt. Dieser weist besonders gute Autokorrelationseigenschaften auf, wobei seine Länge der in den Freigaberichtlinien der Aufsichtsbehörden festgelegten Mindestlänge für einen Spreizcode entspricht.

Das DSSS-Verfahren nach IEEE802.11 nutzt für alle Kanäle den gleichen Code. Das CDMA-Verfahren dient also lediglich der Abgrenzung von anderen Übertragungen im 2,4 GHz-ISM-Band und nicht der Unterscheidung von gleichzeitig in anderen Kanälen betriebenen Stationen in der gleichen Funkzelle. Der wesentliche Grund hierfür ist darin zu suchen, dass die Länge der Spreizcodes und damit der Prozessgewinn (***P**rocessing **G**ain* – GP) zu gering ist, um verschiedene Codes zu unterscheiden. Damit unterscheidet sich der 802.11-Standard wesentlich von anderen CDMA-Systemen, wie sie im Bereich der Mobilkommunikation eingesetzt werden und bei denen auch die Trennung der verschiedenen Kanäle durch unterschiedliche PN-Codes erreicht wird. Die unterschiedlichen Kanäle mehrerer 802.11-Systeme unterscheiden sich durch verschiedene Trägerfrequenzen im Sinne eines FDMA-Verfahrens. Dabei erreicht ein Kanal aufgrund der Spreizung mit einem 11 Bit langen PN-Code die Bandbreite von 22 MHz. Die Verfügbarkeit der Kanäle und die weiteren regionalen Einschränkungen zeigt die Tabelle 4.6. In Nordamerika und in Europa ist auf diese Weise der Betrieb von drei

überlappungsfreien Kanälen möglich. Während in Nordamerika nur die in Abbildung 4.28 gezeigten Kanäle 1, 6 und 11 mit einem Bandabstand von 3 MHz überlappungsfrei betrieben werden können, sind in Europa mit 13 Auswahlkanälen unterschiedliche Kombinationen oder größere Bandabstände möglich. So erreicht man z.B. bei der Nutzung der Kanäle 1, 7 und 13 Bandabstände von 8 MHz. Wenn man die Kanäle 1, 6 und 13 nutzt, dann beträgt der Bandabstand zwischen den Kanälen 6 und 13 immerhin 30 MHz.

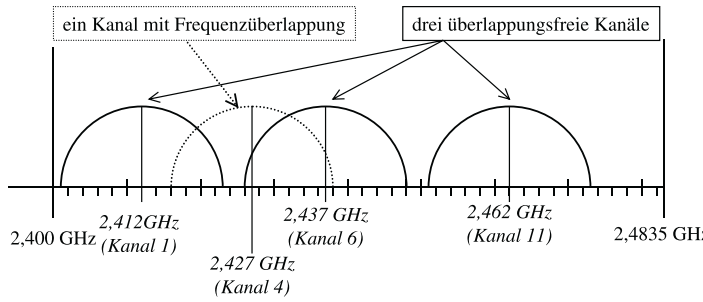


Abbildung 4.28: Kanalanordnung beim DSSS-Verfahren im IEEE802.11

Dieser Aspekt wird von den Befürwortern der anderen Frequenzspreiztechnologie, dem Frequenzsprungverfahren, gern als Kritikpunkt angeführt. Basierend auf den Erläuterungen in Abschnitt 2.7.3 leuchtet es ein, dass die Qualität von DSSS-Systemen nicht nur im Sinne ihrer Kanaleffizienz, sondern auch in Bezug auf ihre Störunempfindlichkeit mit wachsendem Spreizfaktor steigt. Entsprechend erfüllt das IEEE802.11-Verfahren nur minimale Anforderungen.

Präambel und Header werden grundsätzlich mit einer Datenrate von 1 Mbps übertragen, während die Datenpakete mit 1 oder 2 Mbps gesendet werden können.

Um darüber hinaus die Möglichkeit zu eröffnen, Büschelfehler besser ausgleichen zu können, werden die Daten in eine neue Abfolge gebracht. Im Gegensatz zu Systemen der Sprachübertragung dient diese Verwürfelung (*Scrambling*) nicht der höheren Fehlertoleranz bei Büschelfehlern, sondern einem Ausgleich des Frequenzspektrums (*Whitening*).

Kanal-ID	Mitten-frequenz	Nord-amerika	Europa	Frankreich	Spanien	Japan
1	2,412 GHz	x	x			
2	2,417 GHz	x	x			
3	2,422 GHz	x	x			
4	2,427 GHz	x	x			
5	2,432 GHz	x	x			
6	2,437 GHz	x	x			
7	2,442 GHz	x	x			
8	2,447 GHz	x	x			
9	2,452 GHz	x	x			
10	2,457 GHz	x	x	x	x	
11	2,462 GHz	x	x	x	x	
12	2,467 GHz		x		x	
13	2,472 GHz		x		x	
14	2,484 GHz					x

Tab. 4.6: Kanalanordnung beim DSSS-Verfahren im IEEE802.11 (Hinweis: Seit Anfang 2000 steht auch in Frankreich und Spanien das gesamte Spektrum von 2400 bis 2483 MHz zur Verfügung.)

Das Rahmenformat der DSSS-Übertragung ist in Abbildung 4.29 gezeigt.

PPDU						
PLCP Protocol Data Unit						
PLCP-Präambel		***PLCP Header***				***MPDU***
Synchronisation	*Start Frame Delimiter*	*Signal*	*MPDU Length Word*	*PLCP Signaling Field*	*Header Error Check*	*MAC Protocol Data Unit*
SYNC	***SFD***	***PLW***	***PLW***	***PSF***	***HEC***	*14 .. 4095 Bytes*
128 Bits	*16 Bits*	*12 Bits*	*12 Bits*	*4 Bits*	*16 Bits*	
besteht aus abwechselnden Nullen und Einsen; dient dem Empfänger der Erkennung eines ankommenden Signals und der Synchronisation	*feststehendes Bitmuster, das den Anfang des eigentlichen Frames kennzeichnet*	*spezifiziert die Länge des MPDU in Byte; maximale Länge: 2^{12}-1 = 4095 Bytes*	*spezifiziert die Länge des MPDU in Byte; maximale Länge: 2^{12}-1 = 4095 Bytes*	*spezifiziert die Datenrate, mit der das MPDU gesendet wird*	*Fehlerüberprüfung für den PLCP Header mittels 16b CRC*	*Nutzdaten*

*Abbildung 4.29: Rahmenformat des **P**hysical **L**ayer **C**onvergence **P**rocedure-(PLCP)-Rahmens für das DSSS-Verfahren im IEEE802.11*

Dieser höherbitratige Datenstrom wird nun noch mit einer DQPSK-Modulation (***D**ifferential **Q**uadrature **P**hase **S**hift **K**eying* - DQPSK) moduliert, was bei der Übertragung mit 1 Mbps dem Fall a) aus Abbildung 2.12 entspricht. Wird die Datenrate auf 2 Mbps gesetzt, werden die vier Zustände aus Fall b) in Abbildung 2.12 gewählt. Um noch höhere Datenraten zu erreichen, wird das in Abschnitt 4.7.2 beschriebene Verfahren eingesetzt.

Als grundlegende Parameter wurden für den DSSS-Standard die in Tabelle 4.7 genannten Größen festgelegt.

Tab. 4.7: Grundlegende Parameter der DSSS-Übertragung im 802.11-Standard

Größe	Wert
AslotTime	20 μs
ASIFSTime	10 μs
AMPDUMaxLength	4095 Byte

4.5 Weitere Dienste

4.5.1 Synchronisation

Mit Hilfe der ***T**iming **S**ynchronisation **F**unction* (TSF) werden alle Stationen auf eine Systemzeit synchronisiert. Die Synchronisation wird durch regelmäßiges Versenden des TSF-Zeitgebers in einem so genannten Beacon zu den durch ***T**arget **B**eacon **T**ransmission **T**ime* (TBTT) festgelegten Zeiten gewährleistet. In einem Infrastrukturnetz ist der Zugangspunkt für die Aussendung des Synchronisations-Beacons zuständig, während in einem Ad-hoc-Netz die Beacon-Erzeugung auf alle Stationen verteilt wird. Hierzu wird die Ausstrahlung des Beacons von den verschiedenen Stationen mit verschiedenen, zufällig ausgewählten Verzögerungszeiten durchgeführt.

4.5.2 Energiesparmodus

Da viele der drahtlosen Geräte batteriebetrieben sind, sieht der Standard unmittelbar einen Energiesparmodus vor, der mit den anderen Stationen abgesprochen werden muss. Insbesondere müssen die Stationen auch im so genannten *Doze*-Modus weiterhin ihre Erreichbarkeit gewährleisten. Hierfür wurden bestimmte Monitoring-Algorithmen entwickelt, die sich für den Infrastruktur- und den Ad-hoc-Modus unterscheiden.

4.5.3 Dienste im ESS

Für den Betrieb von ***E**xtended **S**ervice **S**ets* (ESS) müssen folgende Dienste bereitgestellt werden:

- der *Distribution Service* für die Datenübermittlung zwischen den Zugangspunkten von Sender und Empfänger,
- der *Integration Service* für die Datenübermittlung vom Zugangspunkt der sendenden Station zum Portal des Empfängers im Festnetz, wobei je nach Bedarf eine Adress- und Protokollanpassung erfolgen muss, und
- der *Association Service*, der die An- bzw. Abmeldung von Stationen beim Wechsel ihres BSS übernimmt und alle Zugangspunkte im Distribution System über die neue Lokation benachrichtigt.

4.6 Sicherheit

Drahtlose Netzwerke unter Nutzung elektromagnetischer Wellen stellen in besonderem Maße ein Sicherheitsrisiko dar, da die Wellen nicht auf das Netzwerk im engeren Sinne beschränkt sind, sondern innerhalb der Funkreichweite von beliebigen Stationen abgehört werden können.

Im Bereich der Sicherheit sind drei Ebenen zu unterscheiden. Dabei müssen (wie immer) auch einige Einschränkungen berücksichtigt werden:

- Auf der niedrigsten Ebene erfolgt eine Zulassung der Teilnehmer auf der Grundlage eines Schlüssels, der als ***E**lectronic **Sys**tem **ID*** (SSID, ESSID) bezeichnet wird. Diese ID wird von einem Administrator in allen mobilen Teilnehmern und allen Zugangspunkten eingetragen. Dieser zeigt die Zugangsrechte des Teilnehmers an, aber nicht die eindeutige Identifikation des Teilnehmers. Dabei ergeben sich zwei Einschränkungen:
  - Es ist häufig kein Problem, eine allgemeine Zugangsnummer herauszufinden, um den Verkehr auf dem Netzwerk »kriminell« abzuhören.
  - Die meisten Hersteller von mobilen Stationen erlauben die Angabe der Option *any* in ihren Konfigurationsdateien, wodurch der Einsatz in allen Netzwerken authentisiert ist.
- Die Authentisierung erlaubt die Teilnahme nur der zugelassenen Stationen an der Kommunikation. Die Identität von Stationen wird bei der im Rahmen des 802.11 möglichen *Link Level Authentification* zwischen den beteiligten Stationen ausgetauscht. Hierzu werden die MAC-Adressen der mobilen Teilnehmer in die Zugangslisten der Zugangspunkte eingetragen. Das hat jedoch folgende Nachteile:
  - Bei den meisten auf dem Markt verfügbaren Produkten kann die MAC-Adresse des mobilen Teilnehmers verändert werden, so dass auch hier ein missbräuchlicher Einsatz möglich erscheint.
  - Während die Authentisierung im Bereich kleiner drahtloser Netzwerke recht problemlos umzusetzen ist, ergibt sich bei großen Netzwerken mit mehreren Zugangspunkten die Notwendigkeit einer umfangreichen Administration jeder Station für jeden Teilnehmer, um einen Wechsel zwischen den Funkzellen zu ermöglichen (*Roaming*). Bislang bieten nur einige wenige Hersteller komfortable Werkzeuge zur Verwaltung größerer drahtloser Netzwerke an.
- Um die Authentisierung nicht nur auf Geräteebene, sondern auch benutzerbezogen zu unterstützen, implementieren fast alle Hersteller den ***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice* (RADIUS). Dieser ermöglicht die zentrale Verwaltung von Benutzeridentifikationen und Passwörtern.
- Der Inhalt von Funknachrichten kann im Rahmen des optionalen ***W**ired **E**quivalent **P**rivacy* (WEP) mit 40 Bit verschlüsselt werden. Dabei muss allerdings berücksichtigt werden, dass

- WEP lediglich ein optionaler Bestandteil des Standards ist, so dass bei der Systemauswahl 802.11-konformer Systeme unbedingt auf dessen Implementierung geachtet werden sollte.
- über die 40 Bit-Kodierung hinausgehend einige Hersteller eine Kodierung mit 128 Bit anbieten. Hierbei handelt es sich jedoch um proprietäre Entwicklungen, die die Interoperabilität der Systeme unterschiedlicher Hersteller behindern.
- auch die Werkzeuge zur Verwaltung der WEP-Schlüssel herstellerspezifisch sind.

Darüber hinaus können aufgrund der Einpassung in den IEEE802-Standard natürlich auch alle Sicherheitsmechanismen der höheren Protokollebenen wie z.B. IPSec eingesetzt werden.

Das WEP-Verfahren basiert auf einem symmetrischen Algorithmus, bei dem Sender und Empfänger einen gemeinsamen Schlüssel (*Shared Key*) verwenden. Ausgehend von diesem Schlüssel und einem zufällig bestimmten ***I**nitialisierungs**v**ektor* (IV) wird mit Hilfe eines Generators für Pseudo-Zufallszahlen eine Schlüsselfolge bestimmt, mit der der Klartext bitweise mit einem Exklusiv-Oder-Gatter verknüpft wird (vgl. Abbildung 4.30).

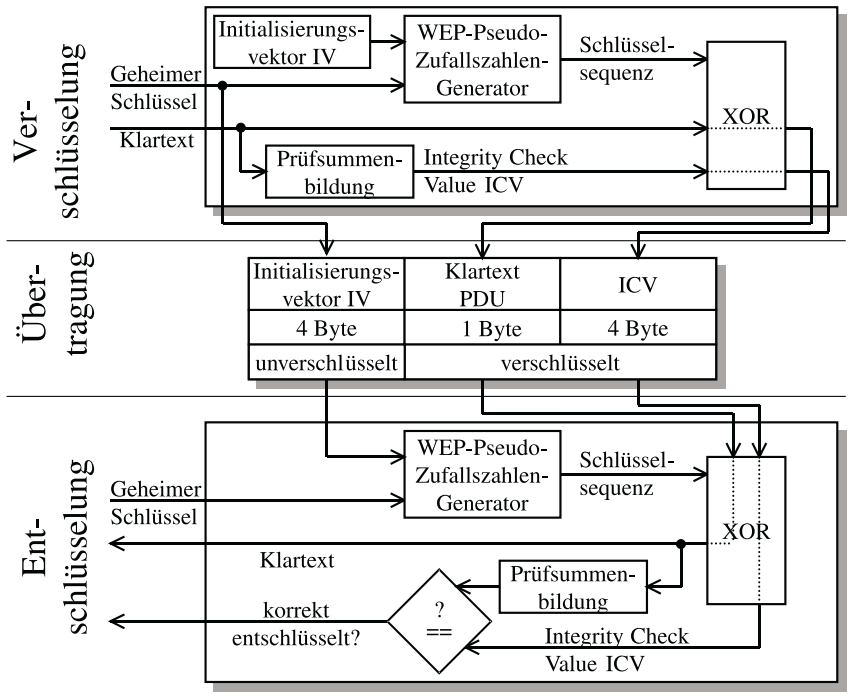


Abbildung 4.30: Verschlüsselung, Übertragung und Entschlüsselung nach dem WEP-Algorithmus

Dieser Generator arbeitet nach dem RC4-Verschlüsselungsalgorithmus (***K**ey **S**cheduling **A**lgorithm* - KSA), der mit einem statischen Schlüssel von 40 Bit (WEP) oder 128 Bit (WEP2) arbeitet. Dieser Algorithmus basiert darauf, dass

ein vergleichsweise kurzer Schlüssel in einen pseudozufälligen unendlich langen Schlüssel expandiert wird, mit dem der zu übertragende Text verschlüsselt wird. Dabei werden sowohl der Klartext als auch die Prüfsumme verschlüsselt und mit dem unverschlüsselten Initialisierungsvektor übertragen. Auf der Empfängerseite wird der verschlüsselte Text mit dem ebenfalls expandierten Schlüssel mit einer Exklusiv-Oder-Verknüpfung entschlüsselt.

Weitere Aspekte bezüglich der Sicherheit des IEEE802.11-Standards werden in Abschnitt 10.1 diskutiert.

4.7 Erweiterungen des Standards

4.7.1 Der IEEE802.11a-Standard

Der Standard 802.11a des IEEE stellt eine Erweiterung des grundlegenden Standards 802.11 dar. Dabei werden die Mechanismen des Kanalzugriffs auf der MAC-Schicht unverändert übernommen. Auf der Bitübertragungsschicht findet die Übertragung nunmehr im 5 GHz-Bereich statt, wobei die Entwicklung insbesondere die Regeln des US-amerikanischen ***U**nlicensed **N**ational **I**nformation **I**nfrastructure* (UNII)-Bands berücksichtigt. Grundsätzlich sind Datenraten von 6 bis 54 Mbps geplant. Der 802.11a greift auf ein ***O**rthogonal **F**requency **D**ivision **M**ultiplex* (OFDM)-Verfahren (vgl. Abschnitt 2.8) zurück, das weitgehend den Festlegungen des HiperLAN/2-Standards entspricht und deswegen in Kapitel 8 besprochen wird. Dort finden sich auch einige Anmerkungen bezüglich der Konkurrenzsituation der beiden Technologien.

Die ersten 802.11a-konformen Geräte sind für das Ende des Jahres 2001 angekündigt. Aufgrund der vergleichsweise hohen Kosten kann vermutet werden, dass die ersten Anwendungen im Bereich der LAN-LAN-Kopplungen positioniert sein werden, zumal dort der Bandbreitenbedarf am höchsten und die Kostensensitivität am geringsten erscheint.

Aufgrund der identischen Eigenschaften des Kanalzugriffs haben einige Hersteller bereits Geräte angekündigt, die die Migration zu den leistungsfähigeren Systemen erleichtern sollen [Proxim 2001].

4.7.2 Der IEEE802.11b-Standard

Der im September 1999 ratifizierte 802.11b-Standard, der in älteren Quellen zunächst auch als 802.11HR (***H**igh **R**ate*) bezeichnet wurde, spezifiziert Systeme mit einer Bandbreite von 5,5 oder 11 Mbps im 2,4 GHz-Band. Er hat mittlerweile eine so große Verbreitung gefunden, dass kaum noch Systeme nach dem 802.11-Standard auf dem Markt verfügbar sind, die Datenraten von nur 1 oder 2 Mbps unterstützen.

Der IEEE802.11b-Standard basiert auf dem DSSS-Verfahren, wobei die Systeme rückwärts kompatibel zum 802.11-1997-DSSS-Standard sind. Im Verlauf des Standardisierungsverfahrens war es zu starken Interessenkonflikten zwischen den Befürwortern von FHSS einerseits und DSSS andererseits gekommen, wobei auch noch mehrere DSSS-Verfahren zur Diskussion standen. Im Sinne des eigenen Investitionsschutzes hatten vor allem die Hersteller Lucent und Harris (Prism) versucht, mit der Entwicklung proprietärer Systeme den Standardisierungsprozess im 2,4 GHz-Bereich für ihre Produkte zu entscheiden. Aber das Standardisierungsgremium wählte weder die ***P**ulse **P**osition **M**odulation* (PPM) von Lucent für Datenraten von 5 und 10 Mbps noch das MBOK (***M**-ary **Bi**-**O**rthogonal **K**eying, **m**-ary=m-fach*) von Harris mit Datenraten von 5,5 und 11 Mbps (Heeg 1999).

Von großer Bedeutung war jedoch die Tatsache, dass nur noch ein physischer Standard verabschiedet und somit auch die Interoperabilität aller standardisierten 11 Mbps-Geräte gewährleistet wurde. Die Erhöhung der Datenrate wird im Wesentlichen durch ein Modulationsverfahren mit verbesserter Nutzung des Frequenzspektrums erreicht. Dieses erlaubt weiterhin die Bandbreite eines Kanals von 22 MHz, so dass unverändert drei unabhängige Kanäle betrieben werden können. Insbesondere werden im ***Q**uadrature **P**hase **S**hift **K**eying* (QPSK) mehr Bits pro Symbol übertragen als im ***B**inary **P**hase **S**hift **K**eying* (BPSK). Darüber hinaus finden auf 8 Bits verkürzte Chipfolgen Anwendung.

Dabei wird das CDMA-Verfahren bei den hohen Datenraten nun auch zur Unterscheidung der übertragenen Datenbits eingesetzt. Die aus acht komplementären und komplexen Chips bestehenden Codewörter werden nach einer verallgemeinerten Hadamard-Kodierung berechnet, bei der

- φ_1 zu allen Chips,
- φ_2 zu allen ungeradzahligen Chips,
- φ_3 zu allen ungeradzahligen Paaren von Chips und
- φ_4 zu den ersten vier Chips

addiert wird. Zusätzlich werden das vierte und siebte Chip mit einem negativen Vorzeichen versehen, um die Korrelationseigenschaften der Codes zu verbessern.

$$\underline{C} = \left\{ e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, \right.$$
$$\left. e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1} \right\}$$

mit

Bei der Übertragung mit 5,5 Mbps besteht ein Symbol aus vier Datenbits. Die ersten beiden Bits d_0 und d_1 wählen die Phasenverschiebung φ_1 in Übereinst $\varphi_i \in \{0, \pi/2, \pi, 3\pi/2\}, i \in \{1,2,3,4\}$1 aus, während in Abhängigkeit von d_2 und d_3 die Werte von φ_2, φ_3 und φ_4 gemäß

$$\varphi_2 = d_2 * \pi + \pi/2$$
$$\varphi_3 = 0$$
$$\varphi_4 = d_3 * \pi$$

bestimmt werden.

Bei der Verdopplung der Übertragungsrate auf 11 Mbps müssen acht Bits in einem Symbol zusammengefasst werden. Dabei bestimmen die Datenbits d_0 und d_1 wiederum die Phasenverschiebung φ_1 in Übereinstimmung mit der Abbildung 4.31, während die Paare d_2-d_3, d_4-d_5 und d_6-d_7 die Phasen φ_2, φ_3 und φ_4 in Übereinstimmung mit Abbildung 4.32 vorgeben und damit eines von 64 möglichen CCK-Codewörtern auswählen, das über φ_1 DQPSK-moduliert wird.

d_0	d_1	φ_1	
		für die Symbole c_0, c_2, c_4 und c_6	*für die Symbole c_1, c_3, c_5 und c_7*
0	*0*	*0*	*π*
0	*1*	*π / 2*	*3π / 2*
1	*0*	*π*	*0*
1	*1*	*3π / 2*	*π / 2*

Abbildung 4.31: Bestimmung der Phasen der DQPSK-Modulation bei 5,5 Mbps

d_2	d_3	$\varphi_2 = \varphi_3 = \varphi_4$
d_4	d_5	
d_6	d_7	
0	*0*	*0*
0	*1*	*π / 2*
1	*0*	*π*
1	*1*	*3π / 2*

Abbildung 4.32: Bestimmung der Phasen der DQPSK-Modulation bei 11 Mbps

Abbildung 4.33 zeigt die vier Übertragungsverfahren in der Übersicht. Dabei wird der Zusammenhang zwischen der auf 1,375 MSymbol/s vergrößerten Symbolrate und der verringerten Codelänge deutlich, die in der unveränderten Chiprate von 11 MChips/s resultiert.

Dabei ist es offensichtlich, dass mit der Erhöhung der Datenrate auch die Störanfälligkeit der Übertragung steigt. Der Empfänger muss nun acht statt bisher zwei oder vier verschiedene Zustände pro Symbol unterscheiden können. Entsprechend müssen höhere Anforderung an den Signal-Rausch-Abstand (SNR, vgl. Abschnitt 2.5) gestellt werden. Tabelle 4.8 zeigt typische Werte für die zusätzlichen Anforderungen an das SNR relativ zu den Werten für eine erfolgreiche Übertragung bei 1 Mbps.

Abbildung 4.33: Erhöhung der Datenrate durch mehrwertige Übertragung bei Verkürzung der PN-Codes beim IEEE802.11b

		Datenrate	Chiprate
1 Mbps	11 chips/Symbol 1 bit/Symbol 1 MSymbol/s	$1\frac{bit}{Symbol} * 1\frac{MSymbol}{s} = 1\frac{Mbit}{s}$	$11\frac{Chips}{Symbol} * 1\frac{MSymbol}{s} = 11\frac{MChips}{s}$
2 Mbps	11 Chips/bit 2 bit/Symbol 1 MSymbol/s	$2\frac{bit}{Symbol} * 1\frac{MSymbol}{s} = 2\frac{Mbit}{s}$	$11\frac{Chips}{Symbol} * 1\frac{MSymbol}{s} = 11\frac{MChips}{s}$
5,5 Mbps	8 Chips/bit 4 bit/Symbol 1,375 MSymbol/s	$4\frac{bit}{Symbol} * 1{,}375\frac{MSymbol}{s} = 5{,}5\frac{Mbit}{s}$	$8\frac{Chips}{Symbol} * 1{,}375\frac{MSymbol}{s} = 11\frac{MChips}{s}$
11 Mbps	8 Chips/bit 8 bit/Symbol 1,375 MSymbol/s	$8\frac{bit}{Symbol} * 1{,}375\frac{MSymbol}{s} = 11\frac{Mbit}{s}$	$8\frac{Chips}{Symbol} * 1{,}375\frac{MSymbol}{s} = 11\frac{MChips}{s}$

Aus diesem Grund können die höheren Datenraten nur dann erreicht werden, wenn bei unveränderter Ausgangsleistung und Antennencharakteristik die Kanalqualität ausreichend gut ist. Sinkt die Kanalqualität unter die erforderliche Grenze ab, kann immer noch mit einer geringeren Geschwindigkeit übertragen werden. Die meisten Geräte verfügen über eine solche adaptive Anpassung der Übertragungsgeschwindigkeit.

Tab. 4.8: Anforderungen an das Verhältnis von Signalstärke zu Rauschen für die verschiedenen Geschwindigkeitsstufen im 802.11b-Standard

Datenrate	SNR-Anforderung, relativ zu 1 Mbps
1 Mbps	0 dB
2 Mbps	2 dB
5,5 Mbps	4 dB
11 Mbps	8 dB

Für die höheren Geschwindigkeiten sind im IEEE802.11b-Standard zwei Möglichkeiten zur Kodierung in den Paketrahmen vorgesehen. Zum einen können – neben kleineren Veränderungen, die hier nicht näher dargestellt werden sollen – im Signalfeld des normalen PLCP-PPDU, wie er in Abbildung 4.29 dargestellt ist, die höheren Geschwindigkeiten eingetragen werden. Der Steuerrahmen wird dabei aber weiterhin mit 1 Mbps übertragen, was u.a. dazu führt, dass der relative Anteil des Protokolls am übertragenen Verkehr weiter steigt.

Um diesen Anstieg geringer zu halten, sieht der Standard auch ein verkürztes Format vor, das die Übertragungszeit des Headers halbiert, indem

- die Länge der PLCP-Präambel von 144 Bits auf 72 Bits halbiert wird,
- die Übertragungsgeschwindigkeit des PLCP-Headers mit unveränderter Länge auf 2 Mbps heraufgesetzt wird.

Auf diese Weise ist der verkürzte Header auch noch kompatibel mit IEEE802.11-Systemen, die nur Datenraten von 1 und 2 Mbps unterstützen.

4.7.3 Weitere Standards

Neben den bereits erwähnten Teilstandards 802.11a und b existieren noch eine Reihe weiterer Aktivitäten, die dem gesamten Standard zu weiterem Erfolg verhelfen sollen und die in Tabelle 4.9 aufgeführt sind.

802.11b-cor	Korrekturen des MIB aus 802.11
802.11d	Aktualisierung der *Regulatory Domains*
802.11e	Verbesserungen bei der Unterstützung von Dienstgüten (QoS) und der Sicherheitsmechanismen (128b, verbesserte Authentifizierung, Verwaltung der Schlüssel)
802.11f	IAPP (***I**nter **A**ccess **P**oint **P**rotocol*) für *Roaming* und *Load Balancing*
802.11g	Erweiterung des 802.11b für 22 Mbps
802.11h	Frequenzspektrum des 802.11a

Tab. 4.9: Erweiterungen der IEEE802.11-Protokollfamilie

Einige der Teilstandards, die zum gegebenen Zeitpunkt noch nicht verabschiedet sind, werden noch kurz vorgestellt:

- Der 802.11e versucht, den MAC-Layer dahingehend zu erweitern, dass auch Datenströme unter Nutzung der PCF mit größerer Funktionalität transportiert werden können. Insbesondere die Unterstützung der PCF beim Roaming und beim Peer-to-Peer-Betrieb ist bislang noch mit Schwierigkeiten behaftet.
- Auch im Rahmen des 802.11f wird der Betrieb von komplexeren Netzwerken diskutiert. Dabei steht die Kommunikation zwischen den Zugangspunkten im Zentrum der Aufmerksamkeit. Insbesondere der Austausch von Verwaltungs- und Zugangsdaten soll vereinheitlicht werden.
- Von den weiteren Unterstandards ist der 802.11g von besonderer Bedeutung, der von einer Arbeitsgruppe vorbereitet wird. Ziel ist die Ausarbeitung einer Spezifikation mit einer weiteren Erhöhung der Datenrate auf 22 Mbps für den 802.11 MAC im 2,4 GHz-Trägerband. Die Aktivitäten werden im Rahmen des IEEE802.11g von der *Higher Rate IEEE802.11b Study Group* (HRbSG) durchgeführt. Dabei wird ein OFDM-Modulationsverfahren (vgl. Abschnitt 2.8) zum Einsatz kommen.

5 Bluetooth

5.1 Standard

5.1.1 Hintergrund

Die Anfänge der Aktivitäten zu Bluetooth gehen bereits auf das Jahr 1994 zurück, als die Mobile Communications Division von Ericsson eine Machbarkeitsstudie zum Ersatz der vielfältigen Kabelverbindungen zwischen Mobiltelefonen und den verschiedenen Peripheriegeräten in Auftrag gab. In der Folge wurde Anfang 1998 die ***B**luetooth **S**pecial **I**nterest **G**roup* (BSIG) von den fünf Firmen IBM, Toshiba, Intel, Ericsson und Nokia gegründet, um einen firmenübergreifenden Standard für ***P**ersonal **A**rea **N**etworks* (PAN) zu erstellen. Die Zielsetzung wurde zu diesem Zeitpunkt durchaus im Sinne eines *Wireless USB* verstanden. Die erste Version 1.0 konnte dann bereits 1999 verabschiedet werden. Eine erste Überarbeitung im Rahmen der Version 1.0b erfolgte im Dezember 1999. Seit Februar 2001 liegt der Standard nun in der Version 1.1 vor, die dem Einvernehmen nach die erste solide Basis für marktgerechte Produkte darstellt, da die Vorversionen eine Reihe von Ungenauigkeiten und Fehlern aufwiesen, die Fehler bei der Kompatibilität, der sauberen Implementierung von Pico-Netzen sowie einer eindeutigen Master-Slave-Zuweisung zur Folgen hatten [Klinkenberg 2001]. Aber auch die Version 1.1 verfügt noch über einige Schwächen in Bezug auf die Interoperabilität [Blaesner1]. Der Bluetooth-Standard V1.1 ist unter *http://www.bluetooth.com/developer/specification/specification.asp* verfügbar.

Der engere Kreis der BSIG-Gründer ist im Rahmen einer Promoter-Group um die Firmen 3Com, Lucent, Microsoft und Motorola erweitert worden. Die BSIG umfasst rund 2.500 Mitglieder.

Der Name der Technologie ist abgeleitet von Harald II. Blaatand (Blauzahn), der von 940 bis 981 als König von Dänemark das Land christianisierte und Norwegen und Dänemark vereinigte. Dabei ist der Name vermutlich auf die beiden Worte blå für dunkelhäutig und tan für großer Mann zurückzuführen, was in diesem Fall gleichbedeutend mit König oder Anführer ist.

Der Bluetooth-Standard verfolgt im Wesentlichen drei Anwendungsszenarien, mit denen er auf der Ebene der Personal Area Networks positioniert ist:

- Ersatz von Kabeln
- Daten- und Sprachzugangspunkte
- Personal Adhoc Networks

Um diese Anwendungen erfüllen zu können, werden nicht notwendigerweise PCs benötigt. Vielfach gilt es, vergleichsweise einfache und günstige Geräte mit einer drahtlosen Anschlussmöglichkeit zu versorgen. Aus diesem Grund muss es ein wesentliches Merkmal des Bluetooth-Standards sein, möglichst einfache und somit kostengünstige Lösungen zu ermöglichen.

5.1.2 Aufbau

Die wichtigsten Bestandteile des Bluetooth-Standards in der gegenwärtigen Version 1.1 zeigt die Abbildung 5.1. Dabei sind folgende Besonderheiten hervorzuheben:

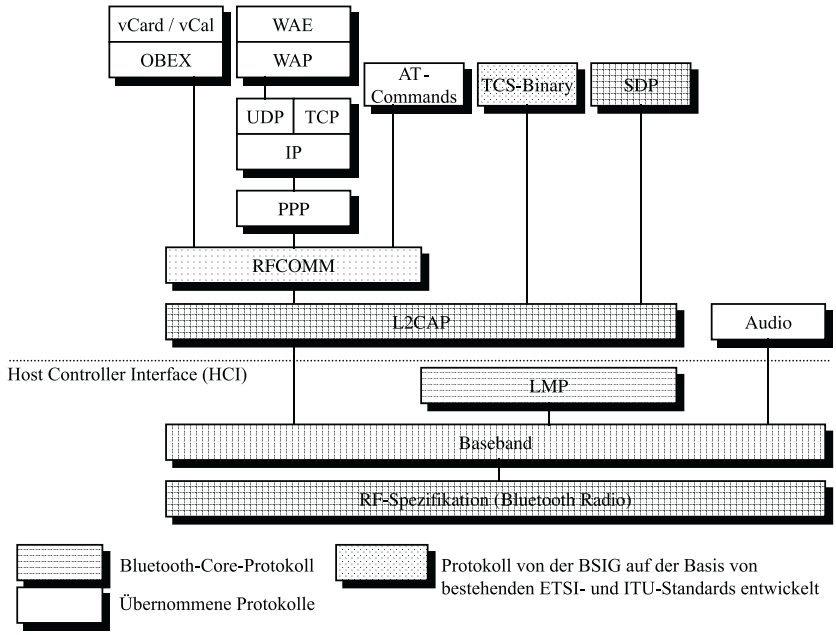


Abbildung 5.1: Aufbau des Bluetooth-Standards (Mettala 1999)

- Die Beschreibung der Bluetooth-Kommunikationsprotokolle umfasst alle Ebenen der Protokollschichten. Insbesondere die Steuerprotokolle zum Aufbau der Ad-hoc-Netzwerke, aber auch die Bestandteile zur Übertragung isochroner Verkehrsströme reichen deutlich über die reinen Transportdienste eines IEEE802.11 hinaus. Bluetooth stellt ein komplettes Funksystem bereit. Dieser Vorteil muss allerdings vor dem Hintergrund der Interoperabilität der unterschiedlichen Gerätetypen betrachtet werden (vgl. Abschnitt 5.7).
- Der gesamte Protokollstapel weist nicht nur Bluetooth-spezifische Protokolle auf, sondern greift insbesondere auf den höheren anwendungsorientierten Schichten auf bestehende und verbreitete Protokolle zurück. Als Beispiel seien die Internet-Protokolle des TCP / IP-Stapels genannt.

- Betrachtet man den Umfang der in Abbildung 5.1 gezeigten Protokollbestandteile, so leuchtet unmittelbar ein, dass eine Bluetooth-Station, die den kompletten Umfang realisiert, eine Komplexität erreicht, die der angestrebten einfachen und kostengünstigen Realisierung entgegensteht. Deswegen ist statt einer kompletten Implementierung vorgesehen, nur die notwendigen Bestandteile in den Geräten zu implementieren. Lediglich die Kernprotokolle müssen in jeder Station enthalten sein.
- Die Bluetooth-Spezifikation umfasst mit dem Host Controller Interface (HCI) auch eine Befehlsschnittstelle zu Baseband Controller und Link Manager sowie zu Hardware-Status und Befehlsregistern. Die Positionierung des HCI kann angepasst werden. Abbildung 5.1 zeigt ein typisches Beispiel.
- Bei der Standardisierung wurde nicht auf eine Konformität mit den Schichten der verbreiteten Referenzmodelle (OSI-Referenzmodell oder TCP / IP-Referenzmodell) geachtet.
- Bluetooth ist außerhalb eines bestehenden Gremiums standardisiert. Eine Einpassung in andere Standardfamilien, wie z.B. den Standards nach IEEE802.x, wird zwar – vor allem von Seiten des IEEE – angestrebt, erscheint aber auf der Grundlage der vorangehend genannten Punkte nur nach umfassenden Anpassungen möglich.

5.1.3 Bestandteile

Im Folgenden werden die wichtigsten Bestandteile des Bluetooth-Standards kurz vorgestellt:

- RF und Baseband: Die beiden Spezifikationen RF und Baseband entsprechen näherungsweise der PHY- und der MAC-Ebene im IEEE-Protokollstapel. Die Funktionsweise dieser beiden Ebenen wird in den folgenden Abschnitten erläutert.
- ***L**ink **M**anager **P**rotocol* (LMP): Das LMP erfüllt Aufgaben der Netzverwaltung. Diese umfassen insbesondere den Verbindungsaufbau zwischen Stationen, die Authentifizierung und Verschlüsselung sowie die Steuerung der Energiesparmodi und der Gerätezustände in einem Piconetz.
- ***L**ogical **L**ink **C**ontrol and **A**daptation **P**rotocol* (L2CAP): Das L2CAP verbindet die Protokolle der höheren Schichten mit den Aufgaben des Basisbands. Es ist in der Weise parallel zu LMP angeordnet, dass L2CAP die Übertragung der Nutzdaten übernimmt. L2CAP stellt sowohl verbindungsorientierte als auch verbindungslose Dienste zur Verfügung, greift selbst aber nur auf die verbindungslosen asymmetrischen ACL-Verbindungen des Basisbandprotokolls zu.
- ***S**ervice **D**iscovery **P**rotocol* (SDP): Die Erkennung der verschiedenen Dienste und der Charakteristika der jeweiligen Dienste durch das SDP ist ein wesentlicher Bestandteil des Bluetooth-Protokolls. Es besteht die Möglichkeit, die zur Verfügung stehenden Dienste abzufragen und

darauf basierend eine Verbindung aufzubauen. SDP stellt die Grundlage dar, auf der die Bluetooth-Stationen vergleichsweise einfach Ad-hoc-Netzwerke aufbauen können.

- *Drahtloses Kabel* (RFCOMM): Der RFCOMM-Standard, der einen Teil der ETSI-Spezifikation TS 07.10 für den Bluetooth-Standard anpasst, emuliert eine serielle RS-232-Schnittstelle. Er stellt einen wesentlichen Bestandteil für viele Anwendungen dar und zeigt deutlich Intention und Leistungsumfang des Bluetooth-Standards. Dieser beschreibt vor allem die Punkt-zu-Punkt-Verbindung zwischen zwei Geräten über die »serielle Schnittstelle Luft«. Aus diesem Grund werden zum Beispiel auch LAN-Verbindungen über TCP/IP über das serielle Point-to-Point-Protocol (PPP) über RFCOMM implementiert.
- *Telefonkopplung:* Zwei Bestandteile beschreiben die Kopplung von Telefondiensten. Während ***T**elephony **C**ontrol **S**ervice – Binary* (TCS Binary) die Signalisierung zum Gesprächsaufbau und -abbau auf der Grundlage der ITU-T-Empfehlung Q.931 spezifiziert, hat die Bluetooth SIG einen Satz der so genannten AT-Kommandos aus den einschlägigen ITU- und ETSI-Spezifikationen übernommen, um die Ansteuerung von Modems und Mobiltelefonen zu gewährleisten. Darüber hinaus stehen auch Fax-Dienstleistungen zur Verfügung.

  Es ist darauf hinzuweisen, dass nur der Gesprächsaufbau über das TCS-BIN-Protokoll und die L2CAP-Ebene erfolgt. Die Übertragung der Nutzdaten erfolgt über das Audioprotokoll, das unmittelbar auf einen SCO-Link im Baseband zugreift.

Darüber hinaus haben verschiedene anwendungsnahe Protokolle Eingang in den Bluetooth-Standard gefunden.

- Hierzu zählt das ***Ob**ject-**Ex**change*-(OBEX-)Protokoll, das aus dem IrDA-Standard für Infrarot-Verbindungen übernommen wurde und das die Repräsentation von Objekten und die Strukturierung von Dialogen zwischen den Objekten modelliert.
- Mit Hilfe von OBEX wird das *vCard*-Protokoll abgewickelt, das den Austausch von virtuellen Visitenkarten ermöglicht.
- Das ***W**ireless **A**pplication **P**rotocol* (WAP), das für die Übermittlung von WML-Ressourcen auf Mobiltelefone entwickelt wurde, steht ebenfalls im Bluetooth-Standard zur Verfügung und wird über die TCP/IP-Schichten realisiert.

5.1.4 Profile

Im Bluetooth-Standard sind ebenfalls die Details der jeweiligen Protokollstapel festgelegt. Insbesondere wird beschrieben, auf welche Weise Anwendungssoftware auf die verschiedenen Ebenen des Protokollstapels zugreifen darf. Diese Festlegung erfolgt im Rahmen der Profiles. Dabei handelt es sich

um ***A**pplication **P**rogram **I**nterfaces* (API), die die Mehrzahl der möglichen Anwendungsmodelle abdecken und die den Dienstzugangspunkten aus dem ISO-OSI-Referenzmodell (vgl. Abschnitt 2.2.1) entsprechen. Dies hat den Vorteil, dass Programme unterschiedlicher Hersteller auf verschiedenen Geräten problemlos miteinander kommunizieren können, solange sie sich an diese möglichst vollständigen Definitionen halten. Diese Festlegungen erreichen jedoch aufgrund der vielfältigen Aspekte eine sehr hohe Komplexität. Dies führt zu drei Aussagen:

- Die vollständige und konsistente Definition ist sehr aufwändig und stellt das hauptsächliche Ziel der Überarbeitungen bis zum gegenwärtigen Standard V1.1 dar.
- Der Standard wird sehr umfangreich. Die Version V1.1 umfasst beispielsweise 13 anwendungsbezogene Profile beispielsweise für die Kommunikation über eine serielle Schnittstelle (*Serial Port*), mit einem Headset, einem Fax, für die Ankopplung an ein LAN und für den Datentransfer mittels ***F**ile **T**ransfer **P**rotocol* (FTP).
- Aber auch die fehlerfreie und effiziente Nutzung der Schnittstellen setzt ein umfangreiches Know-how voraus und erhöht die Eintrittsschwelle für neue Bluetooth-Entwicklungen.

5.2 Architekturen

Ein Bluetooth-Netzwerk ist grundsätzlich nach dem Master-Slave-Prinzip aufgebaut, wobei der Master die Steuerung des Verkehrsflusses übernimmt. Auf diese Weise sind vergleichsweise einfach isochrone Verkehrsströme abzuwickeln, wie sie beispielsweise im Rahmen des Audiomoduls benötigt werden. Alle Bluetooth-Geräte besitzen identische Hardware-Eigenschaften, so dass die Auswahl des Masters erst während des Aufbaus des Netzwerks erfolgt. Die Kriterien zur Übernahme der Master-Rolle werden in Abschnitt 5.4.2 beschrieben.

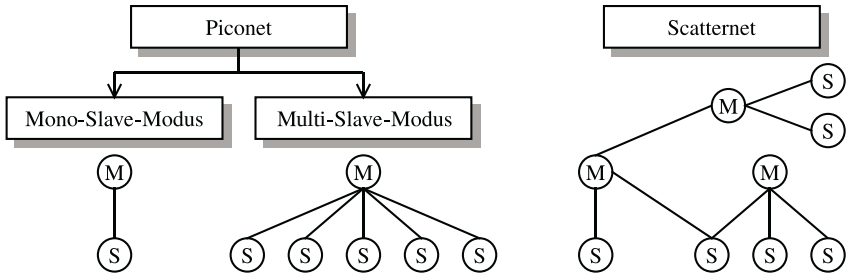


Abbildung 5.2: Architekturen von Bluetooth-Netzwerken

Grundsätzlich sind folgende Arten von Bluetooth-Netzwerken zu unterscheiden (vgl. Abbildung 5.2):

- Wenn nur ein Master in einem Netzwerk vorhanden ist, handelt es sich um ein *Piconet*.
  - Wenn der eine Master ausschließlich mit einem Slave im Rahmen einer Punkt-zu-Punkt-Verbindung (Point-to-Point) kommuniziert, wird das Netzwerk im *Mono-Slave-Modus* betrieben.
  - Der eine Master kann aber auch im *Multi-Slave-Modus* Punkt-zu-Multipunkt-Verbindungen (Point-to-Multipoint) mit bis zu sieben aktiven Slaves etablieren, wobei weitere Slaves im geparkten Zustand passiv teilnehmen können. Die Beschreibung der Zustände erfolgt in Abschnitt 5.4.
- Ein *Scatternet* setzt sich aus mehreren Piconetzen zusammen (engl.: *to scatter about* (oder *around*) verstreuen, ausstreuen; *to be scattered all over the place* überall herumliegen). Da jedes Piconetz von einem Master verwaltet wird, gibt es im Scatternet-Modus folgerichtig mehrere Master. Dabei kann eine Station als Slave in mehreren Piconets angemeldet sein und nacheinander in diesen Netzen auch aktiv sein. Darüber hinaus kann ein Master eines Piconetzes gleichzeitig auch Slave in einem anderen Piconetz sein.

5.3 Kanalzugriff

5.3.1 Einordnung

Die Vorgaben der Bluetooth-Core-Standards unterscheiden sich in wesentlichen Aspekten von den Regeln des IEEE802.11, da explizit verschiedene Verkehrstypen mit einer garantierten Dienstgüte unterstützt werden sollen. Hierzu wird im Gegensatz zur PCF bei Bluetooth genau festgelegt, zu welchen Zeitpunkten der Master und zu welchen Zeitpunkten die Slaves senden dürfen. Die Auswahl, welcher Slave zu welchem Zeitpunkt auf den Kanal zugreifen darf, wird zentral durch den Master verwaltet. Auf diese Weise ist eine einfache Verwaltung der Übertragungskapazität möglich.

Um die unterschiedlichen Anforderungen der verschiedenen Verkehrstypen zu erfüllen, sieht Bluetooth mit Hilfe von Verbindungen, Paketen und Kanälen verschiedene Mechanismen vor, die in Abbildung 5.3 im Überblick gezeigt und im Folgenden erläutert werden.

Verbindungen

Der Bluetooth-Standard sieht in den bisherigen Versionen zwei grundsätzliche Kommunikationsarten vor:

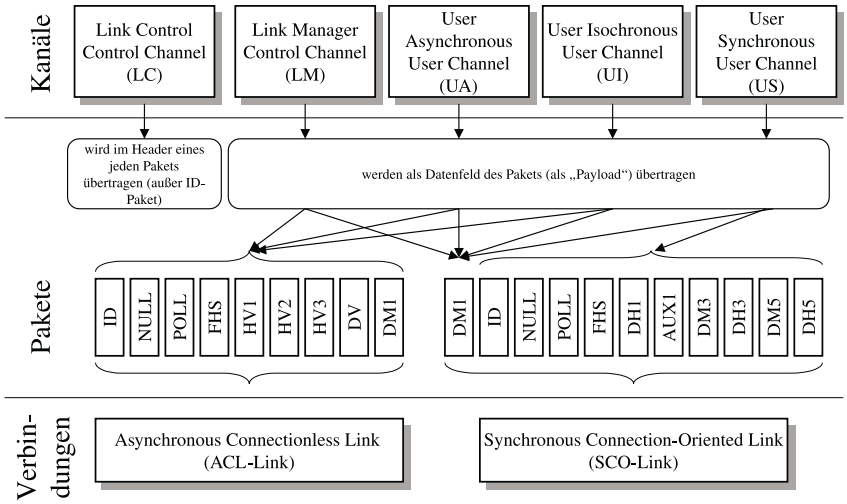


Abbildung 5.3: Zuordnung der unterschiedlichen Typen von Verbindungen, Paketen und Kanälen

Um Missverständnisse zu vermeiden, muss auf eine Schwierigkeit bei der deutschen Formulierung hingewiesen werden. Die englische Sprache besitzt mit den beiden Worten Connection und Link zwei Begriffe, die im Deutschen im Umfeld der Kommunikationstechnik nur sinnvoll mit »Verbindung« übersetzt werden können. Connection bezieht sich allerdings auf die Verbindung, wie sie in Abschnitt 2.2.4 mit den drei Phasen Aufbau, Operation, Abbau beschrieben wurde, während sich Link in Zusammenhang mit Bluetooth auf die Verbindung zwischen Master und Slave bezieht, wie sie nach dem gegenseitigen Anmelden zustande kommt. Ein Link kann also mehrere Connections unterstützen.

- Die synchrone verbindungsorientierte Kommunikation (***S**ynchronous **C**onnection-**O**riented Link* – SCO) realisiert eine symmetrische Punkt-zu-Punkt-Kommunikation zwischen dem Master und genau einem Slave. SCO entspricht funktional einer leitungsvermittelten Übertragung, da der Master in regelmäßigen Abständen Zeitschlitze reserviert. Dies bedeutet, dass der Master in festgelegten Zeitschlitzen Daten an den Slave sendet, wobei der Slave berechtigt ist, in dem jeweils folgenden Zeitschlitz seine Daten abzusetzen. Das Intervall zwischen zwei Übertragungen von Master zu Slave bezeichnet man als T_{SCO}.

  Ein Master kann bis zu drei SCO-Verbindungen zu einem oder mehreren Slaves unterhalten. Ein Slave kann seinerseits bis zu drei SCO-Verbindungen mit einem Master oder maximal zwei SCO-Verbindungen von verschiedenen Masters unterstützen.

  Die SCO-Verbindungen sind darauf ausgelegt, eine effiziente Sprachübertragung zu gewährleisten. Wie in Abschnitt 2.3 dargelegt, ist bei der Übertragung von Sprachinformation ein Datenverlust in einem gewissen

Umfang unkritisch. Sehr viel störender macht sich hingegen die Verzögerung bei der Übertragung bemerkbar. Deswegen findet bei SCO-Verbindungen keine Überprüfung der Datenintegrität statt. Für den Fall, dass Daten bei der Übertragung verloren gehen, findet auch keine erneute Übermittlung statt, weil dies auch eine Verzögerung der folgenden Sprachinformationen bedeuten würde.

- Die asynchrone verbindungslose Kommunikation (***A**synchronous **C**onnectionless Link* – ACL) hingegen stellt eine Verbindung zwischen dem Master und einem oder mehreren Slaves dar, die nur dann erfolgen darf, wenn der Kanal nicht für einen SCO reserviert ist. Eine ACL-Verbindung entspricht einer paketvermittelten Übertragung. Zwischen einem Master und einem Slave darf zu einem Zeitpunkt nur eine ACL-Verbindung aufgebaut sein.

  Im Rahmen der ACL-Verbindungen kann der Master auch Pakete an alle Slaves in seinem Piconetz versenden, indem er keine Zieladresse angibt. Dies wird dann als Broadcast interpretiert. Eine Broadcast-Übertragung von einem Slave wird nicht unterstützt.

  Die ACL-Verbindungen sind im Gegensatz zu den SCO-Verbindungen für eine effiziente Datenübertragung ausgelegt. Bei Übermittlung von Daten spielt die Verzögerung eine meist untergeordnete Rolle, während die Datenintegrität von zentraler Bedeutung ist. Deswegen werden im Rahmen von ACL-Verbindungen fehlerhafte oder fehlende Informationsbestandteile erneut angefordert.

Pakete

In jeder dieser Verbindungsarten stehen verschiedene Pakettypen zur Verfügung, die versendet werden dürfen. Diese sind in Abbildung 5.4 mit den wichtigsten Eigenschaften aufgeführt. Die verschiedenen Typen werden im Feld *Type* des in Abbildung 5.5 gezeigten Paketheaders mit Hilfe von 4 Bits kodiert.

- *Gemeinsame Pakettypen:* Sowohl für asymmetrische als auch für symmetrische Verbindungen stehen mit ID-, NULL-, POLL- und FHS-Paket *gemeinsame Pakettypen* zur Verfügung, die im Wesentlichen zur Verwaltung der Teilnehmerstationen dienen.

- *DM-Pakete* tragen Daten mittlerer Geschwindigkeitsanforderung (***D**ata - **M**edium Rate*). Wie bei den folgenden Pakettypen auch repräsentiert die Zahl 1, 3 oder 5 die Anzahl der Zeitschlitze, die das Paket einnimmt (vgl. Abschnitt 5.5). Das DM1-Paket kann in beiden Verbindungstypen versendet werden und stellt eine Art Basisverbindung dar.

  Insbesondere besteht auch die Möglichkeit, während der synchronen Verbindung Steuerinformationen zu übertragen.

	Type	Payload Header [Bytes]	User Payload [Bytes]	FEC	CRC	Symmetric Max Rate [kbps]	Asymmetric Max Rate [kbps]	
							Forward	Reverse
Link Control Packets	ID	-	-	-	-	-	-	-
	NULL	-	-	-	-	-	-	-
	POLL	-	-	-	-	-	-	-
	FHS	-	-	-	-	-	-	-
ACL Packets	DM1	1	0 .. 17	2/3	ja	108,8	108,8	108,8
	DH1	1	0 .. 27	nein	ja	172,8	172,8	172,8
	DM3	2	0 .. 121	2/3	ja	258,1	387,2	54,4
	DH3	2	0 .. 183	nein	ja	390,4	585,6	86,4
	DM5	2	0 .. 224	2/3	ja	286,7	477,8	36,3
	DH5	2	0 .. 183	nein	ja	433,9	723,2	57,6
	AUX	1	0 .. 29	nein	nein	185,6	185,6	185,6
SCO Packets	HV1	-	10	1/3	nein	64,0	-	-
	HV2	-	20	2/3	nein	64,0	-	-
	HV3	-	30	nein	nein	64,0	-	-
	DV*	1 D	10 V + 0 .. 9 D	nein V '2/3 D	nein (V) ja (D)	64,0 (V) + 57,6 (D)	-	-

* D steht für „Datenfeld“, V für „Voice“

Abbildung 5.4: Die verschiedenen Pakettypen im Bluetooth-Standard, die in verschiedenen Varianten kombiniert werden können.

- *DH-Pakete* tragen Daten hoher Geschwindigkeitsanforderung (***D**ata - **H**igh Rate*). Sie unterscheiden sich von den DM-Paketen lediglich durch den Wegfall der FEC-Redundanz.
- *HV-Pakete* sind vorgesehen für die Übertragung von Sprache (***H**igh Quality **V**oice*) und anderen synchronen und transparenten Diensten.
- *DV-Pakete* setzen sich aus einem Daten- und einem Sprachblock zusammen (***D**ata **V**oice Combined*). Die beiden Bestandteile werden vollständig unabhängig voneinander bearbeitet. Dies bezieht sich auch auf die Fehlerbehandlung durch Kodierung und Redundanzübertragung.

5.3.2 Rahmenformate

Die grundlegende Bitfolge eines Bluetooth-Pakets ist in Abbildung 5.5 mit einigen wesentlichen Kommentaren dargestellt. Von besonderem Interesse erscheinen dabei die Access Codes, mit deren Hilfe die Verwaltung der Stationen im Netzwerk erfolgt.

Das in Abbildung 5.5 nicht gezeigte Nutzdatenfeld (*Payload*) enthält für die symmetrischen Sprachpakete stets 240 Bits und ist deswegen sehr einfach aufgebaut. Die Datenpakete, wie sie bei asymmetrischen ACL-Verbindungen versendet werden, müssen jedoch aufgrund ihrer größeren Flexibilität einem strukturierten Aufbau folgen. Dieser ist in Abbildung 5.6 dargestellt.

Abbildung 5.5: Format der Bluetooth-Pakete

Access Code			Header						Payload
			Link Control (LC) information						
72 b			54 b						0... 2745 b
Pre-amble	**Sync Word**	**Trailer**	**AM_ ADDR**	**Type**	**Flow**	**ARQN**	**SEQN**	**HEC**	
4 b	64 b	4 b	3 b	4 b	1 b	1 b	1 b	8 b	

Es werden drei Access Codes unterschieden:
• CAC Channel Access Code
• DAC Device Access Code
• IAC Inquiry Access Code
  • GIAC General Inquiry Access Code
  • DIAC Dedicated Inquiry Access Code
			Active Member Address	Pakettyp	zur Flusssteuerung bei ACL; wird vom Empfänger auf STOP (=0) gesetzt werden, um dem Sender mitzuteilen, dass die Übertragung zeitweise unterbrochen werden soll.	Acknowledgement Indication. ARQN wird im Header des Antwortpakets übertragen und signalisiert den fehlerfreien Empfang eines Pakets in Bezug auf den CRC-Code.	Sequential Numbering; Bei jedem Paket, das mit CRC übertragen wird, wird SEQN invertiert.	Header Error Check	

Dabei ist zum einen die unterschiedliche Länge der Payload Header in Abhängigkeit von der Anzahl der Zeitschlitze des Pakets zu beachten, die sich unmittelbar aus der zu kodierenden Länge des Pakets ergibt, und zum anderen die Zuordnung zu den logischen Kanälen der höheren Protokollebenen L2CAP und LMP (vgl. Abschnitt 5.2), die für Single-Slot- und Multi-Slot-Payload-Header identisch sind.

Abbildung 5.6: Format des Bluetooth-Datenpakets

8 bit

Payload Header Format für Single-Slot-Pakete

L_CH	Flow	Length
2 b	1 b	5 b
Informationen zum Logical Channel	Flusssteuerung des logischen Kanals	Länge des Datenpakets

16 bit

Payload Header Format für Multiple-Slot-Pakete

L_CH	Flow	Length	undefined
2 b	1 b	9 b	4 b
Informationen zum Logical Channel	Flusssteuerung des logischen Kanals	Länge des Datenpakets	

Code	Logischer Kanal (LC)	Information
00	NA	reserviert
01	UA/UI	weiteres Fragment einer L2CAP-Nachricht
10	UA/UI	Beginn einer L2CAP-Nachricht oder keine Fragmentierung unterstützt
00	LM	LMP-Nachricht

5.3.3 Audioübertragung

Die symmetrische und synchrone Übertragung von Audiodaten ist ein wesentliches Element des Bluetooth-Standards. Da hierbei Telefonanwendungen eine zentrale Rolle spielen, sind auch mehrere CODECs (***Co****dierer* / ***Dec****odierer*) spezifiziert.

- Ein CODEC greift auf eine logarithmische ***P****ulse* ***C****ode* ***M****odulation* (PCM) mit zwei Charakteristika (A-law und µ-law) zurück, wie sie mit einer Datenrate von 64 kbps auch bei der ISDN-Telefonie eingesetzt werden.
- Ein ***C****ontinuous* ***V****ariable* ***D****elta* ***M****odulation* (CVSD) CODEC überträgt die Daten mit Delta-Modulation.

5.4 Zustandssteuerung

5.4.1 Einführung

Besondere Bedeutung besitzt die Verwaltung der Stationen im Bluetooth-Netzwerk, da sich jede Station zu jedem Zeitpunkt in einem definierten Zustand befinden muss, von dem aus die vom Master initiierten Übertragungen im Piconetz angestoßen werden können. Dabei müssen sich die Kommunikationsmechanismen für den Aufbau eines Netzes und die Regeln zur Abwicklung der Kommunikation in einem etablierten Netzwerk wesentlich unterscheiden. Ist ein Piconetz etabliert, ist gleichzeitig auch der Master festgelegt, der den Zugriff auf den Kanal zentral regelt. Hingegen muss während des Aufbaus eines Netzes noch ein dezentraler Zugriffsmechanismus gelten.

Der Link Controller in einer Bluetooth-Station kann die in Abbildung 5.7 gezeigten Zustände einnehmen.

Der Standby-Zustand ist der Ausgangszustand einer jeden Bluetooth-Station nach dem Einschalten, der auch einen Low-Power-Betrieb erlaubt. Der Standby-Zustand wird verlassen,

- um einen empfangenen Page-Aufruf (*Page Scan*) oder einen empfangenen Inquiry-Aufruf (Inquiry-Scan) zu bearbeiten oder
- um selbst einen Page-Aufruf (*Page*) oder einen Inquiry-Aufruf (*Inquiry*) zu versenden.

Nach der erfolgreichen Bearbeitung eines Page-Aufrufs wechselt die Station in den *Connection*-Zustand. Wenn die Station auf einen Page-Aufruf geantwortet hat, so wird sie als Slave betrieben. Hat sie den Page-Aufruf selbst versendet, so übernimmt sie die Rolle des Masters.

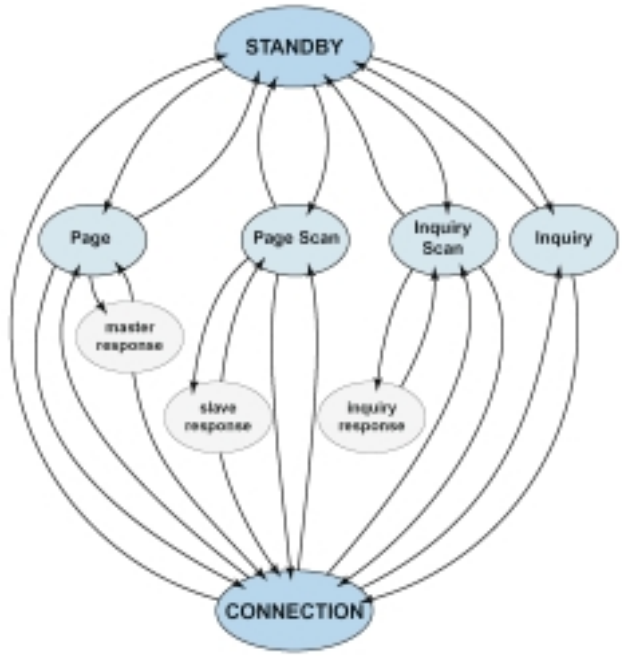


Abbildung 5.7: Zustandsdiagramm eines Bluetooth Link Controllers

5.4.2 Aufbau einer Verbindung

Übersicht

Beim Aufbau einer Verbindung übernehmen *Inquiry* und *Paging* zwei unterschiedliche Aufgaben:

- Mit Hilfe des *Inquiry* können die Stationen herausfinden, welche anderen Stationen mit welchen Adressen und Clock-Zuständen sich im Umkreis ihrer Funkreichweite befinden.
- Das *Paging* dient dazu, eine Verbindung zwischen den Geräten zu etablieren.

Jede eingeschaltete Station versendet in regelmäßigen Zeitabständen Anfragen an die Umgebung und hört den Kanal in den Zeiten zwischen zwei eigenen Anfragen auf Anfragen anderer Stationen ab.

Inquiry

Eine Bluetooth-Station, die Informationen über weitere Stationen in ihrer Umgebung erhalten möchte, versendet eine Inquiry-Message. Dabei handelt es sich um ein ID-Paket, das

- entweder einen ***G**eneral **I**nquiry **A**ccess **C**ode* (GIAC) enthält, wenn alle vorhandenen Stationen antworten sollen,

- oder einen ***D**edicated **I**nquiry **A**ccess **C**ode* (DIAC) mit der Nummer einer bestimmten Geräteklasse enthält, wenn nur bestimmte Typen von Geräten antworten sollen.

Empfängt eine Station eine Inquiry-Anfrage, so wechselt sie in den Inquiry-Scan-Zustand, in dem sie mit einem FHS-Paket mit seiner Geräte-Adresse (*Device ID*) antwortet. Dabei existiert nur die Möglichkeit, als Slave eine Inquiry zu beantworten. Die Station, die die Inquiry-Anfragen versendet, übernimmt die Rolle des Masters. Wenn dieser die Inquiry-Antwort erhält, trägt er sie in eine Liste ein. Er versendet allerdings keine Bestätigung an den Slave. Dies ist deswegen wichtig, weil es bei der Beantwortung einer Inquiry-Anfrage durchaus vorkommen kann, dass mehrere Slaves gleichzeitig oder annähernd gleichzeitig antworten. Schließlich ist das Piconetz noch nicht etabliert, die Stationen sind demnach noch nicht synchronisiert und die Verwaltung des Kanalzugriffs wird noch nicht vom Master übernommen. Allerdings setzt auch Bluetooth einen zufallsbasierten Backoff-Algorithmus ein, der mit den Algorithmen des IEEE802.x durchaus vergleichbar ist, um die Wahrscheinlichkeit von gleichzeitigen Inquiry-Antworten zu minimieren. Für den Fall einer Kollision gehen die Inquiry-Antworten beider Slaves verloren. Entsprechend können diese dann erst auf die nächste Inquiry-Anfrage antworten.

Eine weitere Problematik bei der Organisation des Inquiry-Algorithmus besteht darin, dass die Stationen

- sich gegenseitig noch nicht kennen. Insbesondere sind die Geräte-Identifikationsnummern noch nicht bekannt, die die Grundlage für die Berechnung der Frequenzsprünge darstellen. Deswegen wird für die Inquiry-Anfrage eine feste Sprungfolge *Inquiry* und für die Antwort eine weitere feste Sprungfolge *Inquiry-Response* verwendet.
- noch nicht synchroniert sind und dass deswegen auch die Nutzung von vordefinierten Frequenzsprungfolgen noch nicht gewährleistet, dass sich die Stationen auch tatsächlich verstehen.

Bluetooth-Stationen führen den in Abbildung 5.8 dargestellten Inquiry-Vorgang so lange fort, bis sie eine vordefinierte Anzahl von weiteren Stationen detektiert haben oder bis eine voreingestellte Zeit verstrichen ist.

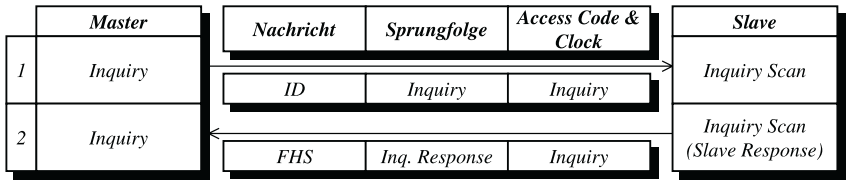


Abbildung 5.8: Inquiry-Algorithmus von Bluetooth-Stationen

Paging

Der Page-Zustand wird vom Master genutzt, um eine Verbindung mit einem Slave aufzubauen. Dabei versucht der Master den Slave anzusprechen, in dem er wiederholt seinen ***D**evice **A**ccess **C**ode* (DAC) versendet. Den Slave kann er allerdings nur dann erreichen, wenn sich dieser im Zustand *Page Scan* befindet, den er regelmäßig einnimmt. Allerdings sind dem Master weder Zeitpunkt noch Frequenzsprungfolge bekannt, in dem/der der Slave »aufwacht«. Deswegen folgt der Master einem ausgeklügelten Algorithmus, um mit möglichst wenig Versuchen vom Slave empfangen zu werden.

Nach dem erfolgreichen Empfang einer Page-Anfrage sendet der Slave eine Page Response zurück, die der Master seinerseits mit einer FHS-Nachricht beantwortet. Diese Nachricht enthält insbesondere Informationen über die *Device ID* des Masters – aus der dann die Frequenzsprungfolge für die spätere Übertragung abgeleitet wird – und den Clockzustand. Nach der erneuten Bestätigung durch den Slave im Rahmen einer erneuten Page Response kann die Übertragung beginnen. Nachdem während der Phase des Verbindungsaufbaus die Kommunikation zwischen Master und Slave mit den Clockzustand und dem Access Code des Slave durchgeführt wurde, findet die Übertragung nun nach den Vorgaben des Masters statt. Der Ablauf ist in Abbildung 5.9 in Form einer Übersicht dargestellt.

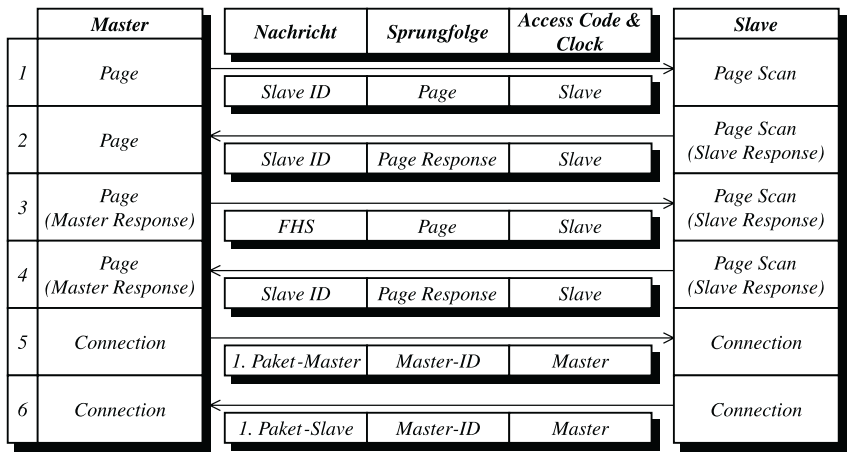


Abbildung 5.9: Page-Algorithmus von Bluetooth-Stationen

5.4.3 Betrieb einer Verbindung

Nach dem erfolgreichen Abschluss des Verbindungsaufbaus im Rahmen des Paging nehmen sowohl Master als auch Slave-Station den Zustand *Connection* ein. Dieser unterteilt sich für die Slaves seinerseits in die in Abbildung 5.10 gezeigten Modi. Diese werden zum einen dazu eingesetzt, um die Stromaufnahme der Geräte so gering wie möglich zu halten. Zum anderen erlauben sie aber auch den Aufbau komplexerer Netzwerke im Sinne von Scatternetzen.

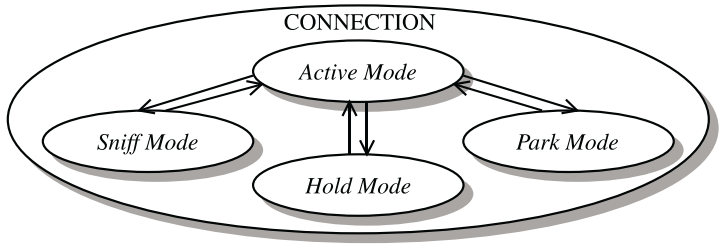


Abbildung 5.10: Zustände eines Bluetooth-Controllers beim Betrieb einer Verbindung

Active Mode

Im aktiven Modus nutzen Master und Slave aktiv den Übertragungskanal. Aktive Slaves erwarten in den geradzahligen Master-Slots Pakete vom Master. Falls der Master kein Paket sendet oder ein Paket an einen anderen Slave sendet, darf der Slave bis zum Beginn der nächsten möglichen Übertragung durch den Master schlafen. Insbesondere kann der Slave aufgrund der Informationen aus dem Steuerteil auch ablesen, wenn der Master ein Paket versendet, das drei oder fünf Slots einnimmt. Dann erwartet der Slave die nächste Übertragung durch den Master vier bzw. sechs Slots später.

Sniff Mode

Im Schnüffelmodus wird die Häufigkeit reduziert, mit der der Slave bereit ist, Pakete von einem Master zu empfangen. Da der Master den Slave somit nicht mehr in allen beliebigen Master-Slots ansprechen kann, muss das Zeitintervall T_{sniff}, nach dem der Slave periodisch zum Empfang bereit ist, zwischen Master und Slave abgesprochen werden. Hierzu senden entweder Master oder Slave einen Schnüffelbefehl im Rahmen des LM-Protokolls aus.

Nach dem Ablauf von T_{sniff} lauscht der Slave für eine bestimmte Anzahl $N_{sniff\ attempt}$ von Slots auf Pakete vom Master. Empfängt er in dieser Zeit keine an ihn adressierten Pakete, legt er sich wiederum für T_{sniff} schlafen. Detektiert er jedoch ein Paket mit der übereinstimmenden Adresse, dann ist er bereit, auch in der unmittelbaren Folge weitere Pakete zu empfangen. Es ist also nicht möglich, dass ein Slave während der Übertragung im Schnüffelmodus beginnt einzuschlafen.

Der Schnüffelmodus lässt sich aber auch dazu nutzen, in einem Zeitmultiplex im Rahmen eines Scatternetzes an zwei Piconetzen teilzunehmen.

Hold Mode

Für längere Zeitabschnitte, in denen der Slave nicht an der ACL-gestützten Kommunikation teilnehmen soll, kann der Slave einen Haltezustand annehmen. Dabei behält er die Parameter der Verbindung, insbesondere auch die Adressen (***A**ctive **M**ember **Addr**ess* - AM_ADDR) und die Synchronisationsinformationen. In diesem Halte-Zustand müssen aber mögliche SCO-Pakete weiterhin empfangen werden können.

Park Mode

Im geparkten Modus nimmt der Slave überhaupt nicht mehr an der Kommunikation im Piconetz teil. Hierzu erhält er zwei Adressen, unter denen er weiterhin vom Master angesprochen werden kann, um aus dem Parkzustand wieder aufzuwachen. Alle Slaves, die sich im geparkten Modus befinden, erhalten zum einen die ***P**arked **M**ember **Addr**ess* (PM_ADDR), die aus acht Nullen besteht und die entsprechend als Broadcast-Adresse eingesetzt wird. Zum anderen kann der Slave den Parkmodus mit Hilfe der ***A**ccess **R**equest **Addr**ess* (AR_ADDR) verlassen.

Im Parkzustand wacht ein Slave in regelmäßigen Zeitabständen auf, um sich zu synchronisieren und den Kanal auf Broadcast-Nachrichten abzuhören. Für die Kommunikation mit den geparkten Slaves verwendet der Master eine spezielle Struktur von Beacons.

Der Parkzustand erlaubt sowohl die Verringerung der Energieaufnahme beim Slave als auch die Aufnahme von mehr als sieben Slaves in ein Piconetz.

5.4.4 Adressierung

Im Rahmen des Bluetooth-Standards treten Adressen auf mehreren Ebenen auf.

- Die 48 Bit lange ***B**luetooth **D**evice **Addr**ess* (BD_ADDR) wird den Geräten nach dem im IEEE802 beschrieben Muster fest vergeben.
- Die aktiven Slaves in einem Piconetz erhalten für die Dauer ihrer Zugehörigkeit eine drei Bit lange ***A**ctive **M**ember **Addr**ess* (AM_ADDR). Dabei wird die Nulladresse zum Broadcast eingesetzt. Auf diese Weise können Broadcast-Nachrichten in einem Piconetz an alle Teilnehmer versendet werden. Insbesondere werden sie auch von den geparkten Stationen empfangen.
- Die ***P**arked **M**ember **Addr**ess* (PM_ADDR) und die ***A**ccess **R**equest **Addr**ess* (AR_ADDR) werden für die Behandlung des Parkzustands, wie in Abschnitt 5.4.3 beschrieben, eingesetzt.
- Darüber hinaus finden im Bluetooth-System noch Access Codes Anwendung, die den ersten Abschnitt des in Abbildung 5.5 gezeigten Rahmens bilden und die teilweise aus den Adressen abgeleitet werden.

5.5 Bitübertragung

Auch der Bluetooth-Standard ist für den Einsatz im 2,4 GHz-ISM-Band ausgelegt und muss entsprechend der Vorschrift ein Frequenzspreizverfahren nutzen. Dabei wird das Frequenzsprung-Spread-Spectrum-Verfahren (FHSS) eingesetzt, das einfacher und preiswerter zu realisieren ist. In der Version 1.x limitiert dies allerdings die Datenrate auf 1 Mbps.

Dabei muss – wie bereits beim IEEE802.11-Standard (vgl. Abschnitt 4.4) – Rücksicht auf die regionalen Restriktionen genommen werden. Der Aufwand wird gering gehalten, indem nur zwei Betriebsmodi unterschieden werden: Ein Modus mit 79 Sprungfrequenzen steht für Nordamerika und Europa zur Verfügung, ein zweiter Modus mit 23 Sprungfrequenzen wurde für Japan, Frankreich und Spanien definiert.

Die Frequenzfolge wird im etablierten Piconetz vom Master vorgegeben und folgt einer Pseudozufallsfolge, die in Abhängigkeit von der Geräteadresse des Masters nach vergleichsweise aufwändigen Regeln berechnet wird und somit in jedem Piconetz unterschiedlich ist. Auf diese Weise soll der Betrieb von möglichst vielen unabhängigen Piconetzen mit hoher räumlicher Dichte unterstützt werden.

Die nominale Sprungrate beträgt 1600 Hops/s. Hierzu gibt der Master allen Slaves im Piconetz Zeitschlitze mit einer Länge von 625 µs vor, wobei eine Übertragung von allen Teilnehmern nur zu Beginn eines Zeitschlitzes gestartet werden darf. Die Zeitschlitze werden in Abhängigkeit von der Clock des Masters von 0 bis 2^{27}-1 durchgezählt, so dass sich eine Zykluszeit der Zählung von etwa 23 h ergibt.

Zur Unterstützung von bidirektionalem Verkehr wird ein ***T**ime **D**ivision **D**uplex*-(TDD-)Verfahren eingesetzt, bei dem der Master seine Übertragung nur zu Beginn eines geradzahligen Zeitschlitzes, die Slaves nur zu Beginn von ungeradzahligen Zeitschlitzen beginnen dürfen, wie dies in Abbildung 5.11 dargestellt ist.

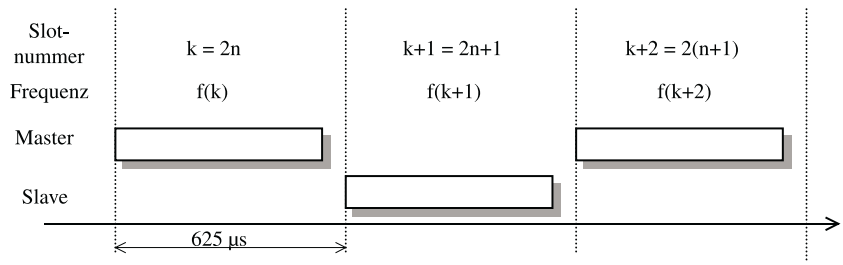


Abbildung 5.11: Zeitmultiplex zwischen Downlink und Uplink

Aufeinander folgende Pakete werden auf verschiedenen Frequenzen übertragen. Im normalen Modus wird mit dem Beginn eines jeden neuen Zeitschlitzes ein Frequenzsprung durchgeführt. Bei der Übertragung von Paketen, die drei oder fünf Zeitschlitze einnehmen, wird die Frequenz bis zur vollständigen Übertragung des Pakets festgehalten. Das folgende Paket wird danach mit der Frequenz übertragen, die dem Zustand der Clock entspricht. Dieser Wechsel ist in Abbildung 5.12 gezeigt.

Aus dieser Zykluszeit lassen sich auch unmittelbar die Anforderungen für eine isochrone Sprachübertragung ableiten. Ein Paket vom Typ HV1 enthält 10 Bytes = 80 Bit Nutzdaten. Ausgehend von einer geforderten Datenrate von 64 kbps für eine Sprachübertragung in ISDN-Qualität können in einem HV1-Paket 1,25 ms Sprache übertragen werden.

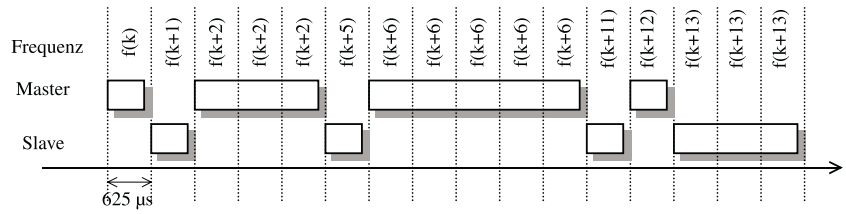


Abbildung 5.12: Übertragung von Paketen mit einer Zeitdauer von mehreren Slots

Legt man nun die Zeitschlitzperiode von 625 µs zu Grunde, ergibt sich, dass in jedem zweiten Zeitschlitz ein zugehöriges HV1-Paket gesendet werden muss. Dies bezeichnet man als $T_{SCO} = 2$. Geht man nun noch von einer symmetrischen Übertragung aus, bei der auch der Rückkanal mit einer Datenrate von 64 kbps übertragen werden soll, so ist ein Kanal komplett belegt. Dieses Beispiel zeigt sehr eindrucksvoll, wie gering die Leistungsfähigkeit eines Kanals ist, der eine Bruttodatenrate von 1 Mbps aufweist. Die Übertragungseffizienz liegt in diesem Fall bei 12,8 % (=128 kbps / 1 Mbps).

5.6 Sicherheit

Zur Gewährleistung der bei drahtlosen Systemen notwendigen Sicherheitsvorkehrungen stehen bei Bluetooth ähnliche Verfahren wie bei IEEE802.11 zur Verfügung. Insbesondere unterscheidet man die drei im Folgenden beschriebenen Stufen:

- Die 48 Bit lange Bluetooth Device Address (BD_ADDR) entspricht der MAC-Adresse, die vom IEEE802 herausgegeben wird. Diese für jede Station eindeutige Adresse ist öffentlich bekannt. Schließlich wird aus ihr im Falle eines Betriebs als Master ja auch die Frequenzsprungfolge berechnet, die im Piconetz zum Einsatz kommt.
- Auf der nächsten Stufe wird ein 128 Bit langer Schlüssel zur Authentifizierung der Stationen (*Authentication Key*) eingesetzt.
- Zum Schutz der übertragenen Informationen wird ebenfalls ein Schlüssel eingesetzt. Um aber auch hier wieder die Herstellung möglichst kostengünstiger Systeme zu erlauben, kann die Länge des Schlüssels von 8 Bit bis 128 Bit variieren. Dabei lässt sich der *Encryption Key* aus dem Authentifizierungsschlüssel herleiten.

Die Mechanismen bei der Anmeldung und der Verschlüsselung verlaufen ähnlich wie bei IEEE802.11.

5.7 Systemimplementierung

Die Frage nach der Systemimplementierung ist bei Bluetooth im Vergleich zu den anderen in diesem Buch beschriebenen Technologien am bedeutendsten, weil die höheren Protokollebenen am weitesten einbezogen wurden. Dabei lässt sich die Partitionierung der Bluetooth-Implementierung entlang des Kommunikationspfads aufteilen. Die wesentlichen Bestandteile ergeben sich recht unmittelbar aus dem in Abbildung 5.1 gezeigten Protokollstapel:

- HF-Teil mit Antenne, Transceiver und Modem
- Low-Level-Basisbandcontroller mit Basisbandverarbeitung, Verbindungssteuerung und -management bis zum Host Controller Interface (HCI). Für die Erfüllung der Basisbandverarbeitung wird typischerweise ein 32 Bit-Mikroprozessor eingesetzt. Eine verbreitete Plattform auch in diesem Zusammenhang stellt der ARM7TDMI-Prozessor dar [Bläsner 2001 (1)].
- Protokollstapel der höheren Ebenen
- Anwendungssoftware

Diese Bestandteile lassen sich nunmehr in verschiedenen Systemkonfigurationen sinnvoll zusammenfassen. Dabei sind zwei wesentliche Anwendungsszenarien zu unterscheiden, die in Abbildung 5.13 dargestellt sind.

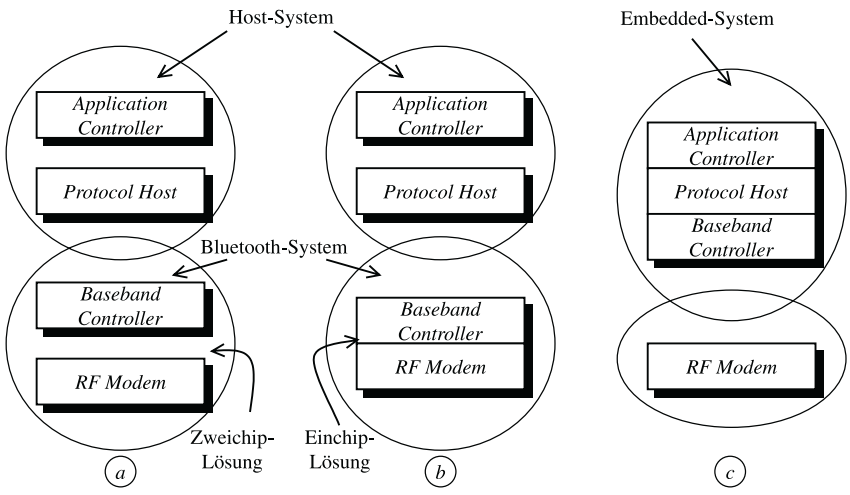


Abbildung 5.13: Systemkonfigurationen eines Bluetooth-Moduls

- Bei Host-gestützten Anwendungen wird nur die Kommunikationsfunktionalität (die Ebenen 1 und 2 im Referenzmodell) vom Bluetooth-Modul erbracht, während die anwendungsbezogene Funktionalität flexibel per Software auf dem Host ausgeführt werden kann. Dabei kann der Einsatz einer kostengünstigen Einchip-Lösung sinnvoll sein (Konstella-

tion *b*), wenn keine besonderen Anforderungen an das RF-Modul gestellt werden und eine monolithische Integration in kostengünstigen CMOS-basierten Prozessen möglich ist [Sikora 2001 (5)]. Ist dies der Fall, muss für absehbare Zeit der Zweichip-Lösung (Konstellation *a*) der Vorrang gegeben werden.

- Bei der Implementierung in einem Embedded System, das nur für eine Anwendung oder für eine begrenzte Anzahl von verwendeten Anwendungen ausgerichtet ist, bietet sich die Zusammenfassung dieser gesamten Funktionalität in einem Chip an, der im Allgemeinen aber dann nicht mehr in der Lage ist, auch noch die RF-Komponenten mit aufzunehmen. Es ergibt sich die Konstellation *c*.

  Für diese Konstellation ist der Einsatz von vorgefertigten Entwurfsblöcken im Sinne von IP (***I****ntellectual* ***P****roperty*) sinnvoll.

6 DECT

6.1 Standard

Seit 1992 der DECT-Standard ETS 300 175 für ***D**igital **E**uropean **C**ordless **T**elecommunications* vom Europäischen Standardisierungsinstitut für Telekommunikation (ETSI) festgelegt wurde, haben sich vor allem die drahtlosen Telefone im Haus- und Firmenbereich sehr stark in mehr als 100 Ländern, darunter fast allen wichtigen Industrienationen verbreitet. Die europäische Entwicklung eines digitalen, abhörsicheren, stabilen und komfortablen Protokollstandards für die lokale Anbindung von tragbaren Sprachtelefonen an eine ortsfeste Basisstation war und ist ein voller Erfolg. Als Alternative hat sich in Japan und einigen anderen ostasiatischen Staaten das ***P**ersonal **H**andy-Phone **S**ystem* (PHS) etablieren können, das jedoch sehr viele Gemeinsamkeiten aufweist.

Die außerordentlich erfolgreiche Markteinführung mit geschätzten Stückzahlen von weltweit 38 Mio. im Jahr 2001 (*www.dectweb.com/Introduction/market_statistics.htm*) und einer kumulierten installierten Basis von etwa 100 Mio. Stück verschafft DECT den immensen Vorteil der bereits zahlreich und vergleichsweise kostengünstig verfügbaren Funkmodule. Die weitere Vorwärtsintegration [Hascher 1999] sowie neue Techniken im HF-Modul [Bläsner 2000 (2)] versprechen weitere Kostensenkungen.

Um untereinander kompatible DECT-Datenprodukte zu etablieren, haben sich auf dem DECT-Weltkongress 1999 in Barcelona die Firmen Ascom, Canon, Dosch & Amand, Ericsson, Hagenuk und National Semiconductor zum DECT-Multimedia-Consortium (DECT-MMC) (*www.dect-mmc.com*) zusammengeschlossen. Mittlerweile haben sich weitere Unternehmen der Initiative angeschlossen.

Weitere grundlegende Informationen und Hinweise finden sich im DECT-Web (*http://www.dectweb.com*) und beim DECT-Forum (*www.dect.ch*). Ein allgemeiner Überblick über die DECT-Technologien ist in [Sikora2001 (2)] verfügbar.

6.2 Architekturen

DECT ist für die Punkt-zu-Punkt-Verbindung zwischen einer Basisstation (***F**ixed **P**art* - FP) und einem Mobilteil (***P**ortable **P**art* - PP) ausgelegt. Dabei kann eine Basisstation den Verkehr mehrerer Mobilteile mit dem Festnetz

oder auch untereinander abwickeln. Darüber hinaus ist auch die Verschaltung mehrerer Basisstationen möglich, um Roaming und Handover zu unterstützen.

6.3 Kanalzugriff

Die Verteilung der Frequenzen für die verschiedenen Kanäle innerhalb dieses Frequenzbands folgt einem MC/TDMA/TDD-Algorithmus. Dies bedeutet:

- ***M**ulti **C**arrier* (MC): dass mehrere Trägerfrequenzen im Sinne eines Frequenzmultiplex zur Verfügung stehen (vgl. Abschnitt 2.6.3),
- ***T**ime **D**ivision **M**ultiple **A**ccess* (TDMA): dass innerhalb einer Trägerfrequenz mehrere Zeitschlitze für die verschiedenen Kanäle nacheinander vergleichbar mit einem üblichen Zeitmultiplex genutzt werden können (vgl. Abschnitt 2.6.2),
- ***T**ime **D**ivision **D**uplex* (TDD): dass die Downlink-Übertragung zwischen Basisstation und Mobilteil und die Uplink-Übertragung zwischen Mobilteil und Basisstation ebenfalls auf einer Trägerfrequenz in verschiedenen Zeitschlitzen gemultiplext übertragen werden (vgl. Abschnitt 2.6.2).

Abbildung 6.1: Frequenz-Zeit-Spektrum bei DECT

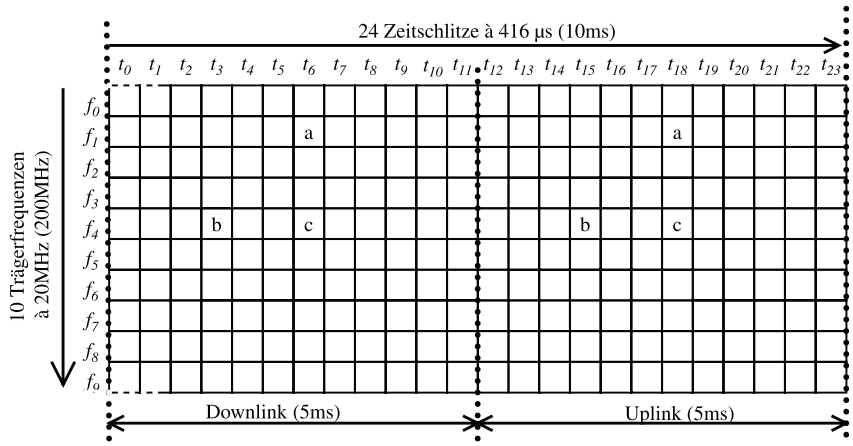


Abbildung 6.1 zeigt das Frequenz-Zeit-Spektrum von DECT. Es stehen auf zehn verschiedenen Trägerfrequenzen 24 Zeitschlitze mit einer gesamten Periodendauer von 10 ms zur Verfügung. Jeweils zwölf dieser Zeitschlitze werden für die Downlink-Übertragung von der Basisstation zum Mobilteil und jeweils zwölf für die Uplink-Verbindung vom Mobilteil zur Basisstation genutzt. In Abbildung 6.1 sind gerade drei Übertragungen aktiv:

- Verbindung **a** nutzt den jeweils siebten Zeitschlitz (t_6 für Downlink und t_{18} für Uplink) auf der zweiten Trägerfrequenz (f_1),
- Verbindung **b** nutzt den jeweils vierten Zeitschlitz (t_3 für Downlink und t_{14} für Uplink) auf der fünften Trägerfrequenz (f_4) und
- Verbindung **c** nutzt den jeweils siebten Zeitschlitz (t_6 für Downlink und t_{18} für Uplink) auf der fünften Trägerfrequenz (f_1).

Insgesamt gibt es also 120 Kanäle, die innerhalb einer Funkzelle vollkommen störungsfrei parallel betrieben werden können. Die Bandbreite eines Kanals beträgt dabei 32 Kbps für die ADPCM-kodierte Übertragung von Sprache. Insgesamt steht, unter Berücksichtigung der in Abbildung 6.1 nicht eingetragenen Steuer-Zeitschlitze, eine Bandbreite von 522 Kbps pro Trägerfrequenz und Übertragungsrichtung zur Verfügung.

6.4 Bitübertragung

DECT arbeitet in einem reservierten Frequenzbereich, der in Europa zwischen 1,88 und 1,9 GHz liegt. Auf anderen Kontinenten werden teilweise auch andere Frequenzbereiche von 1,5 GHz bis zu 3,6 GHz verwendet, wobei in einigen wenigen Fällen auch auf das öffentlich freigegebene 2,4 GHz-ISM-Band (vgl. Abschnitt 2.11) zurückgegriffen wird. Die DECT-Technologien, die in diesen höheren Frequenzbereichen eingesetzt werden, bezeichnet man auch als *Upbanded DECT*.

Die Auswahl des jeweiligen Übertragungskanals übernimmt die Basisstation, indem sie in einem Hintergrundprozess in bestimmten Zeitabständen die Aktivitäten aller Kanäle in ihrem Empfangsbereich auswertet. Die freien Kanäle werden dann gemäß der ermittelten Aktivität in der RSSI-Liste (***R**eceived **S**ignal **S**trength **I**ndication*) abgelegt, so dass bei der Aufforderung, eine neue Verbindung aufzubauen, die Basisstation den für sie optimalen, d.h. am wenigsten gestörten Kanal auswählen kann.

Das DECT-Mobilteil seinerseits überprüft ebenfalls kontinuierlich die Aktivitäten in den zugehörigen Frequenzbereichen und stellt fest, ob die Signale von einer Basisstation stammen, bei der sich das Mobilteil anmelden darf. Das Mobilteil meldet sich dann bei der Basisstation mit der höchsten Signalleistung an, bei der es Anmelderechte besitzt.

Da diese Überprüfungen dynamisch auch während der Übertragung durchgeführt werden (*Dynamic Channel Allocation and Selection*), kann flexibel auf Störereignisse oder Ortswechsel reagiert werden. So kann zum Beispiel auch ein so genanntes Handover eines sich bewegenden Mobilteils von einer Basisstation zu einer anderen Basisstation bei voller Aufrechterhaltung der Verbindung durchgeführt werden, wenn die beiden Basisstationen die Anmeldung erlauben und entsprechend verbunden sind (*Intercell Handover*). Darüber hinaus kann ein Mobilteil auch bei Aufrechterhaltung der Verbindung innerhalb einer Funkzelle den Kanal wechseln, wenn der bislang

benutzte Kanal durch ein neu auftretendes Ereignis gestört wird (*Intracell Handover*). Eine solche Notwendigkeit kann zum Beispiel auftreten, wenn sich ein Mobilteil in einer Funkzelle während der Übertragung einer zweiten Funkzelle nähert, in der im gleichen Kanal kommuniziert wird.

6.5 Anwendungsprofile

6.5.1 Sprachtelefonie

Auf der Grundlage des oben erläuterten Standards wurden zahlreiche weitere anwendungsbezogene Standards entwickelt, die den Anwendungsbereich von DECT insbesondere im Bereich der Sprachtelefonie erweitert haben.

- Das herstellerübergreifende Zugangsprofil (***G**eneric **A**ccess **P**rofile* - GAP – ETS 300 444) garantiert die Interoperabilität zwischen den Basisstationen und Mobilteilen verschiedener Hersteller für Sprachanwendungen.
- Das *DECT/**G**SM **I**nterworking **P**rofile* (GIP – ETS 300 370) erlaubt die Kopplung von verschiedenen, auch räumlich getrennten DECT-Domänen durch die Nutzung von GSM-Mobilitätsfunktionen.
- Das *DECT **R**adio Local Loop **A**ccess **P**rofile* (RAP – ETS 300 765) beschreibt die Realisierung von öffentlichen Funknetzen zur Anbindung von Endkunden mit Hilfe von DECT, um den Wettbewerb auch beim direkten Kundenanschluss mit vergleichsweise geringen Kosten zu erhöhen. Zahlreiche Feldversuche auch in Deutschland sowie erste Installationen in verschiedenen Ländern, unter anderem in Italien und in Polen, haben die technische Realisierbarkeit gezeigt. Die Wirtschaftlichkeit ist jedoch in hohem Maße von der jeweiligen regulatorischen Situation und der Wettbewerbssituation abhängig.

6.5.2 Datenverkehr

Während die im vorherigen Abschnitt aufgeführten Profile im Wesentlichen auf die erweiterte Funktionalität von Sprachtelefonienetzen ausgerichtet sind, konnten im vergangenen Jahr in zwei weiteren Standards Profile für Multimedia- und Netzwerkanwendungen von der ETSI verabschiedet werden.

- Der ***D**ECT **P**acket **R**adio **S**ervice* (DPRS – ETS 301 649) ergänzt den DECT-Standard um die für paketorientierte Datenübertragung wichtigen Dienste. Hierzu gehören insbesondere:
  - die Verhandlung und Garantie von bestimmten Dienstgüten (***S**ervice **N**egotiation* - SN) sowie

- die dynamische Ressourcenzuteilung (***D**ynamic **R**esource **M**anagement* - DRM), um büschelartiges Verkehrsaufkommen effizient handhaben zu können. DRM erlaubt auch die Bündelung von mehreren Kanälen, um die für Multimedia-Anwendungen benötigten höheren Bandbreiten realisieren zu können. Dabei werden in der ersten Stufe die Zeitschlitze einer Trägerfrequenz zusammengefasst. Da Datenverkehr in den meisten Fällen eine asymmetrische Verkehrscharakteristik aufweist, erscheint es sinnvoll, beide Zeitschlitze der Duplexübertragung für eine Übertragungsrichtung zu nutzen, so dass pro Trägerfrequenz Bandbreiten von bis zu 1 Mbps zur Verfügung stehen. Durch die zusätzliche zeitgleiche Nutzung der zehn Trägerfrequenzen können theoretisch alle 120 Übertragungskanäle parallel eingesetzt werden. DRM strebt somit eine Bandbreite innerhalb einer Zelle von bis zu 20 Mbps an.

  Die Bezeichnung DPRS ist bewusst an die ***G**eneral **P**acket **R**adio **S**ervice* (GPRS)-Erweiterung von GSM-Mobilfunknetzen angelehnt, da die Vorgehensweise der Bündelung der Zeitschlitze identisch ist.

- Das ***D**ECT **M**ultimedia **A**ccess **P**rofile* (DMAP – ETS 301 650), das auf dem ***M**ulti**m**edia **A**ccess **P**rofile* (MMAP[8]) von Dosch & Amand basiert, bietet Datendienste mit zusätzlichen Mehrwertdiensten. DMAP basiert auf den bereits erwähnten Standards GAP und DPRS, schließt aber auch zusätzliche Dienste wie ***D**irect **L**ink **A**ccess* (DLA) für Ad-hoc-Netzwerkverbindungen ein.

7 HomeRF

7.1 Standard

Der HomeRF-Standard wurde als offener Firmenstandard von der ***Home Radio Frequency Working Group*** (HomeRF WG) erarbeitet, die im März 1998 von Compaq, Hewlett-Packard, IBM, Intel und Microsoft gegründet wurde. Im Sommer 2001 waren etwa fünfzig Firmen als Mitglieder eingetragen. Die innere Gruppe der HomeRF »Promoters« umfasst mittlerweile die Firmen Siemens, Compaq, Motorola, National Semiconductor und Proxim. Die Homepage der Gruppe kann man unter *http://www.homerf.org* besuchen. Der Standard ist nicht öffentlich verfügbar.

Der HomeRF-Standard liegt gegenwärtig in zwei Versionen mit praktischer Relevanz vor, die in Tabelle 7.1 dargestellt sind.

Version	Bandbreite	Status
V1.2	1,6 Mbps	2000
V2.0	10 Mbps	Mai 2001
V2.1	20 Mbps	In Vorbereitung für 2002

Tab. 7.1: Versionen des HomeRF-Firmenstandards

Wie der Name bereits signalisiert, ist HomeRF primär auf die Vernetzung von privaten Haushalten ausgerichtet. Mit der Verabschiedung des HomeRF2.0-Standards werden aber nunmehr auch kleinere Firmennetzwerke adressiert, da neben der höheren Geschwindigkeit auch der mobile Wechsel der Stationen zwischen den Funkzellen (*Roaming*) unterstützt wird. HomeRF unterstützt insbesondere die Anforderungen der unterschiedlichen Verkehrsströme bei nunmehr vergleichbaren Datenraten.

Auf der logischen Ebene vereint HomeRF die DECT-Technologie für den Sprachverkehr und Ethernet-ähnlichen Kanalzugriff für den Datenverkehr. Darüber hinaus steht noch ein dritter Verkehrstyp für Multimedia-Daten zur Verfügung.

Während der Ausarbeitung der Regeln findet sich gelegentlich auch die Bezeichnung DECTplus [Tourrilhes (2)].

HomeRF wird von Proxim auch als Migrationstechnologie für Geräte eingesetzt, die ursprünglich der OpenAir-Spezifikation folgten, für die sich keine weiteren Befürworter gefunden haben [Frost 1999].

7.2 Architekturen

7.2.1 Systemarchitektur

In der HomeRF-Sprachregelung erhalten die Stationen, die als Datenquellen oder -senken fungieren, die Bezeichnung Knoten (*Nodes*). Dabei werden in Abhängigkeit von den Verkehrsanforderungen der Stationen bestimmte Klassen von Knoten mit identischen Bedürfnissen gebildet.

HomeRF-Netzwerke erlauben die gleichen Netzwerkarchitekturen wie 802.11. Das heißt, dass sowohl die Kommunikation von Knoten untereinander als auch zwischen einer Zentrale (***C**entral **P**oint*, manchmal auch ***C**onnection **P**oint* – CP) und mehreren Knoten unterstützt wird. Darüber hinaus wird seit HomeRF 2.0 auch das Roaming der Knoten aus der Funkzelle einer Zentrale in die einer anderen Zentrale unterstützt.

Bei den Knoten unterscheidet man unterschiedliche Klassen, die die in Abschnitt 2.3.1 aufgeführten Verkehrstypen widerspiegeln:

- Asynchrone Knoten (A-Node) unterstützen Verkehr mit der klassischen Datencharakteristik. Anwendungen stellen z.B. Laptops dar.
- Synchrone Knoten (S-Node) erlauben die Übertragung von konstanten Datenströmen (*Streaming Data*), wie sie z.B. für ein Audio Headset benötigt werden.
- Isochrone Knoten (I-Node) gewährleisten bidirektionalen Verkehr im Sinne der klassischen Sprachtelefonie.

Darüber hinaus können Stationen auch mehrere Verkehrscharakteristiken aufweisen. Hierdurch wird der Konvergenz im Bereich der Endgeräte im Sinne von Internet Appliances Rechnung getragen. So kann beispielsweise ein Webpad sowohl klassischen Datenverkehr als auch konstante Datenströme erhalten.

7.2.2 Protokollarchitektur

Der HomeRF-Standard beschreibt die beiden unteren Schichten des Referenzmodells (vgl. Abbildung 7.1). Diese sind aber insbesondere ausgelegt für bereits existierende Protokolle der darüber liegenden Schichten. Dabei sind vor allem drei Verkehrsströme antizipiert:

- Der Datenpfad *(»Ethernet« Data Path*) ist für den klassischen Datenverkehr in digitalen Netzwerken ausgelegt. Insbesondere ist der Zugriff durch das verbindungsorientierte TCP/IP-Protokoll vorgesehen. Der Datenpfad selbst verwendet einen verbindungslosen CSMA/CA-Zugriff, der dem des IEEE802.11 sehr ähnlich ist. Der Datenpfad wird für die Anbindung von asynchronen Knoten genutzt.

- Der Medienpfad (*Streaming Media Path*) wurde optimiert für den Zugriff durch das verbindungslose und unzuverlässige UDP/IP-Protokoll, das insbesondere den Anforderungen von Musik- oder Videodaten entspricht. Der Medienpfad greift über ein priorisiertes CSMA-Protokoll in regelmäßigen Zeitintervallen auf den Übertragungskanal zu. Er kommt bei der Kommunikation von synchronen Knoten zum Einsatz.
- Der Sprachpfad (*Toll-Quality Voice Path*) ist für die isochrone, bidirektionale und symmetrische Übertragung von Daten ausgelegt, wie sie von den höheren Protokollschichten des DECT-Standards vorgesehen sind. Der Sprachpfad nutzt ein TDMA-Verfahren, das in die CSMA-Zugriffe eingeschoben wird. Er implementiert den Verkehr der isochronen Knoten.

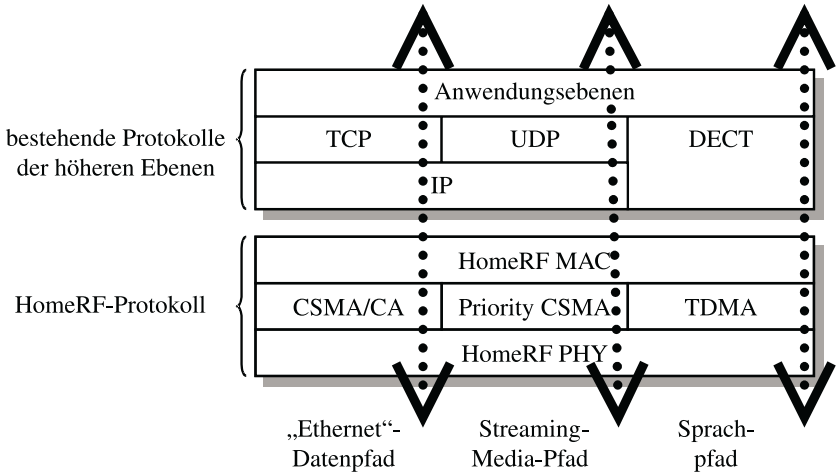


Abbildung 7.1: Aufbau des HomeRF-Standards

7.3 Kanalzugriff

7.3.1 Einordnung

Das im Rahmen des HomeRF-Standards umgesetzte Protokoll auf der MAC-Ebene wird als ***S**hared **W**ireless **A**ccess **P**rotocol - **C**ordless **A**ccess* (SWAP-CA) bezeichnet. Teilweise werden die Bezeichnungen HomeRF und SWAP fälschlicherweise als Synonyme verwendet. Dies ist insbesondere in älteren Publikationen der Fall.

Der Zugriff auf den Kanal erfolgt mit Hilfe der drei im Folgenden beschriebenen Dienstarten, wobei die Verwaltung des Zugriffs durch den CP erfolgt. Der grundsätzliche Ablauf eines Rahmens ist in Abbildung 7.2 dargestellt. Dabei wird zu Beginn eines jeden Rahmens ein Frequenzsprung durch den PHY durchgeführt (vgl. Abschnitt 7.4).

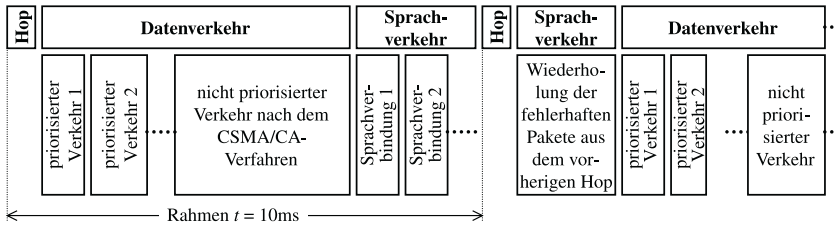


Abbildung 7.2: Ablauf des Kanalzugriffs für die verschiedenen Verkehrstypen in HomeRF

Dabei treten in jedem Zeitablauf mit dem Daten- und dem Sprachverkehr zwei grundsätzliche Bestandteile auf:

- Der Datenverkehr wickelt zu Beginn eines jeden Rahmens zunächst die priorisierten Datenströme ab, bevor der normale – und nicht angemeldete – Verkehr der anderen Datenknoten übernommen wird. Die priorisierten Datenströme haben dabei zu Beginn eines jeden Rahmens Priorität, auch wenn sie unterschiedliche Bitlängen in Anspruch nehmen.
- Zum Ende eines jeden Rahmens wird der Sprachverkehr abgewickelt. Er erhält jeweils feste Zeitschlitze für Downlink und Uplink im Sinne eines TDMA / TDD-Verfahrens. Für den Fall, dass die Übertragung des Sprachverkehrs aus irgendeinem Grund nicht erfolgreich war – z.B. aufgrund einer temporären Störung des Kanals – kann zu Beginn des nächsten Rahmens eine erneute Übertragung (Re-Transmission) stattfinden.

7.3.2 Asynchrone Übertragung

Der asynchrone Verkehr wird innerhalb einer verlängerten Rahmenstruktur, dem so genannten *Superframe*, mit einer Dauer von jeweils 20 ms abgewickelt (vgl. Abbildung 7.3). Der Zugriff erfolgt nach einem CSMA-CA-Verfahren, das sehr eng an den IEEE802.11-Standard angelehnt ist. Erfolgreich übertragene Pakete werden mit Hilfe einer Empfangsbestätigung quittiert.

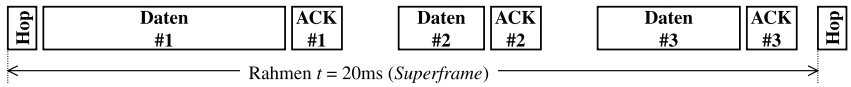


Abbildung 7.3: Übertragung von asynchronen Rahmen über HomeRF

7.3.3 Synchrone Übertragung

Im Rahmen des HomeRF2.0-Standards können bis zu acht priorisierbare bidirektionale *Streaming Media Sessions* für Audio- oder Videoanwendungen unterstützt werden.

7.3.4 Isochrone Übertragung

Für den Fall, dass isochroner Verkehr für einen I-Node abgewickelt werden muss, lassen sich drei Veränderungen in Abbildung 7.4 beobachten:

- Die Rahmenlänge verkürzt sich auf 10 ms. Auf diese Weise kann die Latenzzeit für die Übertragung von Sprachsignalen möglichst gering gehalten werden.
- Zu Beginn des Rahmens wird ein Steuersignal (*Beacon*) vom CP versendet, der die anderen im Funkbereich aktiven Stationen darüber informiert, dass am Ende des Rahmens zwei Zeitschlitze für den isochronen Verkehr reserviert werden.
- Am Ende des Rahmens wird in einem Zeitmultiplex (TDD) der Sprachverkehr vom CP zur Station (*Downlink*) und von der Station zum CP (*Uplink*) abgewickelt. Dabei sind zwei Aspekte zu berücksichtigen:
  - Es müssen pro Rahmen 320 Bit in jeder Richtung übertragen werden, wenn Sprachtelefonie in der von DECT übernommenen ADPCM-Kodierung nach G.726 mit einer Datenrate von 32 kbps pro Übertragungsrichtung unterstützt wird. Bei einer Bitdauer von 625 ns im 1,6 Mbps schnellen HomeRF1.2-Standard nimmt ein solcher Teilrahmen also 0,2 ms zuzüglich der Steuerinformationen ein.
  - Dass die Übertragung zunächst in Downlink- und danach in Uplink-Richtung erfolgt, erleichtert die Synchronisation beim Kanalzugriff, da die Downlink-Übertragung ja vom zentralen Knoten ausgeht.

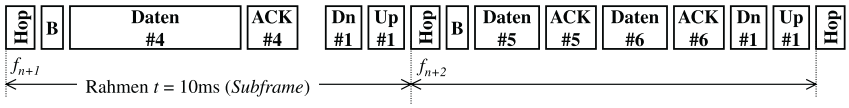


Abbildung 7.4: Ergänzung des asynchronen Datenverkehrs durch ein isochrones Telefongespräch

Wird nun noch ein zweites Telefongespräch hinzugefügt, dann sind die Veränderungen im ersten Rahmen mit f_{n+3} in Abbildung 7.5 zu beobachten:

- Das Steuersignal (*Beacon*) reserviert nunmehr vier Zeitschlitze am Ende des Rahmens für den isochronen Verkehr.
- Zunächst werden die Daten beider Stationen in Downlink-Richtung und danach in Uplink-Richtung übertragen.

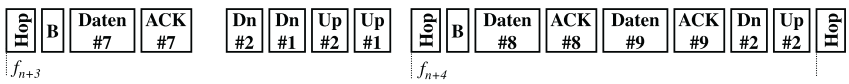


Abbildung 7.5: Ergänzung des asynchronen Datenverkehrs durch zwei isochrone Telefongespräche

Wird während der Laufzeit des zweiten Gesprächs das zuerst begonnene Gespräch #1 beendet, dann müssen die Übertragungen des zweiten Gesprächs umsortiert werden, so dass wieder ein möglichst langer Zeitraum für die Übertragung asynchroner Daten zur Verfügung steht. Dies erfolgt im zweiten Rahmen mit f_{n+4} in Abbildung 7.5.

Nach der Beendigung des zweiten Gespräches muss nur noch asynchroner Datenverkehr abgewickelt werden. Dies bedeutet, dass

- das Steuersignal wieder entfernt und
- der Rahmen wieder auf 20 ms verlängert wird.

Der Rahmen erhält also wieder das gleiche Format wie in Abbildung 7.3, nur dass nun auf der nachfolgenden Frequenz f_{n+5} übertragen wird.

Im HomeRF2.0-Standard können gleichzeitig maximal vier isochrone Verbindungen unterstützt werden. Im geplanten HomeRF2.1-Standard soll diese Zahl auf acht heraufgesetzt werden.

7.4 Bitübertragung

7.4.1 1 MHz-Kanäle

Auf der Bitübertragungsebene nutzt der HomeRF-Standard das Frequenzsprung-Spread-Spectrum-Verfahren (FHSS) im 2,4 GHz-ISM-Band. Auf diese Weise versucht man, bezüglich der Kosten für die Bitübertragungsebene in den Bereich der Bluetooth-Module zu gelangen. Die Anforderungen an die Bauelemente sind so ähnlich, dass auch die Möglichkeit von kombinierten Funk-Transceiver-Lösungen besteht, wie sie beispielsweise für den Einsatz von Bluetooth, HomeRF und Upbanded DECT in [Vinayak 2001] besprochen wird.

Für die Nachrichtenübertragung wird das Frequenzumtastverfahren eingesetzt.

Aufgrund der Bandbreitenbeschränkungen des freigegebenen 2,4 GHz-Bands werden 75 Basiskanäle mit einer jeweiligen Bandbreite von 1 MHz zur Verfügung gestellt. Diese werden für die Übertragung der Geschwindigkeitsstufen 0,8 Mbps und 1,6 Mbps eingesetzt, mit denen alle Verkehrstypen übertragen werden und die bereits im HomeRF1.2-Standard definiert wurden.

7.4.2 5 MHz-Kanäle

Sollen nun auch höhere Datenraten umgesetzt werden, so ist zu berücksichtigen, dass die von der US-amerikanischen Aufsichtsbehörde FCC (vgl. Abschnitt 1.5) aufgestellten Regeln für den Einsatz des Frequenzsprungverfahrens im 2,4 GHz-ISM-Bereich Folgendes besagen:

- Die maximale Ausgangsleistung darf 1 W betragen.
- Es müssen mindestens 75 Kanäle von maximal 1 MHz verwendet werden, die bezogen auf ihre 20 dB-Bandbreite nicht überlappend sein müssen.

- Die durchschnittliche Belegungszeit einer Frequenz, dies ist die Zeit zwischen zwei Frequenzwechseln, muss kleiner als 0,4 s in einem 30 s-Intervall sein.

Auf dieser Grundlage ist eine Geschwindigkeitserhöhung nur dann möglich, wenn:

- entweder die Anzahl der Bits pro übertragenem Symbol vergrößert wird. Dies führt aber zu einer wesentlich erhöhten Fehlerwahrscheinlichkeit, so dass dies kein praktikabler Ansatz ist.
- oder die Bandbreite der Kanäle vergrößert wird. Dies verstößt aber gegen die von der FCC ursprünglich aufgestellten Regeln.

In einer Entscheidung vom August 2000 hat der FCC jedoch den Anträgen der HomeRF-Arbeitsgruppe gegen den Widerstand der WECA-Vertreter stattgegeben und die Regeln für die Nutzung der Frequenzsprungsysteme dahingehend erweitert, dass:

- die maximale Ausgangsleistung von 1 W auf 125 mW reduziert wird,
- die Kanäle eine maximale Bandbreite von 5 MHz aufweisen dürfen, die bezogen auf ihre 20 dB-Bandbreite nicht überlappend sein müssen. Auf diese Weise ergibt sich für den freigegebenen Frequenzbereich eine Anzahl von 15 Kanälen.

Allerdings kann nur der Datenverkehr mit diesen hohen Geschwindigkeiten übertragen werden. Die isochrone Datenübertragung erfolgt weiterhin im Bereich der Basiskanäle. Aufgrund der größeren Bandbreite kann auch nur eine geringere Kanaldichte erreicht werden.

8 HiperLAN/2

8.1 Der Standard

8.1.1 Positionierung

Mit dem ***Hi**gh **Pe**rformance **R**adio **L**ocal-**A**rea **N**etwork, Type **2*** (HiperLAN/2) hat das ETSI im Rahmen des Projekts BRAN (***B**roadband **R**adio **A**ccess **N**etwork*) im April 2000 eine Spezifikation verabschiedet, die Einrichtungen für den Zugang zu Festnetzen sowohl in privaten als auch in öffentlichen Umgebungen mit Bitraten von bis zu 54 MBps über Entfernungen von bis zu 150 m unter Nutzung des 5 GHz-Bereiches zur Verfügung stellen soll. Im Mittelpunkt standen dabei die Gewährleistung von Dienstgüten (***Q**uality **o**f **S**ervice* - QoS) sowie ein flexibles und erweiterbares Dienstmodell.

Die Verbreitung von HiperLAN/2 wird vom ***H**iperLAN/**2** **G**lobal **F**orum* gefördert (H2GF – www.hiperlan2.com), das im September 1999 von den Unternehmen Bosch (jetzt: Tenovis), Dell, Ericsson, Nokia, Telia and Texas Instruments gegründet wurde. Zum gegenwärtigen Zeitpunkt (Mitte 2001) sind 50 Firmen Mitglieder in diesem Forum.

Weitere Aktivitäten haben sich im Umfeld der *5 GHz Industrial Advisory Group* ergeben, die sich seit Anfang des Jahres 2000 zum Ziel gesetzt hat, einen weltweit einheitlichen WLAN-Standard im 5 GHz-Bereich zu etablieren (*http://www.microsoft.com/HWDEV/wireless/5GHz.htm*).

Vor der Spezifikation des HiperLAN/2 hatte die Fachgruppe ***R**adio **E**quipment & **S**ystems* 10 (RES10) im ETSI schon eine erste Version des HiperLAN-Standards erarbeitet. Dieser war ausgerichtet auf das Ad-hoc-Networking von portablen Geräten und basierte auf einem CSMA/CA-Algorithmus. Dabei wurden bereits sowohl eine asynchrone Datenübertragung als auch Anwendungen mit Echtzeitanforderungen unterstützt. Die Fachgruppe RES10 wurde nach der Gründung von BRAN aufgelöst.

Der Standard fand allerdings keine große Unterstützung in der Industrie. Lediglich Proxim stellte 1998 mit dem Rangelan 5 ein auf HiperLAN/1 basierendes System vor, das jedoch bereits nach kurzer Zeit wieder vom Markt genommen wurde.

Der HiperLAN/2-Standard im engeren Sinne wird ergänzt durch zwei weitere Bestandteile, die zusätzliche Anwendungsgebiete erschließen sollen.

- HiperACCESS soll für Entfernungen von bis zu 5 km als Punkt-zu-Mehrpunkt-Architektur Zugang für Wohnviertel und Geschäftskunden bieten. Als typische Datenrate für dieses ehemals als HiperLAN Type III bezeichnete Protokoll für den ***W**ireless **L**ocal **L**oop* (WLL) wird 27 Mbps angestrebt.
- HiperLINK dient zur Punkt-zu-Punkt-Verbindung mit sehr hohen Datenraten von bis zu 155 Mbps über Entfernungen bis 150 m. Insbesondere soll die Anbindung von HiperLAN/2 und HiperACCESS über kurze Strecken unterstützt werden. Für das ehemals als HiperLAN Type IV bezeichnete HiperLINK ist ein Frequenzband um 17 GHz reserviert.

Abbildung 8.1 zeigt die verschiedenen Bestandteile im Überblick. Zusammenfassungen über Aufbau und Funktionalität von HiperLAN/2 finden sich in [Walke 2000], [KhunJush 2000] und [Johnsson 1999]. Es muss darauf hingewiesen werden,

- dass HiperACCESS und HiperLINK völlig selbständige Systeme sind, die gemeinsam im BRAN-Projekt diskutiert wurden, um mögliche Synergien auszunutzen.
- dass HiperLINK seit einiger Zeit so gut wie nicht mehr weiter betrieben wird.

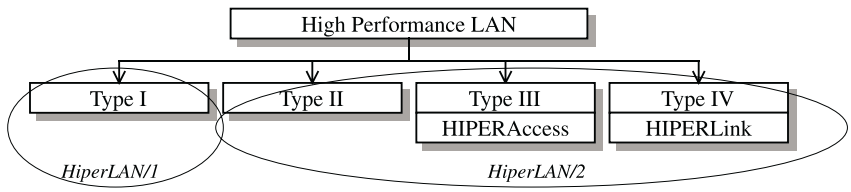


Abbildung 8.1: Die Bestandteile des HiperLAN-Standards

8.1.2 Markteinführung

Während in Europa von der ETSI die notwendigen regulatorischen Rahmenbedingungen für HiperLAN/2 etabliert sind, lassen sich in den USA und in Japan folgende Entwicklungen beobachten:

- In Japan entschied sich die ***M**ultimedia **M**obile **A**ccess **C**ommunications* (MMAC) Promotion Assocation innerhalb der ***A**ssociation of **R**adio **I**ndustries and **B**roadcasting* (ARIB), einen Standard aufzunehmen, der der HiperLAN/2-Spezifikation vergleichsweise ähnlich ist. Dieser wird als ***Hi**gh **S**peed **W**ireless **A**ccess **N**etwork* (HiSWANa) bezeichnet. Zusätzlich zu den veränderten Frequenzzuweisungen in Japan muss aufgrund der anderen regulatorischen Situation ein Mechanismus zur Überwachung des Trägersignals (*Carrier Sensing*) implementiert werden. Darüber hinaus existieren im Detail zahlreiche weitere Unterschiede [Aramaki 2001]. Mittlerweile hat sich eine gemeinsame Arbeitsgruppe aus ETSI, H2GF und MMAC mit dem Ziel der Harmonisierung der beiden 5 GHz-

Standards gebildet. Die gegenseitige Anpassung kann z.B. darin bestehen, derzeit verpflichtende Systembestandteile als optional vorzugeben.

- In den USA ist die Situation deutlich schwieriger, da hier die Spezifikation des IEEE802.11a ebenso in das UNII-Band positioniert wurde. In Bezug auf den Kanalzugriff weisen IEEE802.11a und HiperLAN/2 keine Gemeinsamkeiten auf, während beide ein fast identisches OFDM-Modulationsverfahren verwenden. Weitere Aspekte für die Diskussion über die Voraussetzungen für einen Markterfolg der jeweiligen Technologien werden in Abschnitt 8.6 angeführt.

8.2 Architekturen

8.2.1 Systemarchitektur

Ein HiperLAN/2-Netzwerk besteht typischerweise aus mehreren Zugangspunkten (***A**ccess **P**oints* – AP), die zusammen in einem bestimmten Gebiet eine vollständige oder teilweise Funkversorgung ermöglichen. In diesen Funkzellen kommunizieren mobile Teilnehmer (***M**obile **T**erminals* - MT) mit diesen Zugangspunkten. Dabei wird sowohl ein ***C**entralized **M**ode* (CM) unterstützt, bei dem die mobilen Teilnehmer alle Nutzdaten über die Zugangspunkte übertragen, als auch ein ***D**irect **M**ode* (DM). In diesem können die mobilen Teilnehmer, die sich in Funkreichweite zueinander befinden, unter der Kontrolle einer Steuerinstanz (***C**entral **C**ontroller* - CC) Nutzdaten direkt austauschen. Dabei muss der DM immer unterstützt werden, während der CM in Abhängigkeit vom Geräteprofil optional angeboten werden kann.

8.2.2 Protokollarchitektur

Die Spezifikationen der ETSI/BRAN-Systeme sind auf die unteren drei Schichten des ISO/OSI-Referenzmodells ausgerichtet. In Abbildung 8.2 ist das vereinfachte Dienstmodell von HiperLAN/2 dargestellt. Auf der Bitübertragungsschicht setzt eine Übermittlungs- bzw. Sicherungsschicht auf, die im HiperLAN-Sprachgebrauch als ***D**ata **L**ink **C**ontrol* (DLC) bezeichnet wird und sich mit ***R**adio **L**ink **C**ontrol* (RLC), ***E**rror **C**ontrol* (EC) und ***M**edium **A**ccess **C**ontrol* (MAC) in drei funktionale Einheiten gliedert.

Um den Übergang zu den höheren Schichten herzustellen, wird die in Abbildung 8.2 dargestellte Anpassungsschicht (***C**onvergence **L**ayer* - CL) eingeführt. Diese leistet die Umsetzung der Daten auf Steuer- und Benutzerebene aus den höheren Schichten auf die Daten der Sicherungsschicht. Hierfür ist die Anpassungsschicht noch einmal zweigeteilt. Auf einer gemeinsamen Basis (*Common Part*) baut eine dienstspezifische Schicht (*Service Specific Part*) auf. Hier besteht die Möglichkeit, anderen Netzwerkdiensten die gewohnten Dienstzugangspunkte (SAP) bereitzustellen.

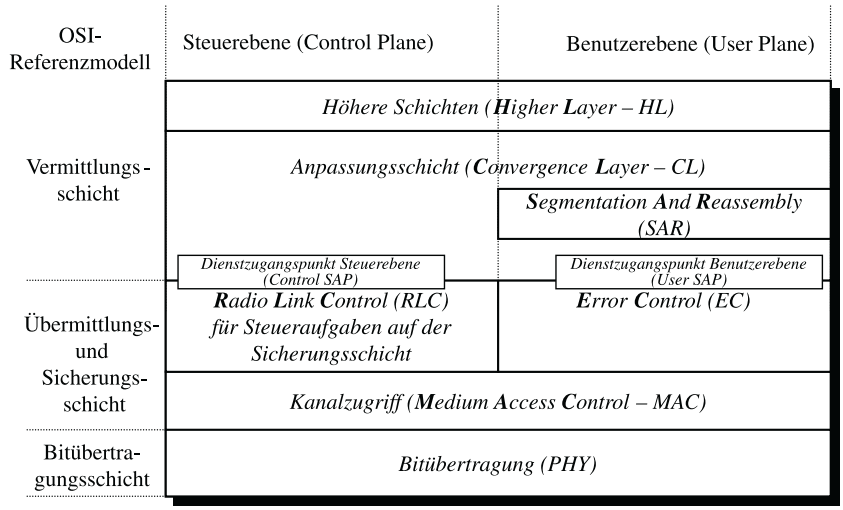


Abbildung 8.2: Vereinfachtes Dienstmodell von HiperLAN/2

Insbesondere lässt sich so auch der Zugang zu UMTS-Kernnetzen herstellen und Roaming und Handover unterstützen. Auf diese Weise hoffen die Befürworter der HiperLAN/2-Technologie, dass die Mobilfunkbetreiber insbesondere an so genannten Hot-Spots den breitbandigen Zugang zu UMTS mit Hilfe von HiperLAN/2 bereitstellen, da hier deutliche Kostenvorteile zu erzielen sind.

Dabei können sowohl die Datenrahmen als auch die Steuerinformationen angepasst werden. Ein Beispiel für die Anpassung der Steuerinformationen besteht darin, dass bei der Nutzung von HiperLAN/2 als Zugang zum UMTS-Netz ein Handover auf der höheren UMTS-Ebene ausgelöst wird, wodurch dann auch ein Handover auf HiperLAN/2-Ebene angestoßen wird. Die notwendige Anpassung übernimmt dabei der CL.

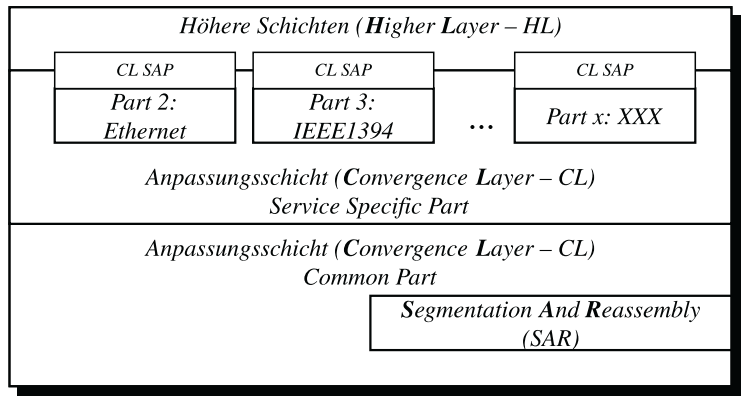


Abbildung 8.3: Dienstmodell der Anpassungsschicht von HiperLAN/2

Diese Schicht ist auch für das Aufteilen und Wiederherstellen (***S**egmentation **A**nd **R**eassembly* - SAR) von Protokolldateneinheiten (***P**rotocol **D**ata **U**nit* - PDU) auf der Benutzerseite verantwortlich. Dabei ist hervorzuheben, dass HiperLAN/2 nicht für ein bestimmtes Netzprotokoll oder bestimmte Anwendungen optimiert ist. Durch die Verwendung von verschiedenen Anpassungsschichten können auch verschiedene Netzprotokolle wie Ethernet, ATM oder IEEE1394 die Übertragungsressourcen des HiperLAN/2 nutzen. Auf diese Weise kann HiperLAN/2 auch die Ankopplung an die jeweiligen *Core Networks* implementieren.

Die SAR wird nur für paketbasierte Netze benötigt. Die Einbindung in zellbasierte Netze wie ATM wird hier nicht betrachtet.

Bezüglich der Instanzen in den Mobilstationen gilt:

- Für jede Mobilstation wird eine RLC-Instanz generiert.
- HiperLAN/2 arbeitet verbindungsorientiert. Hierzu wird für jede Datenverbindung vor der eigentlichen Datenübertragung jeweils eine EC- und SAR-Instanz generiert. Die logischen Verbindungen müssen vor der Übertragung von Nutzdaten eingerichtet werden und unterstützen alternativ Punkt-zu-Punkt-, Punkt-zu-Mehrpunkt- und Broadcast-Verbindungen.

Auf der Seite der Zugangspunkte muss dann jeweils die gleiche Anzahl von RLC-, EC- und SAR-Instanzen generiert werden wie in den zugeordneten Mobilstationen insgesamt.

Auf der Grundlage der Verbindungsorientierung wird eine Unterstützung von Dienstgüten (***Q**uality **o**f **S**ervice* - QoS) möglich. Für jede Verbindung können individuell dienstgütespezifische Parameter, wie Datenrate, Verzögerung, Varianz der Verzögerung und Verlustrate vereinbart werden.

Das Fehlersteuerungs-Protokoll (EC) erlaubt hierzu folgende Dienste:

- Im bestätigten Modus (*Acknowledged Mode*) wird der erfolgreiche Empfang einer Sendung mit Hilfe einer Rückantwort bestätigt.
- Da beim Versenden an mehrere Empfänger der bestätigte Modus nicht sinnvoll unterstützt werden kann, erlaubt der Wiederholungs-Modus (*Repetition Mode*) die Erhöhung der Zuverlässigkeit der Übertragung. Hierzu werden die Abschnitte der Pakete, die die Nutzdaten enthalten, zweimal übertragen.
- Darüber hinaus steht mit dem unbestätigten Modus (*Unacknowledged Mode*) eine einfache und schnelle Übertragung zur Verfügung, die allerdings nur für die unzuverlässigen Verbindungstypen eingesetzt werden kann.

8.3 Kanalzugriff

Die Zugriffssteuerung auf das Medium erfolgt durch die MAC-Teilschicht, die im Sinne eines Master-Slave-Protokolls zentral vom Zugangspunkt verwaltet wird. Der Zugangspunkt weist den Mobilstationen Kapazität zu, die diese dann zur Übertragung von Nutz- und Steuerdaten verwenden. Dabei muss der Zugangspunkt insbesondere die für die verschiedenen Verbindungen benötigten Dienstgüten berücksichtigen.

Hierzu wird der physische Kanal in Rahmen konstanter Länge aufgeteilt. Bei einer Rahmenlänge von 2 ms und einer Symbolzeit auf OFDM-Ebene von 4 µs entspricht dies 500 Symbolen pro Rahmen. Der Rahmen wird dann noch einmal in die in Abbildung 8.4 gezeigten Übertragungsphasen unterschiedlicher Funktionalität aufgeteilt. Dabei ändert sich die Kapazität der einzelnen Kanäle nach Bedarf.

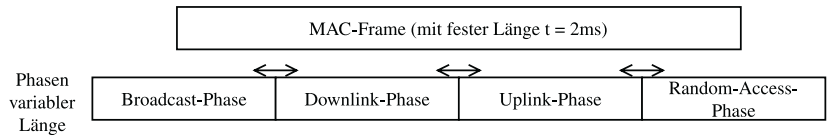


Abbildung 8.4: Flexibler Aufbau der Rahmen im HiperLAN/2

Von großer Bedeutung für das Verständnis des Kanalzugriffs bei HiperLAN/2 ist die Unterscheidung zwischen logischem und Transportkanal, die in der ***D**ata **L**ink **C**ontrol*-(DLC-)Schicht vorgenommen wird. Unter einem logischen Kanal versteht man dabei den Pfad, der für einen bestimmten Datentransportdienst von der MAC-Einheit angeboten wird. Logische Kanäle werden mit Hilfe bestimmter Transportkanäle realisiert. Transportkanäle unterscheiden sich in ihren Nachrichtenformaten. Die definierten Kanäle und ihre jeweiligen Zuordnungen in Downlink und Uplink sind in Abbildung 8.5 und Abbildung 8.6 gezeigt.

8.4 Bitübertragung

8.4.1 Frequenzzuweisungen

Wie bereits in Abschnitt 4.7.1 in Zusammenhang mit den IEEE802.11a-konformen Geräten erwähnt wurde, deren Entwicklung vor allem von US-amerikanischen Unternehmen vorangetrieben wird, ist auch die Nutzung des 5 GHz-Frequenzbands nicht einheitlich. Die weltweite Verfügbarkeit dieser Kanäle ist in Abbildung 8.7 aufgeführt.

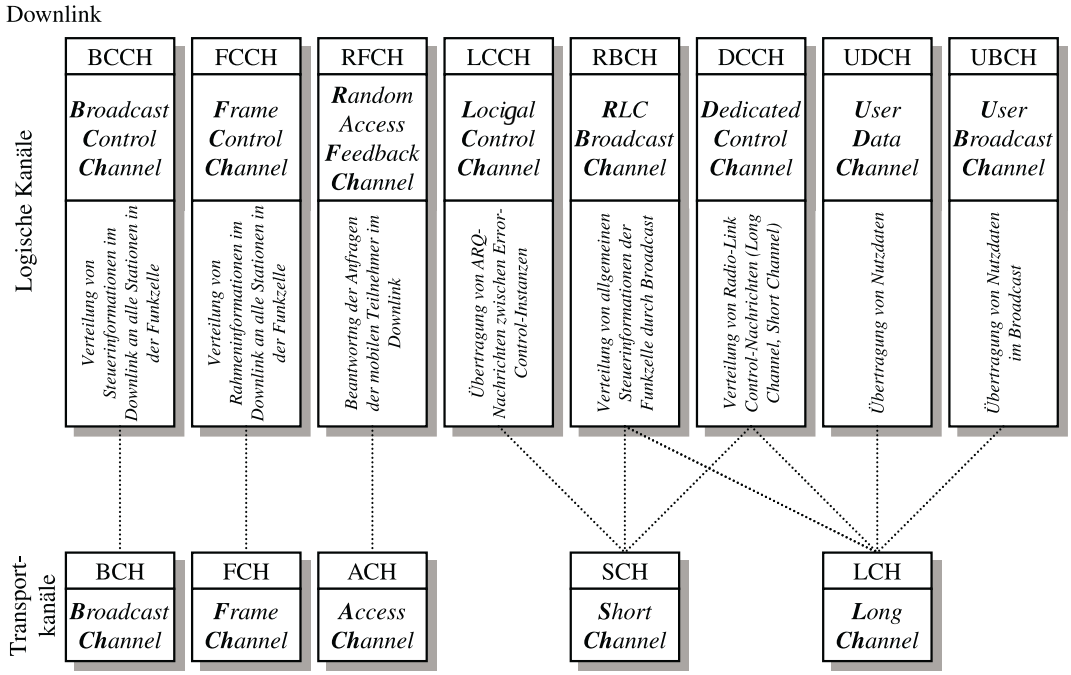


Abbildung 8.5: Logische und Transportkanäle im Downlink von HiperLAN/2

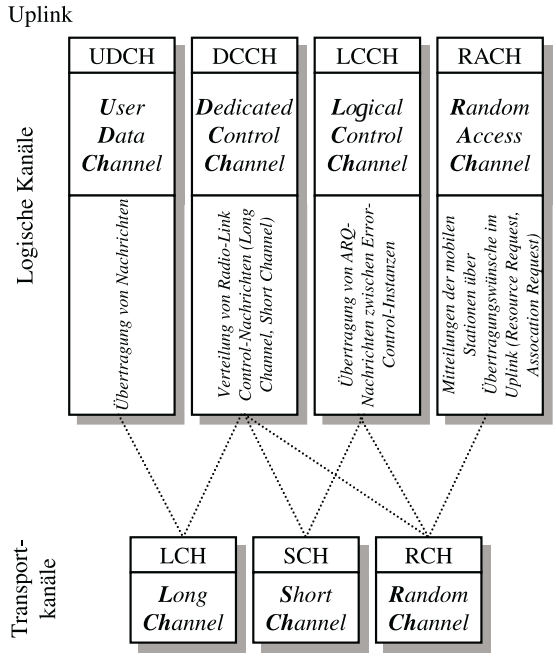


Abbildung 8.6: Logische und Transportkanäle im Uplink von Hiper-LAN/2

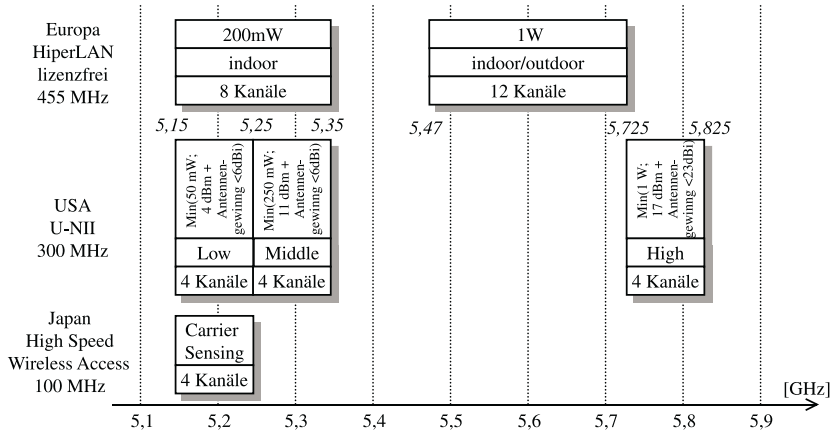


Abbildung 8.7: Frequenzzuweisungen im 5 GHz-Bereich

Neben der Einhaltung der Frequenzbereiche sind folgende weitere regionale Besonderheiten zu berücksichtigen:

- In Europa sind auch die Implementierung einer geregelten Sendeleistung (***P**ower **C**ontrol* – PC, auch ***T**ransmit **P**ower **C**ontrol* – TPC) mit einer großflächigen Leistungsreduktion um 3 dB und die dynamische Frequenzkanalwahl (***D**ynamic **F**requency **S**election* - DFS, auch ***D**ynamic **C**hannel **S**election* - DCS) vorgeschrieben. Der Bereich von 5,15 bis 5,35 GHz ist für den Einsatz in Innenräumen bei einer mittleren Sendeleistung von maximal 200 mW (EIRP) vorgesehen, während in den Frequenzen zwischen 5,47 und 5,725 GHz mit einer mittleren Leistung von maximal 1 W (EIRP) gesendet werden darf. Der gesamte Bereich ist unter Einhaltung der Regularien lizenzfrei zu nutzen (*license exempt*).
- In den USA müssen weder PC noch DFS durchgeführt werden. Entsprechend sind diese Fähigkeiten in dem in diesem Bereich aktiven IEEE802.11a auch nicht vorgesehen.

  Die Sendeleistungen von 200 mW in Innenräumen und 1 W in Außenbereichen für den Bereich zwischen 5,15 und 5,35 GHz beziehen sich auf maximale Spitzensendeleistungen (EIRP). In dem Bereich zwischen 5,725 und 5,825 GHz darf sogar mit 4 W gesendet werden.
- In Japan stehen lediglich 100 MHz Bandbreite zwischen 5,15 und 5,25 GHz zur Verfügung. Es ist vorgeschrieben, dass alle 4 ms ein *Carrier Sensing* durchgeführt wird.

In der Problematik um die Frequenzzuweisung ist neben der Diskussion zwischen den Regionen auch zu berücksichtigen, dass es bereits Anwendungen im 5 GHz-Bereich gibt.

Diese liegen im Wesentlichen im Bereich von Satelliten- und Navigationssystemen. Dabei ist die politische Durchsetzungskraft der Satellitenbetreiber üblicherweise als sehr hoch anzusetzen.

8.4.2 Modulationsverfahren

HiperLAN/2 nutzt ein OFDM-Verfahren (*Orthogonal Frequency Division Multiplex* – OFDM), wie es in Abschnitt 2.8 erläutert wurde. OFDM erreicht eine hohe Leistungsfähigkeit auch bei dispersiven Kanälen, wie sie bei Frequenzen im Multigigahertz-Bereich vorliegen. Dann kann eine im Vergleich mit dem bei HiperLAN/1 eingesetzten FDM einfache und kostengünstige Realisierbarkeit sichergestellt werden. Darüber hinaus findet eine *Multicarrier Modulation* Anwendung. Dabei werden die Daten in verschiedene Datenströme aufgeteilt, die dann über unabhängige Subcarrier mit einer Bandbreite von jeweils etwa 300 kHz übertragen werden. Es stehen die in Abbildung 8.8 dargestellten 52 Subcarrier pro Kanal zur Verfügung, wobei 48 für den Datentransport und 4 Pilot-Subcarrier zur Synchronisation eingesetzt werden. Ein HiperLAN/2-Kanal weist auf diese Weise eine Bandbreite von 20 MHz auf.

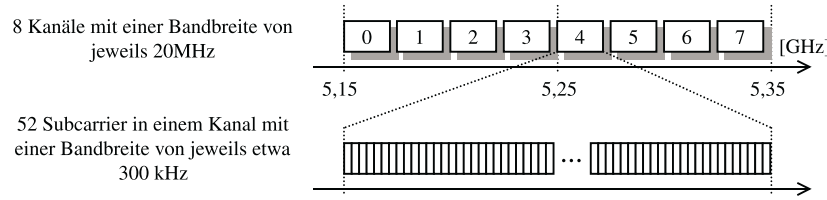


Abbildung 8.8: Aufteilung eines HiperLAN/2-Kanals in 52 Subcarrier

Die unterschiedlichen Datenraten auf der Bitübertragungsschicht werden dann durch die sieben in Tabelle 8.1 aufgeführten Modulationsarten und Code-Raten für die ***F**orward **E**rror **C**ontrol* (FEC) erreicht. Während die Modi 1 bis 6 in jedem Gerät implementiert werden müssen, ist der Modus 7 mit der Unterstützung des 64QAM optional.

Modus	Modulation	Code-Rate	Brutto-Datenrate	HIPERLAN/2	IEEE802.11a
1	BPSK	1 / 2	6 Mbps	ja	ja
2	BPSK	3 / 4	9 Mbps	ja	ja
3	QPSK	1 / 2	12 Mbps	ja	ja
4	QPSK	3 / 4	18 Mbps	ja	ja
5	16QAM	1 / 2	24 Mbps	nein	ja
5	16QAM	9 / 16	27 Mbps	ja	nein
6	16QAM	3 / 4	36 Mbps	ja	ja
7	64QAM	3 / 4	54 Mbps	ja	ja

Tab. 8.1: Modulationsarten von HiperLAN/2 und IEEE802.11a

Die Modulationsarten von HiperLAN/2 und IEEE802.11a sind bis auf den fünften Modus identisch, da die beiden Gremien auf der Bitübertragungsschicht eng zusammengearbeitet haben.

8.5 Weitere Dienste

HiperLAN/2 bietet verschiedene weitere Dienste, die einen komfortablen und sicheren Einsatz ermöglichen:

- Umfangreiche Maßnahmen gewährleisten ein hohes Sicherheitsniveau. Besonders ist dabei darauf hinzuweisen, dass diese Maßnahmen – anders als im IEEE802.11 – integraler Bestandteil des Standards sind und somit auch zwischen Geräten unterschiedlicher Hersteller funktionieren.
- HiperLAN/2 unterstützt mit Hilfe von verschiedenen Funktionen auch Ad-hoc-Networking.

8.6 Diskussion

Im Bereich der 5 GHz-Netze konkurrieren zwei Ansätze, die zwar auf der Ebene der physischen Übertragung weitgehend identisch sind, aber auf der Ebene des Kanalzugriffs sehr unterschiedliche Eigenarten aufweisen. Aus technischer Sicht zeigt sich der HiperLAN/2-Standard deutlich überlegen, wie die Übersicht in Tabelle 8.2 zeigt. Für einen Markterfolg sind aber weitere politische und unternehmensbezogene Aspekte sowie Kostenaspekte von mindestens ebenso weitreichender Bedeutung.

Tab. 8.2: Vergleich des HiperLAN/2-Standards mit dem IEEE802.11a

	IEEE802.11a	HiperLAN/2
Dynamische Frequenzauswahl	nein	ja
Anpassung der Sendeleistung	nein	ja
Sicherheit	teilweise	ja
Unterstützung von QoS	nein	ja
Kopplung mit anderen Standards (UMTS)	nein	optional

9 Betrieb eines WLAN nach IEEE802.11b

9.1 Einführung

Dieses Kapitel vermittelt einen Einblick in Betrieb, Administration und Analyse von drahtlosen lokalen Netzen nach dem IEEE802.11b-Standard. Die Beschreibung erfolgt dabei mit Hilfe von Ausrüstung, die von verschiedenen Herstellern freundlicherweise zur Verfügung gestellt wurde. Diese Serienprodukte geben einen guten Einblick in typische Implementierungen und lassen die Vor- und Nachteile der jeweiligen Umsetzung erkennen.

9.2 Mobile Stationen

9.2.1 Aufbau

Auf Seiten der mobilen Stationen sind verschiedene Bauformen für PC-gestützte Anwendungen anzutreffen, die bereits in Abschnitt 3.2 vorgestellt wurden.

9.2.2 Fähigkeiten

Einige grundlegende Eigenschaften beeinflussen den Komfort für den Benutzer wesentlich. An dieser Stellen seien einige Kriterien genannt:

- Bei der Installation sind kaum Unterschiede festzustellen. Die meisten Systeme unterstützen die Installation der Treiber über den Hardware-Manager von MS Windows, einen komfortablen Wizard. Allerdings zeigen sich manche Geräte empfindlich beim Betrieb von mehreren verschiedenen PC-Cards, so dass bei den Tests eine Wiederherstellung der vorherigen Betriebssysteminstallation notwendig wurde.
- Alle Systeme unterstützen im Wesentlichen die Betriebssysteme der Microsoft-Windows-Familie. In den kommerziellen Standardpaketen spielt die Unterstützung von Unix im Allgemeinen und Linux im Speziellen keine Rolle. Für den Einsatz unter Linux sind seit der Kernel-Version 2.2 die gängigen Karten im Kernel integriert. Für andere Produkte ist man auf das Engagement der Linux-Gemeinde angewiesen [Tourrilhes (1)].
- Fast alle Systeme enthalten menügesteuerte Werkzeuge, die eine einfache Administration der jeweiligen Netzwerkanbindung und eine Analyse der jeweiligen Netze ermöglichen. Diese müssen im Allgemeinen

getrennt von den Hardware-Treibern installiert werden. Hierfür steht in der Regel ein Wizard zur Verfügung.

- Da diese mitgelieferten Systeme einfach in der Bedienung sein müssen und insbesondere auch die Sicherheitsanforderungen anderer Netzwerke erfüllen müssen, stehen dedizierte Analysewerkzeuge zur Verfügung, die in Abschnitt 9.5 näher vorgestellt werden.

9.2.3 Administration

Die Verwaltung der mobilen Stationen erfolgt mit Hilfe von menügestützten grafischen Oberflächen. Der komfortable Aufbau und der Umfang der Einstellmöglichkeiten bei der Bedienung unterscheidet auch die Geräte unterschiedlicher Hersteller.

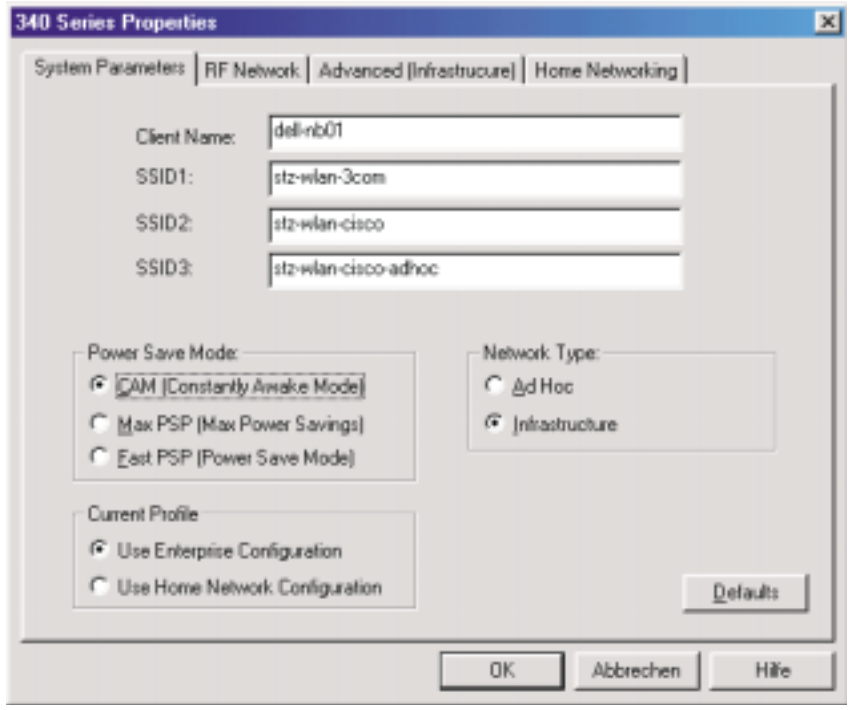


Abbildung 9.1: Aironet Client Utility von Cisco - Parameter der Netzwerkarchitektur

- Abbildung 9.1 zeigt die Parameter-Ebene des Aironet Client Utility von Cisco, auf der die grundsätzlichen Eigenschaften der Netzwerkarchitektur eingestellt werden können. Hierzu zählt insbesondere die Frage, ob der Infrastruktur- oder der Ad-hoc-Modus ausgewählt wird, aber auch die Definition der erlaubten SSIDs sowie die grundlegenden Einstellungen zur Energieverwaltung.

- Dabei ist anzumerken, dass nicht alle verfügbaren Client-Produkte den Ad-hoc-Modus unterstützen.
- Die Sicherheitshürde der SSID-Zuordnung kann bei vielen Produkten umgangen werden, indem eine beliebige Kennung (*any*) vorgegeben wird, die die SSID-Abfrage umgeht.

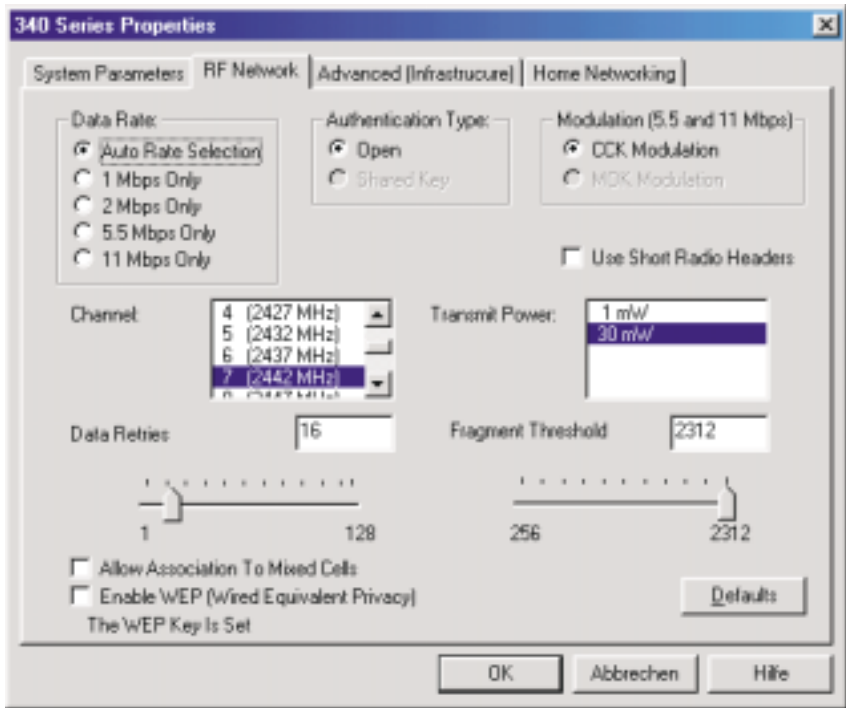


Abbildung 9.2: Aironet Client Utility von Cisco - Parameter der physischen Übertragung

- Mit Hilfe des in Abbildung 9.2 gezeigten nächsten Menüs können die grundlegenden Parameter der physischen Übertragung eingestellt werden. Hierzu zählen unter anderem:
  - Die Auswahl der Geschwindigkeitsstufen und der Modulationsarten. Hierbei wird dem Nutzer von Cisco-Aironet auch noch die Möglichkeit eröffnet, die Vor-Standard-Modulationsart MOK (vgl. Abschnitt 4.7.2) zu selektieren, um auf diese Weise Kompatibilität zu älteren Systemen zu gewährleisten, die nur MOK unterstützen.
  - Die Auswahl des Kanals. Dabei ist festzuhalten, dass dieser – im Gegensatz zu anderen Systemen, wie z.B. DECT (vgl. Kapitel 6) oder HiperLAN/2 (vgl. Kapitel 8) – statisch vom Benutzer eingetragen wird. Auf Seiten der mobilen Station betrifft dies aber lediglich die Reihenfolge, in der die Kanäle abgehorcht werden. Im Infrastruktur-Modus wird die Kanalnutzung vom Zugangspunkt vorgegeben (vgl. Abschnitt 9.3.3).

- Die Einstellung der Sendeleistung. Die übliche Einstellung wird sicherlich 30 mW sein, um noch eine 10 dBi-Antenne betreiben zu können. Darüber hinaus kann die Sendeleistung aber auch reduziert werden. Dies erscheint für den Einsatz von Antennen mit größerem Gewinn und für den Betrieb von stromsparenden Systemen über geringe Entfernungen als sinnvoll.
- Die Aktivierung der Verschlüsselung (vgl. Abschnitte 4.6 und 10.1).

- Das folgende Menü, das in Abbildung 9.3 gezeigt ist, erlaubt weitere Einstellungen zur Einbindung in ein Netzwerk. Insbesondere die *Antenna Diversity*, die Zuordnung erlaubter Zugangspunkte sowie die Einstellung von Sendeparametern können hier ausgewählt werden (vgl. Abschnitt 2.9.2).

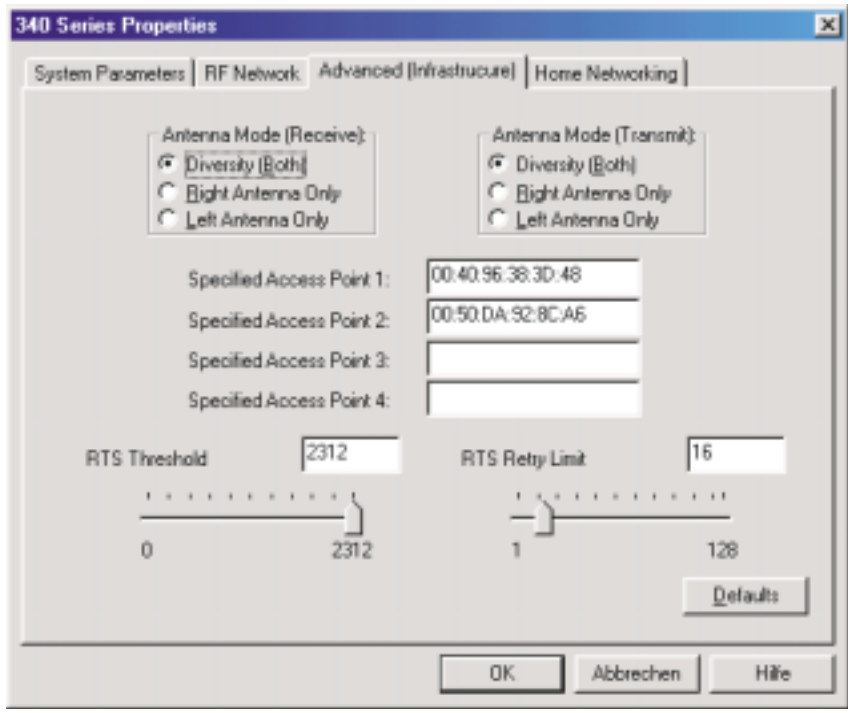


Abbildung 9.3: Aironet Client Utility von Cisco - weitere Parameter der Netzwerkarchitektur

- Das letzte Menü in der Cisco-Administration zeigt einen interessanten, wenn auch bislang halbherzigen Ansatz. Neben den bisher besprochenen Einstellungen für eine aufwändigere Umgebung im Bürobereich ist eine zweite Voreinstellung möglich, die aber deutlich weniger Parameter enthält. Zielrichtung ist der Anwender, der sein Notebook nach der Tätigkeit im Büro auch zu Hause über ein Funk-LAN anschließen möchte. Es ist gut vorstellbar, dass spätere Versionen die grundsätzliche Voreinstellung mehrerer Netzumgebungen ermöglichen, zwischen denen sich der Anwender komfortabel hin und her bewegen kann.

- Schließlich enthält der Lieferumfang der meisten Geräte noch weitere Analysewerkzeuge. Diese werden in Abschnitt 9.5.2 besprochen.

9.3 Zugangspunkte

9.3.1 Aufbau

Die Installation von Zugangspunkten (***A**ccess **P**oints* – AP) unterscheidet sich von der Inbetriebnahme der Client-seitigen Karten. Es handelt sich schließlich um autonom arbeitende Netzwerkknoten, die unter Umständen noch zusätzliche Infrastrukturaufgaben wahrnehmen. Zugangspunkte verfügen zur Steuerung der Abläufe in den meisten Fällen über einen eigenen eingebetteten Mikroprozessor.

Für die Kommunikation und die Administration der Zugangspunkte stehen zwei Wege offen:

- Erfolgt die Kommunikation über die Netzwerkverbindung, wird meist auf einen Embedded HTTP-Server zugegriffen, der auf dem Mikroprozessor des Zugangspunkts aktiv ist. Dies erlaubt den Zugriff mit Hilfe eines HTTP-Clients, also eines herkömmlichen Webbrowsers wie Microsoft Internet Explorer oder Netscape Communicator. Hierzu benötigt der Webserver über eine eigene und feste IP-Adresse. Diese dient aber lediglich zur Adressierung des Webservers, nicht aber zur Ansprache des Netzwerkknotens im Sinne eines Routers.

  Die Netzwerkverbindung kann dabei auf zwei Arten erfolgen:

  - über das drahtgebundene Netzwerk, zu dem der Zugangspunkt die Verbindung herstellt, und
  - über das drahtlose Netzwerk. Dies ist vor allem dann die einzige Möglichkeit, wenn ein autonomes drahtloses Infrastruktur-Netzwerk betrieben wird. Es ist aber zu berücksichtigen, dass in diesem Fall der Zugangspunkt über den zu verwaltenden Zugang verwaltet wird.
- Um insbesondere für die erste Installation die Erreichbarkeit des Zugangspunkts sicherzustellen, steht bei allen Zugangspunkten auch noch ein serieller Port zur Verfügung, der unter Berücksichtigung der jeweils festen Parameter einfach über einen seriellen Port eines PCs angesprochen werden kann. Die Oberfläche eines typischen Terminalzugangs zeigt Abbildung 9.4.

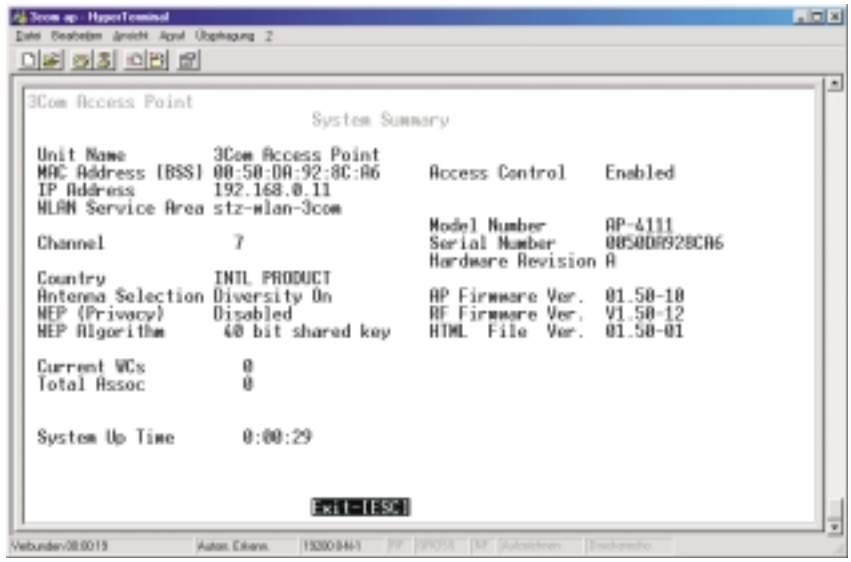


Abbildung 9.4: Oberfläche zur Administration des 3COM Access Point über ein Terminalprogramm

9.3.2 Fähigkeiten

Bei den Zugangspunkten sind ebenso deutliche Unterschiede zu verzeichnen. Aus diesem Grund seien auch hier einige Kriterien genannt:

- Auf der Grundlage der in Abschnitt 9.3.1 beschriebenen Zugriffsmöglichkeiten auf den Zugangspunkt ist eine Installation von zusätzlichen Administrationswerkzeugen nicht notwendig. Benötigt werden lediglich Programme wie Terminalprogramm und Webbrowser, die zur Standardinstallation von PCs zählen.
- Für den Zugriff über die serielle Schnittstelle ist ein serielles Kabel erforderlich. Dabei benötigen einige Systeme ein gekreuztes Nullmodemkabel, andere ein serielles Kabel. Vor diesem Hintergrund ist es sehr praktisch, wenn ein solches Kabel im Lieferumfang enthalten ist.
- Die Menüsteuerung der Systeme ist teilweise gewöhnungsbedürftig. Insbesondere die tastengesteuerten Oberflächen über die Terminalverbindung bergen hier einige Hindernisse. Aber auch die webbasierten Menüs sind nicht immer einfach zu bedienen.
- Bei der Veränderung von Parametern müssen diese vom Webserver an den Zugangspunkt weitergegeben werden. Bei einer solchen Aktualisierung führen manche Geräte einen erneuten Boot-Vorgang aus, der die wiederholte Aktualisierung sehr zeitaufwändig macht.

9.3.3 Administration

Die Administration von Zugangspunkten ist deutlich aufwändiger als die der Client-Karten, da sehr viel mehr Parameter einzustellen sind. Eine Auswahl der Einstell- und Verwaltungsmöglichkeiten wird im Folgenden vorgestellt:

- Von zentraler Bedeutung ist die Verwaltung der angemeldeten Stationen. Abbildung 9.5 zeigt alle Stationen im Netz. Dabei handelt es sich um
  - den Zugangspunkt AP4800-E mit der IP-Adresse 192.168.0.10,
  - ein mobiles Terminal PC4800 Client mit der IP-Adresse 192.168.0.7. Der Zugriff auf den Zugangspunkt erfolgt über diesen Client, was durch die Kennzeichnung *self* gekennzeichnet ist.
  - einen Desktop-PC als Server mit der IP-Adresse 192.168.0.1. Dieser nimmt auch die Aufgabe des DHCP-Servers, eines SMB-Servers und eines http-Servers wahr.
  - einen weiteren Zugangspunkt mit der IP-Adresse 192.168.0.11, dessen Kennzeichnung hier nur als *Generic 802.11* angezeigt wird. Dabei handelt es sich um einen über das verdrahtete Netz gekoppelten Zugangspunkt eines anderen Herstellers (3Com).

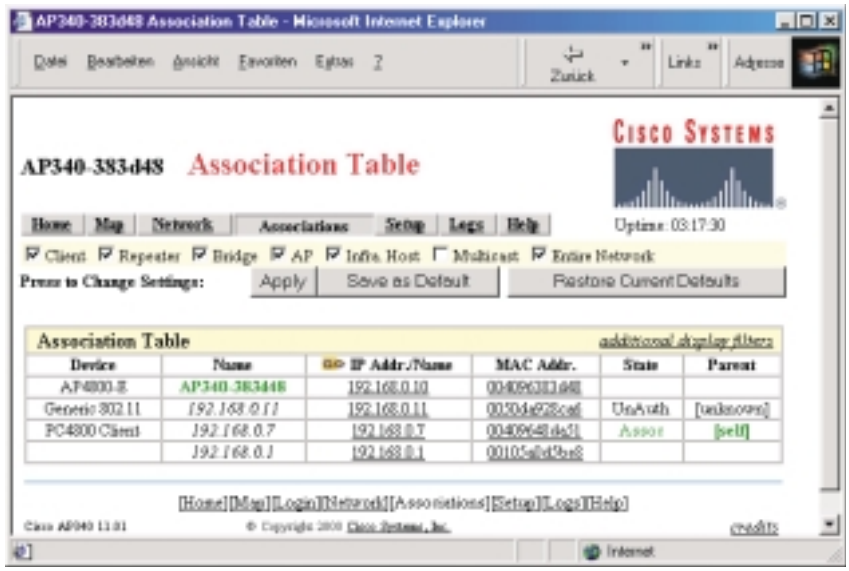


Abbildung 9.5: Aironet AP-Verwaltung von Cisco - Association Table

- Darüber hinaus kann auch die Transportcharakteristik der Funkstrecke wie in Abbildung 9.6 beobachtet werden. Dabei ist die strenge Unterscheidung zwischen den einzelnen Netzwerkschichten sinnvoll. *Ethernet* steht für die MAC-Schicht, *AP-Radio* für die physische Bitübertragungsschicht.

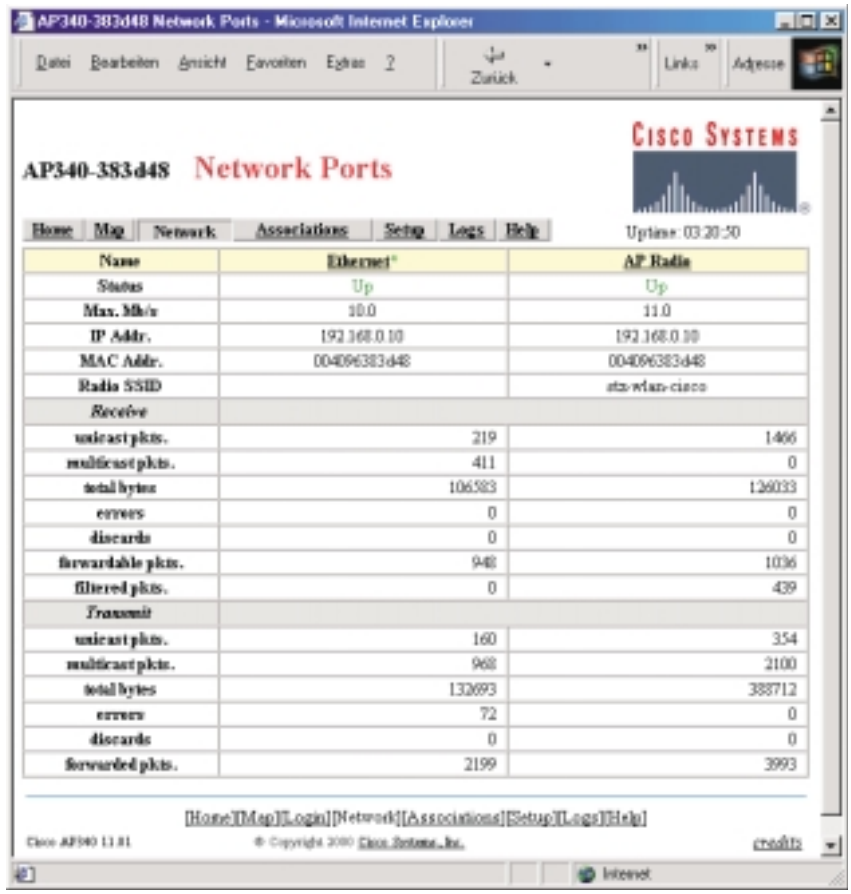


Abbildung 9.6: Aironet AP-Verwaltung von Cisco - Transportcharakteristik der Funkstrecke

Der Zugriff kann auf verschiedene Zugriffsebenen limitiert werden.

- Jeder Zugangspunkt unterstützt eine SSID, die entsprechend auch im Client eingetragen werden muss (vgl. Abschnitt 4.6).
- Die MAC-Adressen der zugelassenen Stationen können eingetragen werden. Hier macht sich ein wesentlicher Sicherheitsaspekt (und dessen Problematik) bemerkbar:
  - Solange die Adressen der Stationen mit Authentifizierung bekannt sind, ist die Eintragung in die Liste der Zugangspunkte unproblematisch. Sobald jedoch eine offene Gruppe Zugang zum Funk-LAN erhalten soll, wie dies im Beispiel in Abschnitt 9.6.3 der Fall ist, wird diese Eintragung unpraktikabel. Ein typischer Ausweg besteht darin, die Limitierung auf Bereiche (*Range*) auszudehnen. Der zunehmende Komfort wird durch einen Verlust an Sicherheit erkauft.
  - Bei der Verwendung mehrerer Zugangspunkte muss jeder Zugangspunkt die MAC-Adressen erhalten. Hier wird die Verwaltung entwe-

der sehr arbeitsaufwändig und fehleranfällig, oder es muss der Einsatz eines RADIUS-Servers in Betracht gezogen werden.

- Ein wichtiges Element der Überwachung der Zugangspunkte besteht darin, die jeweiligen Anmeldungen zu protokollieren, um mit Hilfe von möglichst automatisierten Analysen den Zugriff von nicht erwünschten Teilnehmern feststellen zu können. Abbildung 9.7 zeigt einen Ausschnitt einer solchen Protokoll-Datei, die auf dem Zugangspunkt abgespeichert wird.

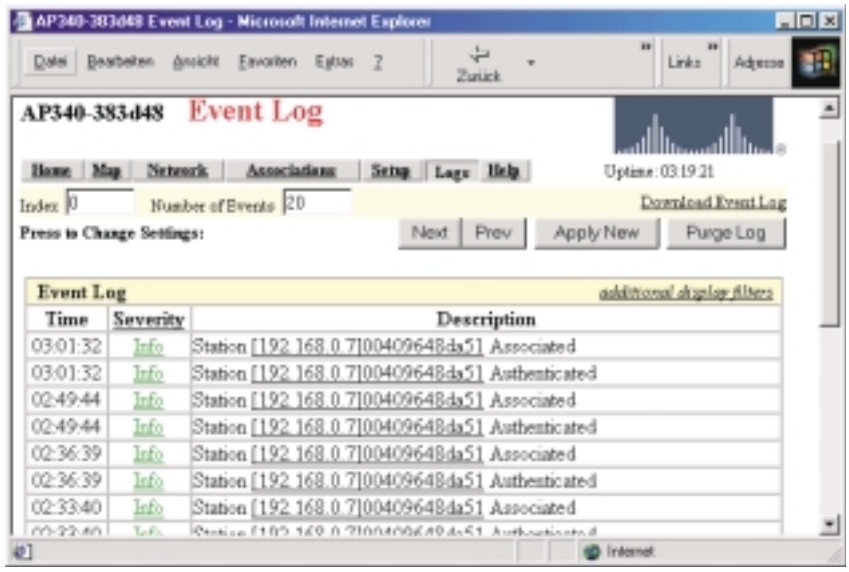


Abbildung 9.7: Aironet AP-Verwaltung von Cisco - Protokollieren aller Ereignisse

- Obwohl der IEEE802.11-Standard keine ***D**ynamic **F**requency **S**election* vorsieht, existieren proprietäre Lösungen, um beim Bootvorgang eines Zugangspunkts nach dem Kanal mit der geringsten Aktivität zu suchen. Ein kompletter Kanalwechsel während des Betriebs ist aber nicht praktikabel, insbesondere dann nicht, wenn Stationen von verschiedenen Herstellern im Netzwerk zum Einsatz kommen.

9.4 Erweiterte Netze

9.4.1 Verbundene Netze

Bei der Abdeckung größerer Gebäude oder Bereiche stellt man oft fest, dass aufgrund der hohen Dämpfung durch Hindernisse und der somit beschränkten Größe der Funkzelle eines einzelnen Zugangspunkts mehrere Funkstationen benötigt werden. Es muss ein verbundenes Netz im Sinne eines ***E**xtended **S**ervice **S**et* (ESS, vgl. Abschnitt 4.2.1) aufgebaut werden.

Der Aufbau eines solchen Netzes ist relativ einfach – insbesondere dann, wenn nur gleichartige Geräte Einsatz finden. Werden unterschiedliche Geräte verwendet oder gar Geräte unterschiedlicher Hersteller, kommt es unter Umständen zu einigen Inkompatibilitäten bei der Administration.

Es ergibt sich der in Abbildung 9.8 schematisch gezeigte Aufbau. Die drei Zugangspunkte AP1 bis AP3 sind räumlich so verteilt, dass sie sich teilweise überlappen. Zielsetzung ist, dass ein mobiler Nutzer, der sich in dem Gebäude bewegt, ohne Veränderung seiner Konfiguration in allen Bereichen auf das Netz zugreifen kann. Hierzu

- arbeiten alle Zugangspunkte auf dem gleichen Kanal,
- erhalten alle Zugangspunkte die identische SSID. Es ist aber auch möglich, den Zugangspunkten verschiedene SSIDs zuzuweisen. Dann müssen diese aber dem mobilen Client bekannt gemacht werden (vgl. Abbildung 9.1).
- erhalten alle Zugangspunkte die identischen WEP-Schlüssel.

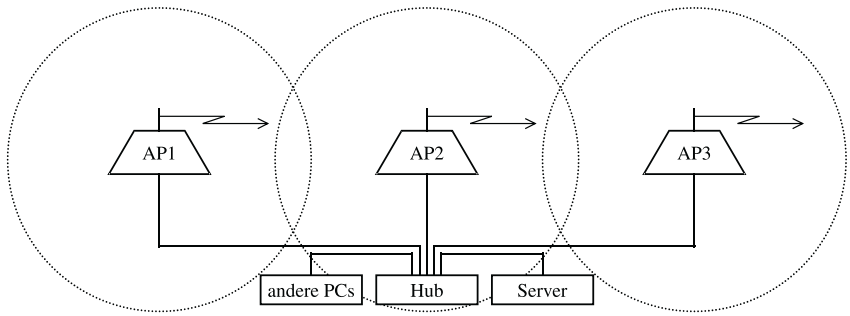


Abbildung 9.8: Betrieb mehrerer Zugangspunkte in nicht oder nur teilweise überlappenden Funkzellen

9.4.2 Strukturierte Netze

Sollen in einem räumlichen Bereich unterschiedliche Arbeitsgruppen zu verschiedenen Domänen zusammengefasst werden, bietet sich folgende Konfiguration an:

- Die Zugangspunkte und damit die Teilnetze arbeiten auf unterschiedlichen Kanälen. Beim Einsatz von DSSS-Systemen nach 802.11b stehen im Wesentlichen die drei nicht überlappenden Kanäle 1, 6 und 11 zur Verfügung.
- Die Zugangspunkte erhalten verschiedene SSIDs.
- Die Zugangspunkte erhalten verschiedene WEP-Schlüssel.

9.4.3 Hohe Nutzerdichten

Sollen Bereiche mit hohen Nutzerdichten, so genannte *Hot Spots*, mit Funknetzen angebunden werden, muss die begrenzte Bandbreite berücksichtigt werden. Typische Anwendungen sind Konferenz- und Klassenräume sowie Warte- oder Messehallen.

Die Einschätzung der maximalen Anzahl von Nutzern, die über einen Zugangspunkt mit einer Brutto-Datenrate von 11 Mbps und einer maximalen Netto-Datenrate im Bereich von 5 bis 6 Mbps arbeiten, hängt in hohem Maße von dem Nutzerverhalten ab. Eine zu große Anzahl von Anwendern bedeutet, dass mehrere Zugangspunkte mit überlappender oder deckungsgleicher Funkzelle parallel eingesetzt werden müssen (vgl. Abbildung 9.9).

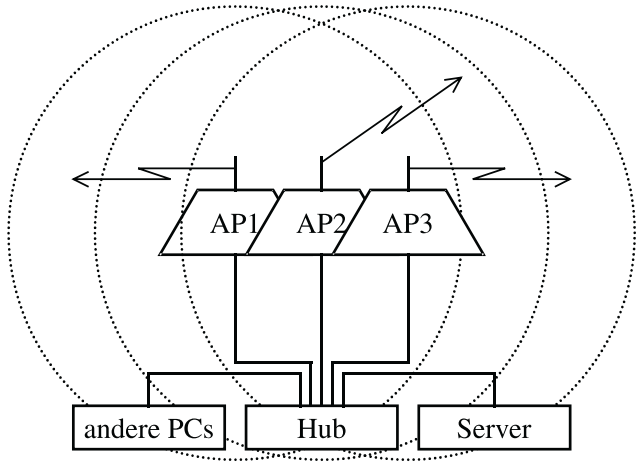


Abbildung 9.9: Betrieb mehrerer Zugangspunkte mit überlappenden oder deckungsgleichen Funkzellen

Zahlreiche der am Markt verfügbaren Zugangspunkte unterstützen für solche Anwendungen ein *Load Balancing*, das die mobilen Stationen den Zugangspunkten in Abhängigkeit der jeweiligen Auslastung zuordnet. Die hierfür notwendigen Signalisierungen sind jedoch in keiner Weise standardisiert, sondern herstellerabhängig. Zur Aushandlung der Zuordnung werden sowohl nicht genutzte Steuerfelder in der Rahmenstruktur (vgl. Abschnitt 4.3.6) als auch spezielle Datenpakete verwendet, die an spezielle MAC-Adressen gesendet werden, die sonst im Netzwerk nicht vorhanden sind. Die Datenpakete enthalten dann ebenfalls die Steuerinformationen.

9.4.4 Verwaltung erweiterter Netze

Die Verwaltung erweiterter Netze stellt hohe Ansprüche, um die Konfigurationen aller beteiligten Stationen konsistent zu halten. Hierzu bietet sich der Einsatz eines ***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*-Servers (RADIUS)

zur Verwaltung an. Diese werden insbesondere von den Herstellern, die sich im professionellen Umfeld positionieren, als ***A**ccess **C**ontrol **S**erver* (ACS) oder als ***A**ccess **P**oint **C**ontroller* (APC) vertrieben.

Problematisch erscheint dabei weiterhin, dass diese Verwaltung proprietäre Bestandteile aufweist.

9.5 Netzwerkanalyse

9.5.1 Übersicht

Bei der Inbetriebnahme und beim Betrieb von Netzwerken ist es sinnvoll und notwendig, zahlreiche Parameter zu berücksichtigen, um eine maximale Leistungsfähigkeit des Netzwerks sicherzustellen. Bei der Administration von Funknetzen unterscheidet man dabei im Wesentlichen zwei Bereiche:

- die Parameter der Bitübertragungsschicht und
- die Parameter des Verkehrsaufkommens auf den logischen Verkehrsschichten.

Zur Analyse der Netzwerke in der Praxis stehen drei grundsätzliche Möglichkeiten offen:

- Der Lieferumfang leistungsfähiger WLAN-Stationen umfasst neben den Werkzeugen zur Administration auch zusätzliche Software zur Analyse der jeweiligen Netzwerkverbindungen.
- Es sind spezielle Analysewerkzeuge am Markt verfügbar, die auf der physischen Grundlage herkömmlicher Hardware einen Überblick über das gesamte drahtlose Funknetz an einem Standort ermöglichen. Diese Werkzeuge bezeichnet man im Allgemeinen als *Sniffer*.
- Und schließlich steht noch dedizierte Hardware zur Verfügung, mit der insbesondere die Charakteristiken der Funkübertragung bestimmt werden können.

9.5.2 Einfache Analysewerkzeuge

Die Leistungsfähigkeit einer Netzwerkverbindung lässt sich am besten anhand der Übertragung von großen Dateien überprüfen (vgl. Abbildung 9.10). Dabei ist aber zu beachten, dass die Geschwindigkeit eines solchen Vorgangs lediglich die Leistungsfähigkeit des gesamten Rechnersystems

beschreibt. So ist beispielsweise bei einer unzureichenden Bandbreite keine Unterscheidung möglich, ob eine Überlastung der Netzwerkverbindung, des sendenden oder des empfangenden Rechners vorliegt.

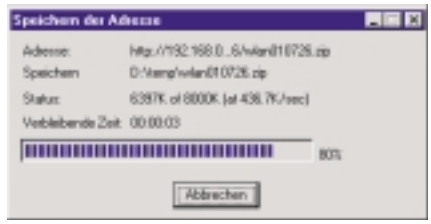


Abbildung 9.10: Beobachtung der Bandbreite auf der Anwendungsebene

Deswegen bedarf es einer getrennten Analyse dieser Bereiche. Hierzu mögen einige typische Beispiele den Leistungsstand der Werkzeuge aufzeigen, die im Lieferumfang leistungsfähiger WLAN-Stationen enthalten sind und die die Analyse der jeweiligen Funkverbindungen erlauben.

- Abbildung 9.11 zeigt den *Link Status Meter* von Cisco, mit dessen Hilfe ein grobes Ausmessen in den räumlichen Gegebenheiten möglich ist.
- Weitere Analysen in Bezug auf fehlerhafte Übertragungen, Geschwindigkeitsstufen etc. zeigt der *3Com Connection Monitor* in Abbildung 9.12.

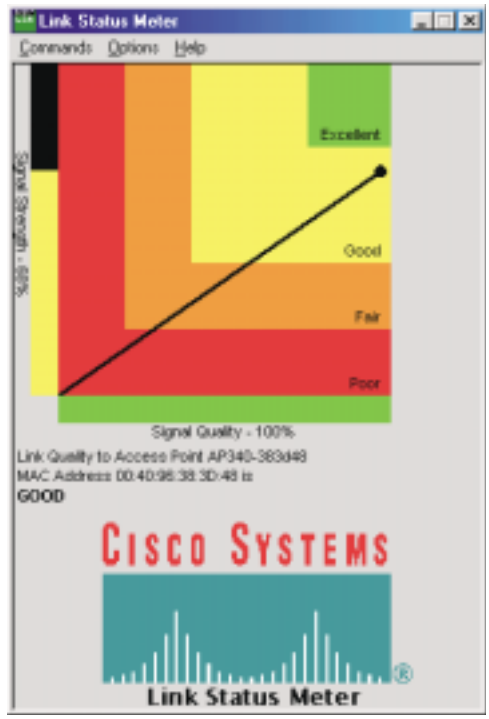


Abbildung 9.11: Informationen über die Charakteristik des Funkfelds

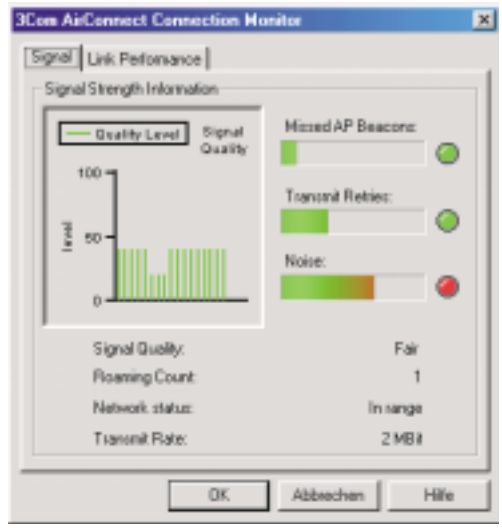


Abbildung 9.12: Weitere Information zu Fehlerrate und Übertragungsgeschwindigkeit

- In fast allen Fällen steht auch ein Werkzeug zur Verfügung, das mit Hilfe des ICMP-Befehls *Ping* die Überprüfung der Erreichbarkeit von Stationen und die Messung der Verzögerungszeit (*Round Trip Time*) der Verbindungen erlaubt. Je nach Leistungsfähigkeit des Werkzeugs können für diese Übertragung aber auch verschiedene Parameter und hierbei insbesondere die Paketgröße eingestellt werden. Unter Umständen stehen auch grafische Auswertungen zur Verfügung (vgl. Abbildung 9.13).

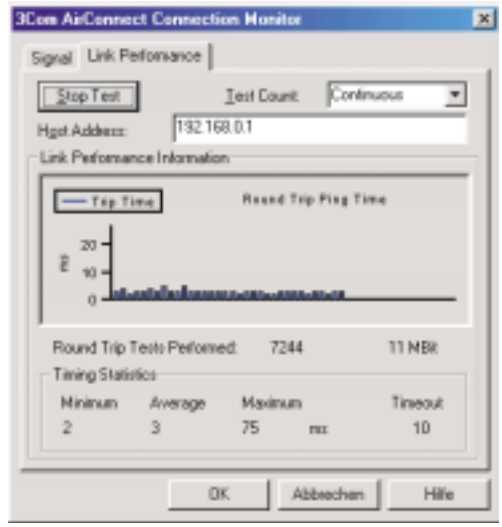


Abbildung 9.13: Integration des Ping-Befehls in die Netzwerkanalyse

9.5.3 Sniffer

Grundlegendes

Unter einem Sniffer (engl. *to sniff*: schnüffeln) versteht man ein spezielles Analysewerkzeug zur Beobachtung von Netzwerkverkehr. Die Bezeichnung geht dabei auf ein Produkt der Firma *Network General* zurück, ist aber nunmehr auch allgemein gebräuchlich. Viele Sniffer greifen auf herkömmliche Netzwerkkarten zurück, nutzen dabei aber oft spezielle Betriebsmodi, die von den Herstellern nicht für alle Anwender freigegeben sind. Grundsätzlich sind zwei Anwendungsbereiche für solche Sniffer zu unterscheiden:

- Analyse eines Netzwerks, um Schwachstellen und Engpässe aufzudecken. Hierzu müssen Verkehrsströme und physische Parameter sichtbar gemacht werden.
- Abhören eines Netzwerks, um sich unerlaubt Informationen zu verschaffen. Aufgrund der fehlenden räumlichen Begrenzung der elektromagnetischen Felder ist dieser kriminelle Aspekt bei drahtlosen Netzen besonders kritisch.

Einige Beispiele sollen einen Einblick in den Leistungsumfang eines solchen professionellen Analysewerkzeugs gewähren. Das WLAN Sniffer von Networks Associates Inc. (NAI, *http://www.nai.com* und *http://www.sniffer.com*) ist unter anderem für den Einsatz mit der Cisco Aironet 340-PC Card entwickelt. Diese nimmt während des Schnüffelns nicht aktiv an der Kommunikation teil, sondern empfängt nur. Um den unmittelbaren Zugriff auf weitere, sonst von Cisco nicht freigegebene interne Register der Netzwerkkarte zu erhalten, muss ein spezieller Treiber installiert werden.

Bei der Beobachtung des Verkehrs auf den Funkkanälen ist aufgrund der räumlichen Verteilung der elektromagnetischen Wellen unbedingt auf die lokale Positionierung der Empfangsantenne zu achten. Besonders vorteilhaft erscheint dabei die Möglichkeit, ein Notebook mit zwei WLAN-Karten auszustatten, wobei eine Karte für die Abwicklung des normalen Verkehrs zum Einsatz kommt, während die zweite für den Sniffer eingesetzt wird. Aufgrund der Antennenbauform ist dies aber nicht mit allen Karten möglich.

Channel Surfing

Um diese Analysen über alle verfügbaren Kanäle zu beobachten, steht ein *Channel Surfing* zur Verfügung, mit dem in bestimmten Zeitabständen die verschiedenen Kanälen in beobachtet werden. Dabei stellt man fest, dass die Frequenzbänder im DSSS-Modus so stark überlappen, dass auch auf den aktiven Kanälen in benachbarten Frequenzbereichen Pakete empfangen und erfolgreich dekodiert werden können (vgl. Abbildung 9.14).

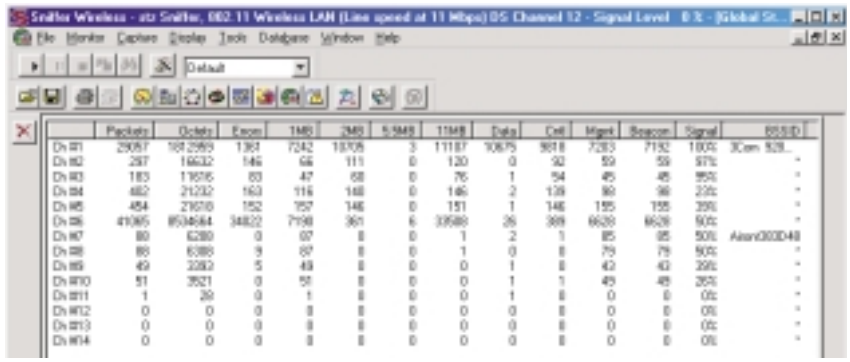


Abbildung 9.14: Aktivitäten der verschiedenen Funkkanäle

Statistiken

Darüber hinaus kann aber auch sehr detailliert das Verkehrs- und das Fehlerverhalten des drahtlosen Netzwerks analysiert werden. Hierzu stellt der Sniffer das in Abbildung 9.15 gezeigte Modul zur Verfügung. Dabei wird deutlich, dass bei einer hohen Auslastung eines Kanals eine sehr hohe Fehlerrate erreicht wird. Diese ist vor allem deswegen so kritisch, weil sie dazu führt, dass die Zeitschlitze, in denen Kollisionen auftreten, nicht zur Übertragung von Nutzdaten verwendet werden können. Bei hoher Auslastung nimmt – wie beim drahtgebundenen Ethernet auch – die nutzbare Kanalkapazität ab.

Einzelanalysen

Für die Analyse von konkreten Fehlern helfen die bisher gezeigten globalen Analysen nur beschränkt. Hierfür ist in den meisten Fällen eine detaillierte Untersuchung der einzelnen Aktivitäten auf dem Funkkanal erforderlich. Zwei Beispiele mögen dies verdeutlichen:

- Abbildung 9.16 zeigt den Anmeldevorgang einer Station an einem Zugangspunkt, wie er in Abschnitt 4.3.7 schematisch beschrieben war.
- Abbildung 9.17 zeigt einen Ausschnitt aus dem Verkehr in einem recht stark belasteten Netz. Bei der Übertragung einer Datei für eine Webseite kann sehr anschaulich nachvollzogen werden, dass nach zwei normalen Übertragungsversuchen (No. 72 und 73), die erfolglos blieben, zwei Versuche unter Zuhilfenahme der *Clear-To-Send* (CTS) und der *Request-To-Send* (RTS) mit der Abfolge der RTS-CTS-Signale stattfinden. Die Abfolge der RTS-CTS-Datenpakete ist in den Schritten 74 bis 76 bzw. 77 bis 79 zu finden. Nach der erfolglosen Durchführung dieser Versuche wird schließlich ein weiterer normaler Übertragungsversuch (No. 80) mit einem ACK in No. 81 bestätigt. Im Ergebnis lässt sich feststellen, dass die erfolgreiche Übertragung von 411 Bytes einen Zeitraum von 8 ms in Anspruch genommen hat. Dies entspricht einer Datenrate von 411 bps.

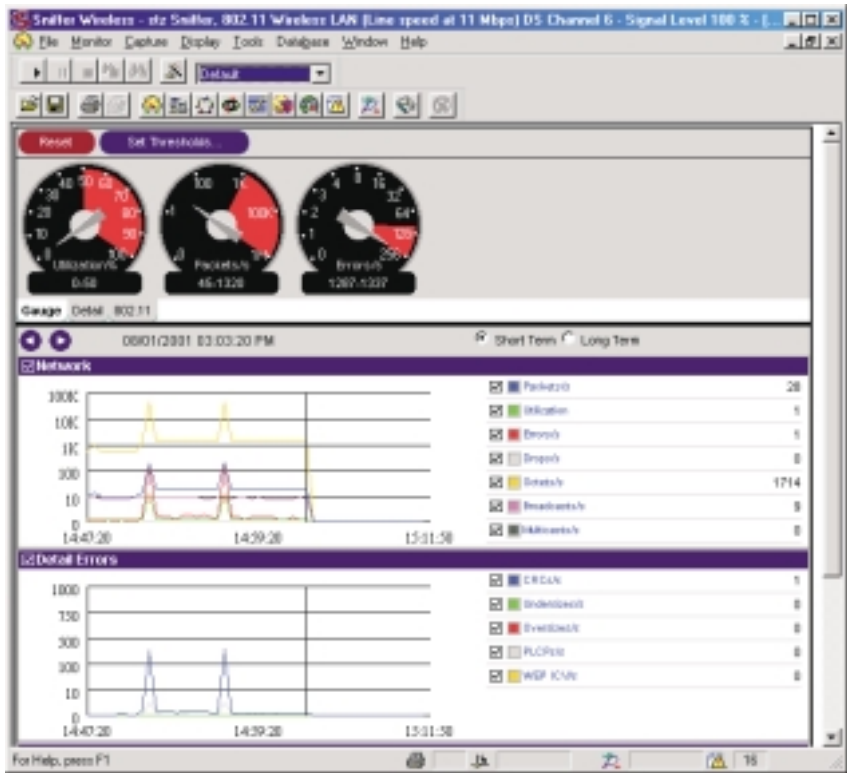


Abbildung 9.15: Analyse des Verkehrsaufkommens und der Fehlerrate

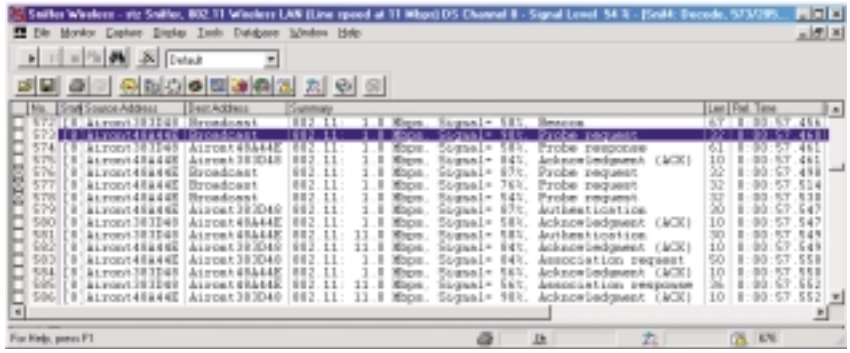


Abbildung 9.16: Trace des Anmeldevorgangs einer Station an einem Zugangspunkt

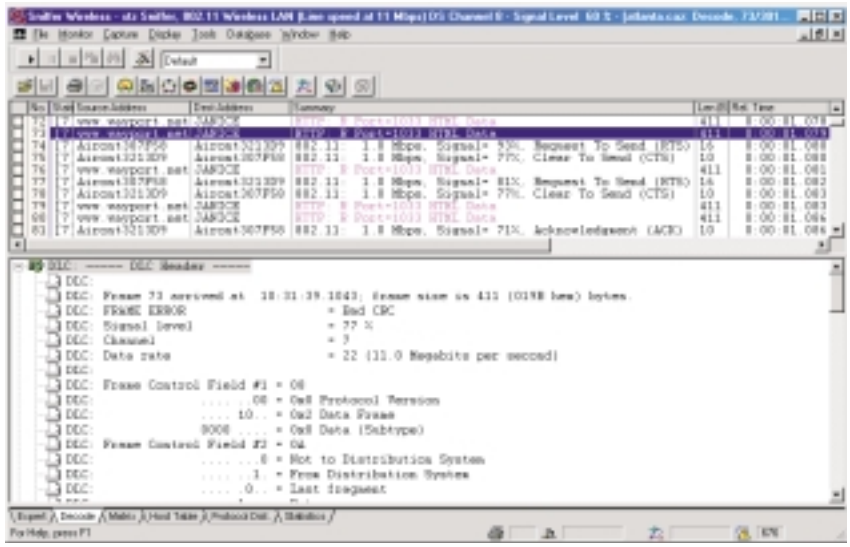


Abbildung 9.17: Trace eines mehrfachen Übertragungsversuchs mittels DCF und PCF

9.6 Praxisbeispiele

9.6.1 LAN-LAN-Kopplung

Ausgangssituation

Bei der Berufsakademie (BA) Lörrach (*http://www.ba-loerrach.de*) handelt es sich um eine Hochschule mit gegenwärtig etwa 1000 Studenten, die Diplom-Betriebswirte (BA), Diplom-Wirtschaftsinformatiker (BA) und Diplom-Ingenieure (BA) ausbildet. Der eigentliche Campus mit zentraler Verwaltung, Rechenzentrum und Laboreinrichtungen befindet sich in mehreren verteilten Gebäuden am Stadtrand. Aufgrund der starken Zunahme der Studentenzahlen wurde Mitte 1999 ein weiteres Gebäude im Stadtgebiet angemietet.

Folgende Rahmenbedingungen sind dabei zu berücksichtigen:

- Aufgrund der räumlichen Situation sollen dort sowohl Büros als auch Unterrichtsräume sowie ein Rechnerraum eingerichtet werden.
- Es besteht keine Sichtverbindung zwischen Campus und Erweiterungsgebäude.
- Um eine ausreichende Trennung zwischen Aktivitäten der Verwaltung und der Dozenten einerseits und der Studenten andererseits zu erreichen, werden zwei getrennte Netze betrieben, die beide am neuen Standort zur Verfügung stehen sollen. Aufgrund der benötigten Anzahl der Studentenaccounts steht insgesamt ein IP-Adressraum aus drei C-Klassen zur Verfügung.

Realisierung

Die in Abbildung 9.18 gezeigte Realisierung wurde im Herbst 1999 installiert:

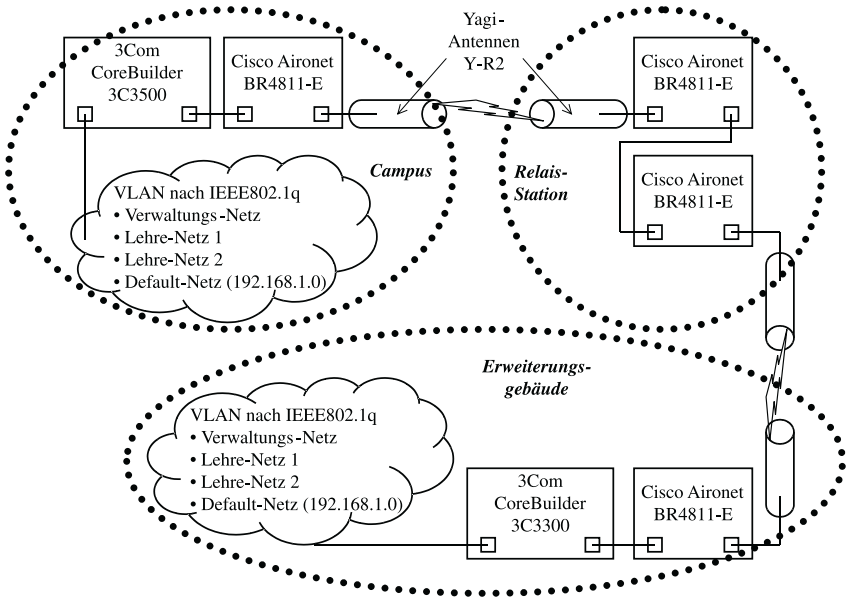


Abbildung 9.18: Funkbrücke zur LAN-LAN-Kopplung zweier Teilnetze

- Die drei Netze werden über ein virtuelles LAN auf einem physischen Kanal gebündelt.
- Dieser wird mit Hilfe einer IEEE802.11b-kompatiblen Funkstrecke in das Erweiterungsgebäude transportiert. Dabei nutzt man eine zusätzliche Relaisstation auf einem hohen öffentlichen Gebäude in der Stadt.
- Insgesamt werden also vier aktive Elemente und Antennen benötigt.

Erweiterungsmöglichkeiten

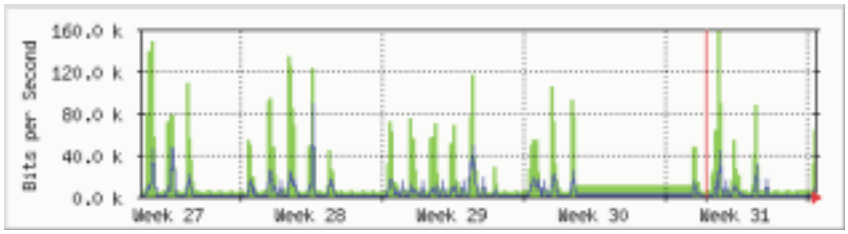


Abbildung 9.19: Verkehrscharakteristik der Funkbrücke im Zweistundenmittel

Die in Abbildung 9.19 gezeigte Nutzungscharakteristik im Zweistundenmittel zeigt einen typischen periodischen Verlauf. Das größte Verkehrsaufkommen ist dabei der Nutzung eines Rechnerraums mit 28 Arbeitsplätzen zuzuordnen.

Da bei der Spitzenauslastung die Funkbrücke einen Engpass darstellt, ist zu überlegen, welche Erweiterungsmöglichkeiten zur Verfügung stehen. Hier sind gegenwärtig vier Szenarien denkbar:

- Die Aufrüstung auf ein Funkmodul im 2,4 GHz-Bereich und eine Datenrate von 22 Mbps. Die fehlende Konformität zu einem zukünftigen Standard IEEE802.11g ist im Bereich von Punkt-zu-Punkt-Systemen wie bei einer hier gezeigten Funkbrücke nicht als grundlegendes Problem einzuordnen.
- Die Nutzung einer Funkbrücke im HiperLAN/2-Standard im 5 GHz-Bereich und eine Brutto-Datenrate von 54 Mbps. Kommerzielle Produkte werden aber nicht vor Mitte 2002 zur Verfügung stehen.
- Die Aufrüstung auf eine Richtfunkstrecke. Diese kann zwar deutlich größere Bandbreiten erreichen, ist aber im Bereich der Investitionen wesentlich höher anzusiedeln und darüber hinaus auch melde- oder genehmigungspflichtig.
- Die Nutzung von bis zu drei parallelen Funkstrecken. Der IEEE802.11b stellt drei nichtüberlappende Frequenzbereiche zur Verfügung, die durch ein *Load Balancing* auf der dritten Netzwerkebene ausgelastet werden können.

9.6.2 Mobiler Rechnerraum

Ebenfalls im Umfeld und in den Räumen der Berufsakademie Lörrach findet sich eine zweite Installation mit einer typischen Anwendung, die hier vorgestellt werden soll.

Im Rahmen eines Fortbildungsprojekts, das gemeinschaftlich von der IHK Oberrhein-Bodensee und dem Steinbeis-Transferzentrum für Business-Consulting an der Berufsakademie Lörrach durchgeführt wird, werden IT-(e)-NetAdministratoren ausgebildet. Für diesen Ausbildungsgang wurde ein mobiler Rechnerraum eingerichtet, der aus zehn Mini-Desktop-PCs besteht und in jedem beliebigen Unterrichtsraum aufgebaut werden kann, der über einen drahtgebundenen Netzwerkanschluss verfügt. Die Verbindung mit dem Netzwerk wird mit Hilfe eines WLAN-Netzwerks nach IEEE802.11b und einem Zugangspunkt realisiert.

9.6.3 Wechselnde Stationen im Hotel

Das Hotel am Rathaus in Freiburg (*http://www.am-rathaus.de*) ist ein in Familienbesitz geführtes Hotel in zentraler Lage der Freiburger Altstadt. Zusätzlich zu vielen anderen zeitgemäßen Diensten der elektronischen Kommunikation bietet das Haus mit dem Internet-Zugang für Gäste eine zusätzliche Dienstleistung, die in vielen modernen Hotels und Kongresszentren verfügbar ist.

Dabei erfolgt die Netzwerkverbindung für die Gäste mit Hilfe eines WLAN-Netzes nach IEEE802.11Bit. Hierzu kann entweder ein komplettes Notebook oder auch nur eine WLAN-Karte zur Installation im eigenen Notebook ausgeliehen werden.

Die räumlichen Gegebenheiten erlauben die komplette Ausleuchtung einer Etage mit einem Access-Point, so dass sich der in Abbildung 9.20 gezeigte sehr einfache Aufbau ergibt. Die Anbindung des gesamten Hotelnetzes an den Internet-Provider erfolgt ebenfalls über ein IEEE802.11b-System im Rahmen einer Punkt-zu-Punkt-Funkbrücke. Die Trennung des Verkehrs erfolgt durch einen Router.

Im Hotelbereich müssen vier Wohnetagen und das Erdgeschoss mit dem Rezeptionsbereich abgedeckt werden. Dabei reicht das Funknetz auch in den Cafébereich vor dem Hoteleingang, so dass die Gäste auch im Freien die Internet-Anbindung nutzen können. Bislang ist es nicht geplant, den Internet-Zugang auch Cafégästen anzubieten, die nicht Hotelgäste sind. Die Zugangsbeschränkung erfolgt über die Netzwerkkennung.

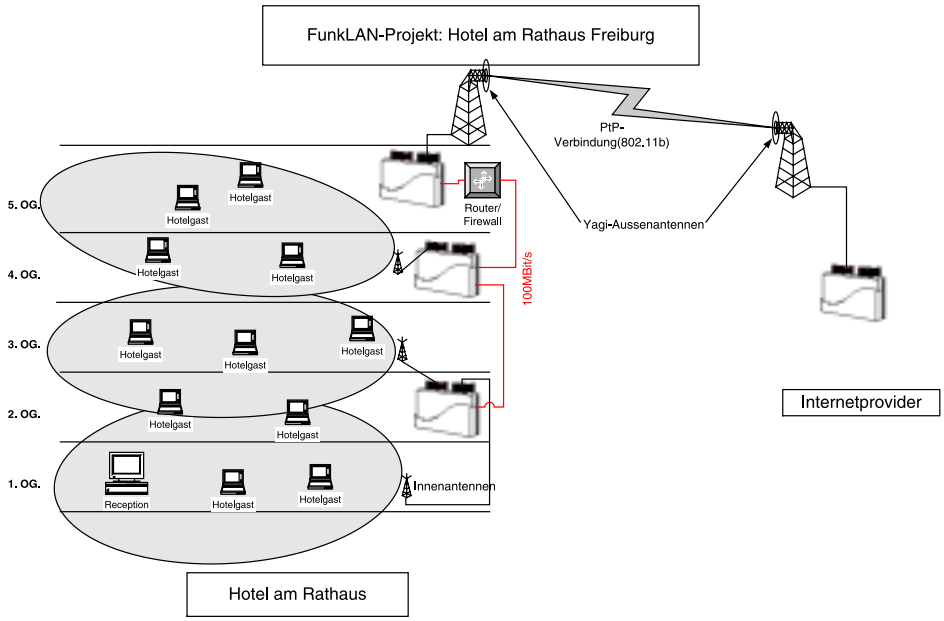


Abbildung 9.20: Architektur der Abdeckung im Hotel am Rathaus, Freiburg (mit freundlicher Genehmigung der Netlight GmbH)

10 Verschiedene Aspekte

10.1 Sicherheit

10.1.1 Grundlegendes

In diesem Abschnitt werden verschiedene Sicherheitsaspekte des IEEE802.11-Protokolls aufgezeigt, die Gegenstand heftiger Auseinandersetzungen sind. Dabei werden sowohl die technologischen Grundlagen als auch die möglichen Risiken diskutiert und eine mögliche Bewertung vorgeschlagen. Kernpunkt der Diskussion ist das im Rahmen des IEEE802.11 eingesetzte ***W**ired **E**quivalent **P**rivacy* (WEP), wie es in Abschnitt 4.6 vorgestellt wurde.

10.1.2 Sicherheitsrisiken

Die Verwendung eines statischen Schlüssels ist zwar vergleichsweise recht einfach zu realisieren, birgt aber ein signifikantes Sicherheitsrisiko, da nach Bekanntwerden des Schlüssels kein weiterer Schutz mehr gegeben ist. Dabei sind zwei grundsätzliche Möglichkeiten zu unterscheiden, an einen statischen Schlüssel zu gelangen:

- Erstens kann der Schlüssel über den menschlichen Weg bekannt werden. Dies ist insbesondere dann kritisch, wenn in einem ganzen Unternehmen alle Stationen den identischen statischen Schlüssel besitzen.

  Allerdings ist das Auslesen der Schlüssel an den mobilen Stationen meist nicht unmittelbar möglich, da der Schlüssel auf der Karte in einem nichtflüchtigen Speicher abgelegt wird.

- Zweitens kann durch verschiedene Algorithmen von extern versucht werden, den Schlüssel zu rekonstruieren.

Hinzu kommt, dass die Verschlüsselung im Rahmen des IEEE802.11 nicht nur für die Verschlüsselung der zu übertragenden Informationen eingesetzt wird, sondern auch Anwendung im Rahmen der in Abschnitt 4.3.7 beschriebenen Authentifizierung von Stationen findet. Die Kenntnis des Schlüssels kann also auch das Eindringen in ein Netzwerk erleichtern.

10.1.3 Angriffe

Im Wesentlichen lassen sich vier Arten von Angriffen unterscheiden:

- *Passives Abhören:* Durch reines Abhören und Beobachten der übertragenen Textmuster können Rückschlüsse auf den verwendeten Schlüssel gezogen werden. Dies gilt insbesondere dann, wenn Teile der Inhalte bzw. der Struktur des übertragenen Textes bekannt sind. Beispielsweise weist TCP/IP das in Abschnitt 2.2.1 erläuterte feste Rahmenformat auf. Ansätze für verwendete Algorithmen werden auch in [Fluhrer 2001] gegeben.

  Darüber hinaus kann ein Angreifer, der zwei mit demselben Schlüssel chiffrierte Texte empfängt, über eine Exklusiv-Oder-Verknüpfung statistische Information über den verwendeten Schlüssel gewinnen [Borisov (1)].

  Voraussetzungen für das Abhören bei den unterschiedlichen im WLAN-Bereich eingesetzten Frequenzspreiztechniken werden in Abschnitt 10.3 diskutiert.

- *Einseitiges Senden:* Durch das Einführen von bekanntem unverschlüsselten Text und Abhören des verschlüsselten Textes können Rückschlüsse auf den zugrunde liegenden Schlüssel erfolgen.

  Dabei reicht es unter Umständen aus, wenn es einem Angreifer gelingt, ein Bit in dem verschlüsselten Text zu verändern. Dann ergibt sich eine Veränderung auch des entschlüsselten Texts, die Aufschlüsse über den verwendeten Schlüssel zulässt [Borisov (1)].

- *Beidseitiges Senden:* Durch die Kenntnis und die entsprechende Veränderung der Header-Informationen können sowohl Rückschlüsse auf den zugrunde liegenden Schlüssel als auch Umleitungen der Pakete auf eigene Maschinen erfolgen [Borisov (2)].

- *Tabellenbasierter Angriff:* Die Tatsache, dass nur ein vergleichsweise geringer Umfang an Initialisierungsvektoren zur Verfügung steht, erlaubt einem Angreifer mit vergleichsweise geringem Aufwand den Aufbau einer Entschlüsselungstabelle.

Zur Verhinderung dieser Angriffe sind in WEP zwei zusätzliche Maßnahmen vorgesehen.

- Der verschlüsselte Text wird durch die Übertragung redundanter Information mittels eines ***C****yclic* ***R****edundancy* ***C****heck* (CRC) gegen Veränderung geschützt. Da der CRC aber linear implementiert ist, kann bei einer Veränderung des Bitstroms auch recht einfach das Ergebnis des CRC angepasst werden, so dass der Empfänger die Veränderung nicht bemerkt.

- Um die Übertragung von zwei unterschiedlichen Datenströmen mit dem gleichen Schlüssel zu verhindern, beginnt der Sender die Verschlüsselung mit einem ***I****nitialisierungs****v****ektor* (IV), der verändert wird. Allerdings ist die Veränderung des IV mit jedem Paket im IEEE802.11 nur optional

vorgesehen. Hinzu kommt, dass die Algorithmen zur Auswahl des IV vergleichsweise einfach nachzuvollziehen sind und die Anzahl der möglichen IV beschränkt ist, so dass auch diese Hürde recht einfach genommen werden kann.

10.1.4 Dynamische Verwaltung der Verschlüsselung

Um die Problematik bei der Verwendung statischer Schlüssel zu umgehen, besteht die Möglichkeit, den Schlüssel im Rahmen eines zusätzlichen Algorithmus zu wechseln. Hierfür haben verschiedene führende Hersteller eine proprietäre Erweiterung entwickelt, die eine Zuordnung verschiedener Schlüssel für jeden Nutzer und jede Sitzung nach dem so genannten Diffie-Hellman-Verfahren erlaubt. Die Eintragung von mehreren Schlüsseln ist in Abbildung 10.1 beispielhaft gezeigt.

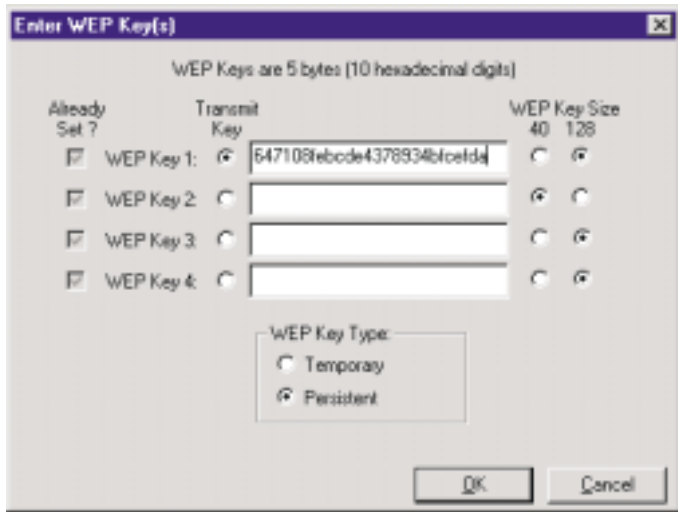


*Abbildung 10.1: Eintragung von maximal vier möglichen Schlüsseln für eine PC-Card im Rahmen des **C**lient **E**ncryption **M**anager (CEM) von Cisco Systems, Inc.*

10.1.5 Fazit

Drahtlose Netze im Rahmen des IEEE802.11-Standards bieten nur unzureichend Schutz gegen Abhören und unter Umständen auch gegen das Eindringen in das Netz. Allerdings ist festzuhalten, dass für dieses Eindringen durchaus ein tiefes Verständnis sowie ausreichend kriminelle Energie notwendig sind, wenn die zur Verfügung stehenden Sicherheitsmechanismen ausgeschöpft werden. Ein potenzieller Angreifer wird also in jedem Fall bewerten müssen, ob ein Eindringen so attraktiv sein kann, dass er die erforderliche Energie aufbringt.

Darüber hinaus weist die WECA in einer Darstellung (WECA, »802.11b Wired Equivalent Privacy (WEP) Security«) deutlich darauf hin, dass das größte Sicherheitsrisiko darin besteht, dass die zur Verfügung stehenden

Maßnahmen nicht ausreichend genutzt werden. Dieser Beobachtung lässt sich uneingeschränkt zustimmen. Ein populäres Beispiel aus der Schweiz ist unter [Mazzara 2001] verfügbar.

10.1.6 Sicherheitsmaßnahmen

Auf jeden Fall sind folgende Maßnahmen zu empfehlen, um die drahtlosen Netze nicht zu einem Einfallstor in das Netzwerk zu machen:

- *Einsatz der WEP-Verschlüsselung:* Auch wenn oben festgestellt wurde, dass WEP keinen absoluten Schutz darstellt, verhindert es jedoch einfaches Abhören und erhöht die Schwelle des Zugriffs ganz erheblich. Allerdings ist festzustellen, dass der praktische Einsatz der WEP-Verschlüsselung Einschränkungen bei der Interoperabilität zur Folge hat [Ahlers 2000].
- *Kein SSID-Broadcast:* Auf diese Weise wird verhindert, dass die Nachrichten eines Access-Points außerhalb der definierten Netzdomäne empfangen werden können. Allerdings ist zu beachten, dass die Stationen, bei denen die Option »any« möglich ist, dennoch empfangen können. Auch Sniffer sind von dieser Einschränkung nicht betroffen.
- *Beschränkung der mobilen Stationen:* Es besteht die Möglichkeit, die Anmeldung (*Association*) mobiler Stationen mit Hilfe der MAC-Adresse zu limitieren. Dies stellt aber keinen Schutz gegen Abhören durch Sniffer dar.
- *Beschränkung der Administrationsrechte:* Die Zugangsrechte für die Verwaltung der Access Points lassen sich bei den meisten Produkten sehr detailliert einstellen. Auch die Zugriffsarten kann man beschränken. Insbesondere die Verwaltung über das ***S**imple **N**etwork **M**anagement **P**rotocol* (SNMP) kann in vielen Anwendungen beschränkt werden.
- *Nutzung von weiteren proprietären Sicherheitsmaßnahmen:* Neben diesen allgemeinen Maßnahmen sollten die von den Herstellern zusätzlich angebotenen Sicherheitsmechanismen aktiviert werden. Allerdings ist dies in heterogenen Netzwerken mit Geräten unterschiedlicher Hersteller nur eingeschränkt möglich.
- Darüber hinaus sollten weitere Sicherheitsmechanismen der höheren Protokollebenen wie z.B. IPSec eingesetzt werden.

10.2 Störeinflüsse

10.2.1 Gliederung

Bei der Analyse der aktiven Störeinflüsse für die jeweiligen Systeme (vgl. auch Abschnitt 2.2.3) müssen folgende Quellen berücksichtigt werden:

- Wenn sich ein Empfänger in der Reichweite von zwei oder mehreren gemeinsam betriebenen Funkzellen befindet, muss er zwei Aufgaben lösen. Er muss eine Zuordnung zu einer der Funkzellen treffen und die Signale der anderen Funkzellen unterdrücken.
- Wenn andere Kommunikationsteilnehmer mit dem identischen Protokoll aktiv sind, ohne dass sie zu dem gleichen Netzwerk gehören, muss dennoch ein möglichst unabhängiger Betrieb aller Stationen gewährleistet werden.
- Insbesondere in den anmeldungsfreien Frequenzbereichen kann es passieren, dass andere Kommunikationsteilnehmer, die nach anderen Protokollen arbeiten, auf den gleichen Frequenzen aktiv sind. Auch dann muss ein möglichst unabhängiger Betrieb der unterschiedlichen Netze unterstützt werden.
- Schließlich müssen auch noch Störungen durch andere Systeme berücksichtigt werden. Hier sind drei Bereiche zu unterscheiden:
  - Andere funkbasierte Kommunikationsnetze, wie GSM oder Radio- und Fernsehsender, die in einem anderen Frequenzbereich betrieben werden.
  - Andere mikroelektronische Systeme, die aufgrund ihres schnellen Schaltverhaltens elektromagnetische Strahlung aussenden. Hierzu zählen schnell getaktete mikroelektronische Bauelemente wie Mikrocontroller oder Mikroprozessoren, aber auch Bauelemente der Leistungselektronik.
  - Andere Geräte, die aufgrund ihrer Betriebseigenschaften elektromagnetische Strahlung aussenden. Hier sind insbesondere Bildröhren in Fernsehgeräten und Bildschirmmonitoren sowie Mikrowellenherde zu nennen.

10.2.2 Beeinflussung durch identische Systeme

Die Frage nach der Beeinflussung durch Systeme, die nach dem gleichen Standard arbeiten, aber in unabhängigen Netzwerken betrieben werden, entspricht der Diskussion um die räumliche Wiederholfrequenz, die in Abschnitt 10.3 besprochen wird.

10.2.3 Beeinflussung durch konkurrierende Systeme

Für den Fall, dass im Bereich des lizenzfreien 2,4 GHz-Bands verschiedene nicht koordinierte Netze mit unterschiedlichen Protokollen betrieben werden, ist eine Erhöhung der Störleistung zu erwarten. Als vielleicht typischstes Beispiel können Computer dienen, die ihre Netzwerkfunktionalität mit Hilfe von Funknetzen nach IEEE802.11b realisieren und gleichzeitig über Bluetooth die Verbindung zu Peripheriegeräten aufbauen. Dieses Beispiel ist auch besonders kritisch, da der Abstand der jeweiligen Antennensysteme

denkbar gering ist. Im schlimmsten Fall befinden sich die PC-Cards für IEEE802.11b und für Bluetooth in den benachbarten Schächten des Notebooks.

Es sind bereits zu einem sehr frühen Zeitpunkt verschiedene Modelle zur Einschätzung der gegenseitigen Beeinflussung angefertigt worden [Zyren 1999 (2), Lansford 2000]. Die Ergebnisse dieser Studien basieren auf einer Vielzahl von Parametern. Zusammenfassend lässt sich feststellen, dass

- die Beeinflussung der Systeme vernachlässigbar ist, wenn der Abstand der konkurrierenden Geräte ausreichend groß ist;
- die Beeinflussung der Systeme durchaus bemerkbar werden kann, wenn die konkurrierenden Geräte sehr nah beieinander angeordnet sind;
- dass die Beeinflussung der Systeme neben einer Beeinträchtigung der Geschwindigkeit [Merritt 2001] die Funktionalität auch ganz unmöglich macht.

Beim praktischen Einsatz müssen jedoch folgende Hinweise zusätzlich beachtet werden:

- Die Tatsache, dass insbesondere die benachbarte räumliche Anordnung konkurrierender Systeme die Übertragung behindern kann, kann bei vielen zukünftigen Anwendungen zu Problemen führen, denn gerade Notebooks werden gleichermaßen über einen drahtlosen Anschluss an das Netzwerk wie über drahtlose Verbindungen zu den Peripheriegeräten verfügen. Deswegen wird durchaus über eine Kopplung verschiedener Standards im Allgemeinen und IEEE802.11x und Bluetooth im Speziellen nachgedacht [Shoemake 2001].
- Die Tatsache, dass die Interferenz der 2,4 GHz-Systeme zum gegenwärtigen Zeitpunkt nur eine untergeordnete Rolle spielt, darf nicht zu der Auffassung verleiten, dass dieses Problem nicht existiert. Denn Systeme, die in offenen Bereichen auf der Grundlage von FDMA arbeiten, werden von diesen Überlagerungen in besonderer Weise dann betroffen sein, wenn keine dynamische Frequenzauswahl (DFS) unterstützt wird. Solange sich die Systeme innerhalb einer Administrationsdomäne befinden, kann die Problematik durch eine Funkplanung entschärft werden. Wenn aber in dicht besiedelten Gebieten Interferenzen von benachbarten Wohneinheiten oder Büroetagen aufgrund gleicher Frequenzauswahl zu beobachten sind, können sich lästige Probleme ergeben.

10.2.4 Beeinflussung durch andere Funknetze

Eigene Untersuchungen bezüglich der gegenseitigen Beeinflussung von Funknetzen, die in anderen Frequenzbereichen eingesetzt werden, und Wireless-LAN-Systemen im 2,4 GHz zeigten, dass hier erwartungsgemäß keinerlei Einschränkungen berücksichtigt werden müssen.

Dies gilt sowohl für GSM-Mobiltelefone, die im 900 MHz-Bereich arbeiten, als auch für DECT-Netze im 1,9 GHz-Bereich.

10.2.5 Beeinflussung durch andere Störsender

Eigene Untersuchungen zeigten bei verschiedenen Systemen nach IEEE802.11b und mehreren handelsüblichen Mikrowellenherden keine Beeinflussung der Übertragungsqualität, solange praktikable Abstände eingehalten wurden. Nur bei sehr geringen Abständen von weniger als etwa 20 cm ließ sich ein leichter Anstieg des Rauschpegels beobachten, der jedoch in keinem Fall zu einer Verringerung der Datenrate führte.

10.3 Wahl des Frequenzspreizverfahrens

10.3.1 Grundlegendes

Die Auswahl der Funkübertragungstechnologie bestimmt im Allgemeinen auch die Wahl des Frequenzspreizverfahrens. Während den Anwender nur die Leistungsparameter des Gesamtsystems interessieren, hat sich bei den Befürwortern der verschiedenen Technologien in manchen Fällen geradezu ein Glaubenskrieg um die Vor- und Nachteile von Frequenzspreizverfahren (FHSS) und Direct-Sequence-Spread-Spectrum-Verfahren (DSSS) entwickelt. Hierfür sind im Wesentlichen zwei Gründe verantwortlich:

- In der Zeit, als lediglich der IEEE802.11-Standard bestand, nutzten die verschiedenen Hersteller die beiden unterschiedlichen Frequenzspreizverfahren und versuchten, mit der Argumentation die Leistungsfähigkeit der eigenen Produkte zu begründen.
- Nach der Verabschiedung des IEEE802.11b-Standards, der ja ein DSSS-Verfahren nutzt, verstummte die Diskussion zunächst, denn mit einem FHSS-Verfahren konnten nur geringere Datenraten erreicht werden. Nachdem die FCC aber die in Abschnitt 7.4.2 dargestellte Erweiterung der FHSS-Regularien genehmigt hat, befinden sich die Hersteller von HomeRF-Produkten im FHSS-Lager, während die Hersteller von IEEE802.11b-kompatiblen Produkten die Vorteile von DSSS propagieren.

10.3.2 Spektrale Effizienz

DSSS-Systeme, wie sie für WLAN-Systeme eingesetzt werden, weisen eine vergleichsweise geringe spektrale Effizienz auf. Beim Vergleich der 1 Mbps-Systeme des IEEE802.11 mit DSSS- bzw. FHSS-Verfahren stellt man fest, dass DSSS eine Bandbreite von 22 MHz und FHSS von 1 MHz pro Kanal beansprucht.

Dennoch kann die räumliche Wiederholfrequenz in vielen praktischen Anwendungsfällen bei DSSS-Systemen höher gewählt werden als bei FHSS-Systemen (vgl. Abbildung 10.2). Je nach Größe der Fläche verkleinert sich jedoch der Unterschied.

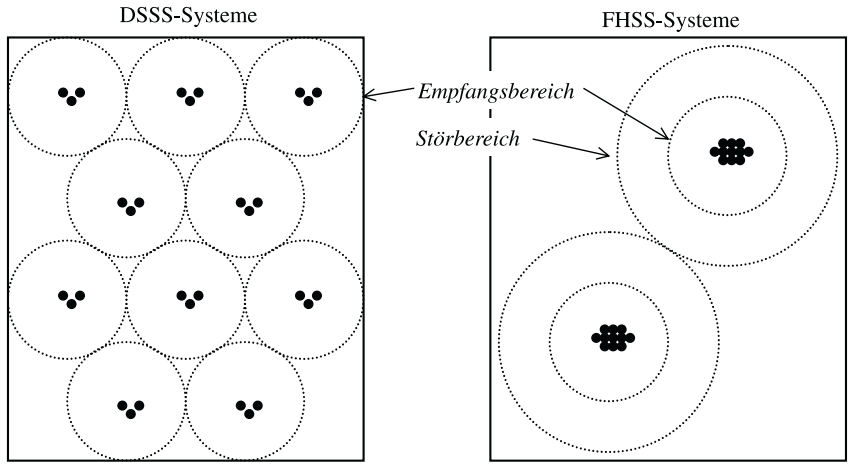


Abbildung 10.2: Räumliche Aufteilung von DSSS- und FHSS-Systemen

10.3.3 Sicherheit gegen Abhören

Bezüglich der oft vertretenen Auffassung, dass Frequenzsprungverfahren schwieriger abzuhören seien als Direct-Sequence-Verfahren, ist anzumerken, dass beide Systeme im Wireless-LAN-Bereich eingesetzt werden, um die Vorgaben des FCC zu erfüllen und nicht, um die Sicherheit der Systeme zu steigern. Dies führt dazu, dass die jeweils erlaubten Zufallsfolgen (PRS) öffentlich bekannt sind.

- Bei den DSSS-Systemen nach IEEE802.11 wird ohnehin nur eine PN-Sequenz eingesetzt. Auch bei der Verwendung des IEEE802.11b sind die möglichen Sequenzen allgemein bekannt.
- Bei den langsamen FHSS-Systemen nach IEEE802.11 oder HomeRF sind die erlaubten Frequenzfolgen ebenfalls im Standard beschrieben. Auf diese Weise kann durch vergleichsweise einfache Auswertung der zeitlichen Abstände der Steuersignale auf einigen verschiedenen Kanälen die verwendete Frequenzsprungfolge bestimmt werden [Zyren 2001 (3)].

Im Ergebnis lässt sich festhalten, dass grundsätzlich das Abhören beider Systeme vergleichsweise einfach möglich ist. Die Erkennung von FHSS-Signalen scheint dabei zunächst jedoch etwas höheren Aufwand zu bedeuten.

10.3.4 Störanfälligkeit

Die Empfindlichkeit gegen die unterschiedlichen in Abschnitt 10.2 aufgeführten aktiven Störquellen werden kontrovers diskutiert. Die hierfür notwendigen Grundlagen können Abschnitt 2.7 entnommen werden. Es liegen verschiedene Simulations- und Testergebnisse vor, die letztlich darauf hindeuten, dass im Wesentlichen die Implementierungen auf Systemebene die Leistungsfähigkeit und die Störanfälligkeit bestimmen [HomeRF Working Group].

10.4 Aspekte der EMV-Belastung

10.4.1 Grundlegendes

Die biologischen Auswirkungen hochfrequenter elektromagnetischer Felder sind ein umstrittenes Thema. Dies gilt zum einen für die wissenschaftliche Untersuchung der tatsächlichen Auswirkungen, die bislang noch keine eindeutigen Ergebnisse bereitstellen konnte. Zum anderen ist das Thema mittlerweile emotional aufgeladen und politisch besetzt. Deswegen sollen an dieser Stelle lediglich einige Aspekte aufgezeigt werden, deren Bewertung dem Leser überlassen wird. Dabei spielt insbesondere der Vergleich mit GSM-Mobilfunk eine Rolle. Dies wird aber nur denjenigen Anwendern helfen, die GSM als unkritisch erachten.

10.4.2 Regularien

Grundsätzlich ist festzuhalten, dass alle drahtlosen LAN-Systeme den jeweiligen nationalen Vorschriften über Sendeleistungen und Feldstärken entsprechen. Wie die meisten Länder folgt die Bundesrepublik Deutschland dabei den Empfehlungen der Internationalen Kommission zum Schutz vor nichtionisierender Strahlung (***I**nternational **C**ommission for **N**on-**I**onizing **R**adiation **P**rotection* – ICNIRP) (*http://www.icnirp.de*). Als Bezugsgröße bei der Festlegung dient die so genannte ***s**pezifische **A**bsorptions**r**ate* (SAR), die die aufgenommene Leistung pro Kilogramm Körpermasse beschreibt. Sie berücksichtigt damit in besonderer Weise den thermischen Effekt durch die Umwandlung der absorbierten Leistung in Wärme. Um die Erwärmung des Körpers für die Allgemeinbevölkerung auf deutlich unter 0,1 Kelvin zu begrenzen, legte die 26. Bundesimmissionsschutz-Verordnung (BImSchV) einen SAR-Wert von 0,08 W/kg zugrunde. Dies entspricht maximalen elektrischen Feldstärken von 42 beziehungsweise 58 V/m [Wuschek 2001].

Zwei spezielle Anwendungsfälle können noch hervorgehoben werden:

- Der Einsatz von Systemen nach IEEE802.11 im medizinischen Bereich ist grundsätzlich zugelassen. Allerdings ist hierfür noch einmal eine gerätespezifische Zulassung zu beantragen. Durchgeführte Tests zeigen auch keine negativen Auswirkungen auf die Funktion von Herzschrittmachern [Cisco Systems, Inc.].
- Der Einsatz von Bluetooth-Systemen in Flugzeugen der zivilen Luftfahrt wird angestrebt und als möglich erachtet.

10.4.3 Vergleich mit GSM-Mobilfunk

Im Vergleich mit GSM-Mobilfunksystemen sind folgende Aspekte zu berücksichtigen:

- *Sendeleistung:* Die maximale Sendeleistung der meisten drahtlosen lokalen Netze ist auf 100 mW beschränkt. Im Vergleich zu den maximal erlaubten 2 W im GSM-Mobilfunk ist hier also ein Unterschied von mehr als einer Größenordnung zu verzeichnen. Allerdings weisen die GSM-Systeme eine dynamische Leistungsanpassung auf, so dass in den meisten Fällen die Sendeleistung der GSM-Stationen deutlich unter diesem Maximalwert liegt.
- *Positionierung:* Darüber hinaus ist zu berücksichtigen, dass die Antenne der GSM-Mobiltelefone in vielen Fällen in unmittelbarer Nähe des Kopfes betrieben wird. Dies ist bei den meisten WLAN-Anwendungen nicht der Fall.
- *Aktivität:* Ein Vergleich der Aktivität in den Funkzellen zwischen GSM und WLAN ist von vielen Parametern abhängig. Bei beiden Systemen hängt sie nicht nur von der eigenen Kanalauslastung ab, sondern auch von der Aktivität der gesamten Funkzelle. Insbesondere verursachen beide Systeme eine gewisse Grundlast durch den Austausch von Verwaltungsinformationen.

10.5 WLAN und TCP/IP

Zwei weitere Aspekte sollen an dieser Stelle angesprochen werden, die dazu führen, dass die Übertragung von TCP/IP-basiertem Verkehr über WLAN-Technologien nicht die Leistungsfähigkeit erlaubt, die theoretisch möglich wäre.

Zunächst handelt es sich bei TCP um ein verbindungsorientiertes Protokoll, das den erfolgreichen Empfang von Paketen mit Empfangsbestätigungen quittiert. In dem üblichen Fall, dass Informationen nur in einer Richtung übertragen werden, muss der Empfänger ein getrenntes Paket an den Sender zurückschicken, das nur die Empfangsbestätigung enthält. Wird diese TCP-Empfangsbestätigung nun über ein WLAN übertragen, das nach dem

CSMA-CA-Algorithmus arbeitet, dann ergibt sich der in Abbildung 10.3 gezeigte Ablauf. Es ist offensichtlich, dass die erreichbare Nutzdatenrate in diesen Fällen deutlich reduziert wird. Bislang ist aber noch kein Verfahren standardisiert, dass eine Einbindung von TCP-Bestätigungen in die CSMA / CA-Bestätigungen erlauben würde [Tourrilhes (3)].



Abbildung 10.3: Unidirektionaler TCP-Verkehr über ein WLAN mit CSMA/CA-MAC.

Jedes Paket wird auf der MAC- und auf der TCP-Ebene bestätigt. Dies führt zu einem erheblich höheren Verkehrsaufkommen und im Falle von fortlaufendem Verkehr vom Sender S1 zum Empfänger S2 zu einer erhöhten Kollisionswahrscheinlichkeit.

Auf den zweiten Aspekt wird in [Schulte 1999] aufmerksam gemacht. Die Tatsache, dass TCP / IP für den Einsatz in drahtgebundenen Netzen entwickelt wurde, führte zu einer Anpassung der Zeitkonstanten an die Gegebenheiten im drahtgebundenen Netz. Dabei wählt TCP die Geschwindigkeit bei der Sendung von Paketen in Abhängigkeit von der gemessenen Zeit vom Senden der vorangegangenen Pakete bis zum Empfangen der zugehörigen Bestätigung (*Round Trip Time*). Da diese Zeiten aber bei drahtlosen Netzen deutlich länger sein können als bei drahtgebundenen Netzen, ohne dass tatsächlich eine Verstopfung des Übertragungskanals vorliegt, liefert TCP unter manchen Umständen deutlich weniger Pakete, als das Netz übertragen könnte.

10.6 Entscheidungskriterien

10.6.1 Grundlegendes

Bei der Auswahl einer Netzwerktechnologie müssen eine Vielzahl von Parametern möglichst objektiv bewertet werden. Da allerdings oft zu beobachten ist, dass die subjektiven Einflussfaktoren überwiegen, wird an dieser Stelle ein beispielhafter Entscheidungskatalog vorgestellt. Dies geschieht in Anlehnung an ähnliche Verfahren in komplexen technischen Entscheidungsräumen [Sikora 2001 (3)].

Bei den im folgenden diskutierten Kriterien, die in Abbildung 10.4 in Form einer Übersicht dargestellt sind, ist allerdings zu berücksichtigen, dass es sich nicht um jeweils unabhängige Entscheidungen auf jeder Ebene handelt, sondern dass die verschiedenen Kriterien wechselweise voneinander abhängen. So kann beispielsweise der Preis für die verfügbaren Produkte die Entscheidung für eine WLAN-Technologie beeinflussen.

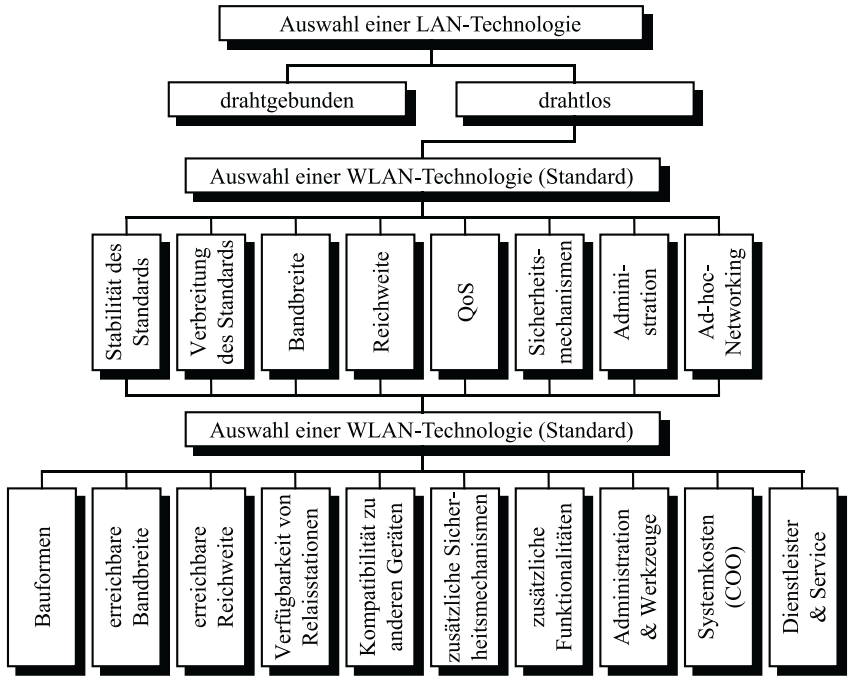


Abbildung 10.4: Auswahlkriterien für eine WLAN-Investition

Ebenfalls zu berücksichtigen ist, dass alle im Folgenden dargestellten Kriterien vor dem Hintergrund der Anforderungen der jeweiligen Anwendung betrachtet und bewertet werden müssen. Beispielsweise kann die Anforderung nach Bandbreite bei einer industriellen Anwendung zur Übertragung von einigen Steuersignalen nur eine untergeordnete Rolle spielen, während bei einer Rechnerrauminstallation mit vielen Stationen die erreichbare Bandbreite ein zentrales Entscheidungskriterium sein muss.

10.6.2 Auswahl einer LAN-Technologie

Im gegebenen Zusammenhang wird vor allem die Entscheidung zwischen drahtgebundenen und drahtlosen Technologien diskutiert. Hier lautet die wesentliche Frage, welcher Mehrwert bzw. welche Einsparungen für die jeweilige Anwendung durch den Einsatz der einen oder anderen Technologie erreicht werden können. Die für die Beantwortung dieser Frage wesentlichen Aspekte wurden bereits in Abschnitt 1.2 diskutiert.

10.6.3 Auswahl einer WLAN-Technologie

Zum Vergleich der verschiedenen zur Verfügung stehenden Technologien sollten mindestens die folgenden Kriterien hinterfragt werden:

- *Stabilität des Standards:* Ist der Standard in seiner gegebenen Version ausgereift und stabil oder sind zusätzliche Erweiterungen und Modifikationen zu erwarten, die den kompatiblen Einsatz mit aktueller Ausrüstung in Frage stellen?
- *Verbreitung des Standards:* Hat der Standard eine ausreichende Akzeptanz gefunden, um auch in Zukunft durch innovative Geräte unterstützt zu werden?
- *Bandbreite:* Welche Bandbreite stellt die jeweilige Technologie zur Verfügung? Hierbei ist unbedingt zwischen Brutto- und Nettobandbreite zu unterscheiden (vgl. Abschnitt 2.3.2).
- *Reichweite:* Welche Reichweite lässt der Einsatz der jeweiligen Technologie erwarten? Dabei sind insbesondere die zulässigen Sendeleistungen bzw. Leistungsdichten zu betrachten. Der Einsatz von anisotropen Antennen zur Erreichung höherer Reichweiten (vgl. Abschnitt 2.9.1) ist im Wesentlichen unabhängig von der gewählten Technologie.
- *Quality of Service:* Werden definierte Dienstgüten unterstützt? Hierbei ist allerdings die Frage nach der Durchgängigkeit dieser Unterstützung über alle Netzwerkebenen zu stellen.
- *Sicherheitsmechanismen:* Welche Sicherheitsmechanismen sind im Standard vorgesehen? Hierbei ist zu berücksichtigen, dass nur diejenigen Mechanismen durchgängig im Betrieb Einsatz finden können, die von allen Geräten unterstützt werden. Solange homogene Netze von nur einem Hersteller betrieben werden, reicht die Unterstützung auf Produktebene vollkommen aus. Dieses Szenario gilt allerdings nur bei Punkt-zu-Punkt-Verbindungen wie Funkbrücken uneingeschränkt.
- *Administration:* Welche Protokolle sind in dem Standard vorgesehen, die eine über alle Hersteller durchgängige Verwaltung des gesamten Netzwerks erlauben?
- *Ad-hoc-Networking:* In welchem Maße werden Funktionalitäten eines Ad-hoc-Networking unterstützt (vgl. Abschnitt 1.3.10)?

10.6.4 Auswahl eines WLAN-Produkts

- *Bauformen:* Welche Bauformen werden unterstützt? Bei den mobilen PC-gestützten Stationen unterscheidet man dabei im Wesentlichen USB-, PCI- oder PC-Card-gestützte Geräte. Bei den Zugangspunkten ist die Vielfalt deutlich größer, die Fragestellung aber meist unkritischer.
- *Erreichbare Bandbreiten:* Im Gegensatz zu drahtgebundenen Systemen sind die erreichbaren Bandbreiten wesentlich abhängig von der Qualität der Empfänger, die nicht im Standard vorgegeben sind (vgl. Abschnitt 1.4.7). Hier geben die aktuellen Testergebnisse in den einschlägigen Fachzeitschriften ausreichend Auskunft.

- *Erreichbare Reichweiten:* Die Frage nach den Reichweiten, über die ein Funknetz betrieben werden kann, ist eng mit der Frage nach der jeweils erreichbaren Bandbreite verknüpft.
- *Verfügbarkeit von Relaisstationen:* Die Reichweite von Funknetzen kann unter Umständen durch den Einsatz von Relaisstationen vergrößert werden. Diese sind im Wesentlichen einsetzbar bei Punkt-zu-Punkt-Verbindungen.
- *Kompatibilität zu anderen Geräten:* Auch wenn die grundsätzliche Kompatibilität der Geräte in heterogenen Umgebungen durch die Konformität zum Standard gegeben ist, stellen viele Geräte zusätzliche Funktionen zur Verfügung, die außerhalb des Standards stehen. Hierbei ist ein unterschiedlicher Grad an Gemeinsamkeiten zu beobachten.
- *Zusätzliche Sicherheitsmechanismen:* Vor allem in den Fällen, in denen die im Standard vorgesehenen Sicherheitsmechanismen als nicht ausreichend angesehen werden, erweitern manche Hersteller ihre Geräte durch zusätzliche Sicherheitsmechanismen. Diese sind dann unter Umständen aber nur in homogenen Netzen zu nutzen.
- *Zusätzliche Funktionalitäten:* Einige Geräte – und hierbei insbesondere die Zugangspunkte – stellen zusätzliche Netzwerkfunktionalität zur Verfügung. Als Beispiele können Routing oder Firewall genannt werden.
- *Administration und Werkzeuge:* Welche Werkzeuge zur Verwaltung der Stationen und des Netzwerks werden bereitgestellt? Bei Zugangspunkten ist es mittlerweile weit verbreitet, dass ein Embedded Webserver den Zugriff über einen normalen Webbrowser ermöglicht. Aber auch hier können erhebliche Unterschiede bei Übersichtlichkeit und Bedienungskomfort beobachtet werden. Bei mobilen Stationen, die ohnehin die Installation von Treibern benötigen, werden meist zusätzliche Administrationswerkzeuge eingesetzt.
- *Preis:* Bei der Bestimmung der kommerziellen Aspekte sind die gesamten Systemkosten zu berücksichtigen. Dies gilt sowohl für den Vergleich zwischen drahtgebundenen und drahtlosen Systemen und der Fragestellung nach Leitungs- und Installationskosten als auch für die Kosten während des gesamten Lebenszyklus. Somit schließen die Systemkosten auch den Administrationsaufwand und eventuelle Erweitungs- oder Ersatzbeschaffungen mit ein.
- *Dienstleister und Service:* Schließlich ist bei der Auswahl – insbesondere bei einer größeren Investitionsentscheidung – zu berücksichtigen, welche Dienstleistungen zusammen mit den WLAN-Produkten angeboten werden. Dabei ist auch in vielen Fällen zu beachten, dass die Auswahl des Produkts von dem bereits etablierten Systemhaus getroffen wird.

10.7 Ausblick

Zum Abschluss der Darstellung sei ein Ausblick auf die weitere Entwicklung erlaubt, auch wenn die Gefahr besteht, dass diese Vorhersagen durch die Wirklichkeit eingeholt und unter Umständen konterkariert werden:

- Das Vordringen von drahtlosen lokalen Netzen (WLANs) wird sich aufgrund zahlreicher praktischer Vorteile fortsetzen und verstärken.
- Hierdurch werden sich die Kosten für die aktiven Elemente weiter verringern.
- Die kostengünstige drahtlose Anbindung wird die Entwicklung neuer Geräte wie Webpads [Bager 2001] und neuer Anwendungen zur Folge haben.
- Dabei werden sich mittelfristig die Entwicklungen auf einige wenige Technologien konzentrieren. Bis dahin werden Geräte auch mehrere Protokollstandards unterstützen.
- Die zur Verfügung stehende Bandbreite der drahtlosen Übertragung wird weiterhin zunehmen.
- Das verstärkte Auftreten von nomadisierenden (mobilen) Teilnehmern im Internet wird den Druck auf die Unterstützung durch die Internet-Protokollfamilie verstärken [Wolisz 2000].
- Die Unterstützung von Ad-hoc-Netzwerken wird eine zunehmende Integration von Intelligenz in die Netzwerke und die Peripheriegeräte zur Folge haben, da ansonsten die eigenen Dienste nicht flexibel und unabhängig von der jeweiligen Netzwerkanbindung angeboten werden können.
- Die zunehmende Konvergenz von Sprach- und Datenverkehr auf allen Netzwerkebenen wird zu einer verstärkten Unterstützung von garantierten Dienstgüten auch im WLAN-Bereich führen. Hier sind gegenwärtig noch nicht alle Systeme geeignet [Köpsel 2001].

A Anhang

A.1 Maxwellsche Gleichungen

Die erste Maxwellsche Gleichung (A.1) besagt, dass jedes sich zeitlich ändernde elektrische Feld ein magnetisches Wirbelfeld erzeugt. Sie wird auch als Durchflutungsgesetz bezeichnet.

$$\oint \vec{H} d\vec{s} = \int \left(\vec{j} + \frac{d\vec{D}}{dt} \right) d\vec{A} \qquad \text{(A.1)}$$

Die zweite Maxwellsche Gleichung (A.2) ist auch als Induktionsgesetz bekannt. Es besagt, dass jedes sich zeitlich ändernde Magnetfeld ein elektrisches Wirbelfeld erzeugt.

$$\oint \vec{E} d\vec{s} = -\int \left(\frac{d\vec{B}}{dt} \right) d\vec{A} \qquad \text{(A.2)}$$

In der Übereinstimmung entstehen elektromagnetische Felder dann, wenn elektrische Ladung beschleunigt wird. Die geniale Voraussage von Maxwell bestand unter anderem darin, dass er seine Gleichungen als Formulierungen für elektromagnetische Wellen interpretieren konnte für den Fall, dass kein Stromfluss vorhanden war ($\vec{j} = 0$), aber sich sowohl das magnetische Feld ($d\vec{B}/dt \neq 0$) als auch die elektrische Verschiebungsdichte ($d\vec{D}/dt \neq 0$) veränderten.

A.2 Physikalische Grundlagen des Direct-Sequence-Spread-Spectrum-Verfahrens

Ausgangspunkt ist das bandbegrenzte Signal der Eingangsdaten, wobei die Grenzfrequenz f_0 gleich der Bitrate r_{Bit} der Nutzdaten ist. Durch die Verknüpfung mit der PN-Sequenz der Bitrate r_{PN} wird das Leistungsspektrum des Signals im Frequenzbereich gespreizt, wobei allerdings die Leistung der Signale S_{PN} (die Integrale unter den beiden Kurven) unverändert bleiben.

Als Nutzleistungsdichte des gespreizten Signals ergibt sich nun mit der Nutzleistungsdichte des originalen Signals *S* und der Bandbreite der PN-Sequenz $f_0 = r_{PN}$:

$$S_{PN} = \frac{S}{r_{PN}} \tag{A.3}$$

Schließlich wird das Signal noch in den Hochfrequenzbereich verschoben. Hierzu wird das Signal mit einem hochfrequenten Trägersignal multipliziert.

Auf der Empfängerseite werden dieses Signal sowie zusätzliche Störsignale empfangen. Folgende Operationen führen zu einem korrekten Empfang des Nutzsignals.

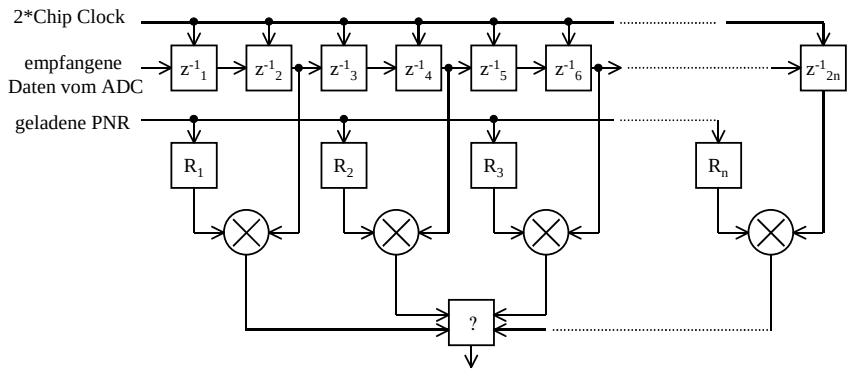


Abbildung A.1: Grundsätzlicher Aufbau eines DSSS-Korrelators (Zyren1)

Mit Hilfe eines so genannten »angepassten Korrelators« (*Matched Filter* - Abbildung A.1) wird die überlagerte PN-Sequenz entfernt. Grundlage eines solchen Korrelators ist die Tatsache, dass sich die wiederholte Exklusiv-Oder-Verknüpfung mit der gleichen Signalfolge aufgrund des Assoziativgesetzes wieder aufhebt. Wenn *D* das Datensignal und *A* der Zustand der PN-Sequenzen ist, dann gilt der in Abbildung A.2 gezeigte Zusammenhang. Dabei müssen die Spreizfunktionen bestimmte Eigenschaften aufweisen [Hatzold 2000]:

- Zum einen müssen die Spektren der von den gespreizten Datenfunktionen modulierten HF-Signale rauschähnlich sein, was durch die Verknüpfung der Datensignale mit Pseudozufallsfunktionen erzielt wird.

- Zum anderen ist für den Vielfachzugriff aber wesentlich, dass die den verschiedenen Stationen zugeordneten Spreizfunktionen zueinander orthogonal oder wenigstens quasiorthogonal sind. Orthogonal sind zwei Funktionen, wenn ihre Kreuzkorrelation den Wert 0 ergibt, quasiorthogonal, wenn die Kreuzkorrelation einen im Vergleich zur Autokorrelation einer der beiden Funktionen sehr kleinen Wert ergibt.

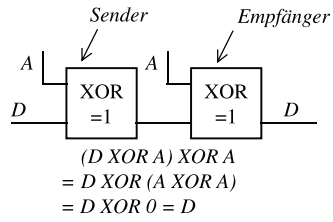


Abbildung A.2: Zur Funktionsweise eines DSSS-Korrelators: Die doppelte Anwendung der Exklusiv-Oder-Funktion liefert das ursprüngliche Signal.

Von grundlegendem Vorteil ist bei diesem Verfahren auch, dass die schmalbandige Störung der hohen Intensität I in ein breitbandiges Rauschen niedriger Intensität I_{PN} gespreizt wird. Als Störleistungsdichte ergibt sich nach der Entspreizung:

$$I_{PN} = \frac{I}{r_{PN}} \tag{A.4}$$

Nach der Tiefpassbegrenzung auf $f_0 = r_{Bit}$ verbleibt als gesamte Störleistung I_R innerhalb der Nutzbandbreite r_{Bit}

$$I_r = I * r_{Bit} \tag{A.5}$$

Somit berechnet sich das Signal-zu-Störleistungs-Verhältnis des resultierenden Signals zu

$$\frac{S}{I_{PN}} = \frac{S}{I} * \frac{r_{PN}}{r_{Bit}} \tag{A.6}$$

Es ist auf diese Weise um den Spreizfaktor r_{PN}/r_{Bit} größer als das Signal-zu-Störleistungs-Verhältnis am Antenneneingang.

Wenn ein Funkübertragungssystem unterschiedliche Spreizfolgen zur Unterscheidung der verschiedenen Kanäle verwendet, dann sind zwei Voraussetzungen zu erfüllen:

- Der Empfänger muss die Entscheidung treffen, welches der an ihn gerichtete Kanal ist. Hierzu empfangen verschiedene Filter das Signal und setzen jeweils unterschiedliche PN-Sequenzen an. Der Filter, der die beste Leistungsfähigkeit zeigt, liefert dann das empfangene Signal. In diesem Filter wird dann auch das Leistungsspektrum des gespreizten Signals zurücktransformiert.

- Zur Unterscheidung der verschiedenen PN-Sequenzen voneinander müssen diese allerdings eine bestimmte Länge aufweisen. Hiermit vergrößert sich die Spreizrate und somit auch die Unterdrückung der Störsignale.

Es stehen eine Reihe von PN-Sequenzen zur Verfügung, die besonders gute Autokorrelationseigenschaften besitzen:

- Ronald H. Barker entwickelte Bitfolgen, die besonders gute aperiodische Autokorrelationseigenschaften aufweisen [Intersil Corp.]. Der IEEE802.11-Standard verwendet einen Barker-Code der Länge $N = 11$.

Tab. A.1: Übersicht über alle bekannten Barker-Codes

Code-Länge (*N*)	Barker-Code
1	+
2	++ oder +-
3	++-
4	+++- oder ++-+
5	+++-+
7	+++--+-
11	+++---+--+-
13	+++++--++-+-

- Alternativ werden komplexe PN-Folgen eingesetzt, die als binäre komplementäre Codes, Folgen oder Sequenzen bezeichnet werden. Das zugehörige Verfahren ist als ***C**omplimentary **C**ode **K**eying* (CCK) bekannt. Dabei versteht man unter einem komplementären binären Code eine Folge, die aus gleichen und ungleichen Paaren (*like pairs:* 1 1, -1 –1, *unlike pairs:* 1 –1, -1 1) bestehen, die identischen Abstand zueinander haben. Dabei besteht die Besonderheit der komplementären Codes darin, dass die Autokorrelationsfunktion dieser Folge nur dann ungleich Null ist, wenn die Phasenverschiebung gleich Null ist [Pearson 2000]. Auf diese Weise kann eine gute Detektion der Folge implementiert werden.

A.3 Antennen mit Richtcharakteristik

Der Gewinn einer Antenne $g(\theta)$ in die Richtung θ wird ausgedrückt durch das Verhältnis von abgestrahlter Leistung zur mittleren Leistung bezogen auf den Raumwinkel:

$$g(\theta) = \frac{P(\theta) * 4\pi}{P_0} \tag{A.7}$$

wobei P_0 die gesamte abgestrahlte Leistung der Antenne ist. Die maximale Leistung der Antenne wird in Richtung der so genannten Hauptkeule abgestrahlt. g_{max} ist der maximale Antennengewinn für $\theta = 0$ und gibt die Verstärkung der Antenne bezogen auf einen isotropen Strahler gleicher Leistung an.

Für die Leistungsdichte einer verlustlosen Antenne mit dem Gewinn g_s ergibt sich hieraus

$$p = \frac{P_S g_S}{4\pi * r^2} = \frac{EIRP}{4\pi * r^2} \qquad \left[\frac{W}{m^2}\right] \tag{A.8}$$

Das Produkt aus der Leistung der isotropen Sendeantenne P_S und dem Gewinn der Sendeantenne g_S bezeichnet man als ***E**ffective **I**sotropically **R**adiated **P**ower* (EIRP). Es gibt die Sendeleistung an, die man bei ungerichteter Abstrahlung mit einem isotropen Strahler benötigt, um die gleiche Leistungsdichte wie im gerichteten Fall zu erreichen.

Typische Werte von in der Praxis erreichten Antennenverstärkungen zeigt die Tabelle A.2.

Antennengewinn	Bauform
21 dBi	Parabolantenne
13,5 dBi	Yagi
5–12 dBi	Omni
6–8,5 dBi	Patch

Tab. A.2: Typische Werte für den Gewinn unterschiedlicher Antennentypen

Den Empfänger erreicht nun die Leistung

$$P_E = P_S g_S g_E * L = P_S g_S g_E * \left(\frac{\lambda}{4\pi * d}\right)^2 \tag{A.9}$$

Dabei ist g_E der Gewinn der Empfangsantenne und L die Freiraumdämpfung in Abhängigkeit von der Wellenlänge λ und der Distanz d.

Für den einfachsten Fall der isotropen Antennen ergibt sich die Freiraumdämpfung L_0 als Quotient von empfangener und abgestrahlter Leistung. In logarithmischer Darstellung erhält man die Differenz der beiden Werte

$$\begin{aligned} L_0[dB] &= P_E[dBm] - P_S[dBm] \\ &= -10\log\left(\frac{P_E[mW]}{P_S[mW]}\right) = -20 * \log\left(\frac{\lambda}{4\pi * d}\right) \end{aligned} \tag{A.10}$$

Unter Berücksichtigung des Antennengewinns von Sende- und Empfangsantenne ergibt sich für den gesamten Pfad eine Dämpfung von:

$$L_F[dB] = -10\log\left(\frac{P_E[mW]}{P_S[mW]}\right) = -10 * \log\left(\frac{P_S g_S g_E}{P_S}\left(\frac{\lambda}{4\pi * d}\right)^2\right)$$
$$= -10\log(g_S) - 10\log(g_E) - 20\log\left(\frac{\lambda}{4\pi * d}\right) \qquad \text{(A.11)}$$

Setzt man diesen Ausdruck gleich der äquivalenten Freiraumdämpfung und löst nach der Distanz *d* auf, so ergibt sich:

$$L_0 = -10\log(g_S) - 10\log(g_E) - 20\log\left(\frac{\lambda}{4\pi * d}\right)$$
$$L_0 + 10\log(g_S) + 10\log(g_E) = -20\log\left(\frac{\lambda}{4\pi * d}\right)$$
$$10^{\frac{L_0 + 10\log(g_S) + 10\log(g_E)}{20}} = \frac{\lambda}{4\pi * d}$$
$$d = \frac{\lambda}{4\pi} * 10^{\frac{L_0 + 10\log(g_S) + 10\log(g_E)}{20}}$$
$$d = \frac{1}{4\pi} * \frac{c}{f} * 10^{\frac{L_0 + 10\log(g_S) + 10\log(g_E)}{20}} \qquad \text{(A.12)}$$

Dabei ist c die Wellenausbreitungsgeschwindigkeit, die in erster Näherung gleich der Lichtgeschwindigkeit gesetzt werden kann.

Die Darstellung in den Gleichungen (A.10) bis (A.12) ist auf Sendeleistungen von 1 mW normiert. Wird nun noch die abgestrahlte Leistung des isotropen Senders um

$$p_{SV} = \frac{\text{abgestrahlte Leistung [mW]}}{1mW} \qquad \text{(A.13)}$$

erhöht, dann muss dieser Faktor ebenfalls berücksichtigt werden. Es ergibt sich:

$$d = \frac{1}{4\pi} * \frac{c}{f} * 10^{\frac{L_0 + 10\log(p_{SV}) + 10\log(g_S) + 10\log(g_E)}{20}} \qquad \text{(A.14)}$$

Setzt man nun folgende typische Werte L_0 = 90 dBm, $g_S = g_E$ = 6 dBi und p_{SV} = 13 dBm an, ergibt sich aus der Gleichung (A.14) unter Berücksichtigung einer einzuhaltenden Marge von 10 dBm eine Reichweite von 2190 m. Voraussetzung ist dabei natürlich die direkte Sichtverbindung im Sinne der bereits erwähnten ***L**ine **o**f **S**ight* (LOS) und ein ausreichender Abstand von den Bodenhindernissen, damit sich die Wellen ungehindert ausbreiten können und die angenommene Dämpfungscharakteristik zumindest näherungsweise erfüllt ist.

Durch den Einsatz von solchen Richtantennen können die beschriebenen WLAN-Systeme auch für die Kopplung räumlich entfernter LANs eingesetzt werden. Limitierend ist dabei für den Geltungsbereich der ETSI und die Nutzung des 2,4 GHz-Bandes zu berücksichtigen, dass in Bezug auf die Nutzung einer Sendeleistung von 1 mW und einen isotropen Sender ein Verstärkungs- und Antennengewinn von weniger als 20 dBm EIRP eingehalten werden muss.

B Literatur

Abramsson, N., »The ALOHA system – another alternative for computer communications«, AFIPS Conf. Proc., Vol.37, FJCC 1970, S. 695–702

Ahlers, E., Živadinović , D., »Datenkuriere – 12 WLAN-Systeme für schnelle Funknetzwerke«, c't 22 / 2000

Andren, C., »Der Teufel steckt im Detail – Wireless LANs in Gebäuden einrichten«, Design&Elektronik, Heft 06 / 2001, S.86–89

Aramaki, T., »Difference between BRAN HiperLAN2 and MMAC HiSWANa«, HIPERLAN / 2 Global Forum, 21. Februar 01

Bager, J., »Die Web-Pads kommen! – Drahtlos surfen ohne PC«, c't 2001, Heft 16, S.120–122

(1) Bläsner, W., »Blaubeere an Blauzahn, bitte kommen! – Mit System zum Markterfolg bei Bluetooth«, Design&Elektronik 6 / 2001, S. 72–76

(2) Bläsner, W., »DECT: Revolution durch LIF-Technik«, Elektronik 7 / 2000, S. 74–76

Bluetooth-Standard (*http://www.bluetooth.com/developer/specification/Bluetooth_11_Specifications_Book.pdf* u. *http://www.bluetooth.com/developer/specification/Bluetooth_11_Profiles_Book.pdf*)

(1) Borisov, N., Goldberg, I., Wagner, D., »Security of the WEP Algorithm«, verfügbar unter: *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*

(2) Borisov, N., Goldberg, I., Wagner, D., »Intercepting Mobile Communications: The Insecurity of 802.11«, Seventh Annual International Conference on Mobile Computing And Networking«, 16.–21. Juli 2001, verfügbar unter: *http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf*

Burkley, C.J., »Coding and Modulation Techniques for RF LANs«, in: Santamaría, A., López-Hernández, F.J., »Wireless LAN Systems«, Artech House, Boston, London 1994, ISBN 0-89006-609-4, S.197–224.

Cisco Systems, Inc. »White Paper: Cisco Systems Spread Spectrum Radios and RF Safety«, verfügbar unter: *http://www.cisco.com/warp/cc/pd/witc/ao340ap/prodlit/rfhr_wi.htm*

Compaq, »Compaq Wireless LAN«, verfügbar unter: *http://www.compaq.de/wireless/technologie/lan/index.htm*

Constantinou, P., »Properties of Wireless RF Channels«, in: Santamaría, A., López-Hernández, F.J., »Wireless LAN Systems«, Artech House, Boston, London 1994, ISBN 0-89006-609-4, S.129–163

FCC Part15 (*http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/2000/fcc00312.txt*)

Fluhrer, S., Mantin, I., Shamir, A,. »Weaknesses in the Key Scheduling Algorithm of RC4«, Preliminary Draft, 25.7.01, verfügbar unter: *http://www.crypto.com/papers/others/rc4_ksaproc.ps*

Frodigh, M., Johannson, P., Larsson, P., »Wireless ad hoc networking – The art of networking without a network«, Ericsson Review No.4, 2000, S.248–263, verfügbar unter: *http://www.ericsson.com/review/2000_04/files/2000046.pdf*

(1) Frost & Sullivan, »World Wireless LAN Markets«, #5781-74, 1999; ausschnittsweise verfügbar unter: *http://www.proxim.com/wireless/research/frost_sul.pdf*

(2) Frost & Sullivan, »Bluetooth puscht Chipnachfrage«, Presseinformation Januar 2001 (www.frost.com)

Gieselmann, H., »Sendung mit der Maus – Neun Funkmäuse und fünf kabellose Tastaturen im Test«, C't 2001, Heft 11, S. 154–165

Haartsen, J.C., Zürbes, S., »Bluetooth voice and data perfomance in 802.11 DS WLAN environment«, Ericsson, 31.5.1999

Halford, K., Webster, M., »Multipath Measurement in Wireless LANs«, Intersil Application Note AN9895, Mai 2000, verfügbar unter: *http://www.intersil.com/data/an/an9/an9895/an9895.pdf*

Hascher, W., »Höchstintegration bei DECT-Bausteinen«, Elektronik 9 / 1999, S. 52–53

Hatzold, P., »Spread Spectrum und CDMA – Was dahinter steckt«, Elektronik 21 / 2000, S. 56–64

Heeg, M., »Vernetzung ohne Schnur«, Elektronik 10 / 99, S. 68–74

HomeRF Working Group, »Interference Immunity of 2.4 GHz Wireless LANs«, verfügbar unter: *http://www.homerf.org/data/tech/hrf_interference_immun_wp.pdf*

Intersil Corp., »A Condensed Review of Spread Spectrum Techniques for ISM Band Systems«, Intersil Application Note AN9820.1, Mai 2000, verfügbar unter: *http://www.intersil.com/data/an/an9/an9820/an9820.pdf*

Johnson, M., »HiperLAN / 2 – The Broadband Radio Transmission Technology Operating in the 5GHz Frequency Band«, HiperLAN / 2 Global Forum, 1999, verfügbar unter: *http://www.hiperlan2.com/web/pdf/whitepaper.pdf*

Kaiser, W., Skript zur Vorlesung »Geschichte der Technik im Industriezeitalter I« und »Geschichte der Technik im Industriezeitalter II«, RWTH Aachen, 1999

Kammeyer, K.D., Nachrichtenübertragung, B.G. Teubner, Stuttgart, 1992, ISBN 3-519-06142-2

Khun-Jush, J., Malmgren, G., Schramm, P., Torsner, J., »HIPERLAN type 2 for broadband wireless communication«, in: Ericsson Review No. 2, 2000, S. 180–119, verfügbar unter: *http://www.ericsson.com/review/2000_02/files/2000026.pdf*

Klinkenberg-Haass, F., »Bluetooth quo vadis?«, www.tecchannel.de, Artikel vom 13.6.2001, verfügbar unter: *http://www.tecchannel.de/hardware/724/index.html*

Köpsel, A., Wolisz, A., »Voice transmission in an IEEE 802.11 WLAN based access network« erscheint in: Proceedings WoWMoM 2001, Rom, Italien, Juli 2001, verfügbar unter: *http://www-tkn.ee.tu-berlin.de/publications/koepsel/wowmom01.pdf*

Lebherz, M., Wiesbeck, W., »Beurteilung des Reflexions- und Schirmungsverhaltens von Baustoffen«, Bauphysik 12, 1990, Heft 3, S. 85–92.

Lüke, H.-D., »Signalübertragung – Grundlagen der digitalen und analogen Nachrichtenübertragungssysteme«, Springer, 4. Auflage, 1990

Mazzara, A., »10 vor 10 vom Donnerstag 24.5.2001«, Schweizer Fernsehen DRS, verfügbar unter: *http://real.sri.ch/ramgen/sfdrs/10vor10/2001/10vor10_24052001.rm?start=0:01:37.905&end=0:10:15.612*

Merritt, R., »Conflicts between Bluetooth and wireless LANs called minor«, EE Times, 21. Februar 2001, verfügbar unter: *http://www.planetanalog.com/story/OEG20010220S0040*

Mettala, R., »Bluetooth Protocol Architecture«, Version 1.0, 25. August 1999, Bluetooth Special Interest Group, Doc.No.1.C.120 / 1.0

Lansford, J,. Nevo, R., Monello, B., »Wi-Fi® (802.11b) and Bluetooth Simultaneous Operation: Charakterizing the Problem«, verfügbar unter: *http://www.mobilian.com/documents/WPSG_2.pdf*

Nett, E,. Mock, M., Gergeleit, M., »Das drahtlose Ethernet – Der 802.11 Standard: Grundlagen und Anwendung«, Addison-Wesley – Datacom Akademie, 2001, ISBN 3-8272-1741-X

Pearson, B., »Complementary Code Keying Made Simple«, Intersil Application Note AN9850.1, Mai 2000, verfügbar unter: *http://www.intersil.com/data/an/an9/an9850/an9850.pdf*

Proxim Inc., »Migration of Wireless LAN Technologies in the Enterprise«, White Paper 2001, verfügbar unter: *http://www.proxim.com/products/harmony/whitepapers/migration.pdf*

Schulte, G., »Fallstricke – TCP/IP im drahtlosen Netz«, C't 1999, Heft 6, S.232–233

Shoemake, M.B., »WiFi (IEEE802.11b) and Bluetooth – Coexistence Issues and Solutions for the 2.4 GHz ISM Band«, Texas Instruments, White Paper, Februar 2001, Version 1.1, verfügbar nach Anmeldung unter: *http://www.ti.com/sc/wirelessnetworking*

Sietmann, R., »Quo vadis, Mobilfunk? – Nebenbuhler und Nachfolger von UMTS«, C't 2001, Heft 5, S. 94–101

(1) Sikora, A., »802.11: Standard für drahtlose Netze«, Artikel vom 12.4.01, verfügbar unter: *http://www.tecchannel.de/hardware/680/index.html*

(2) Sikora, A., »DECT – Die Alternative zu Bluetooth«, Artikel vom 21.8.01, verfügbar unter: *http://www.tecchannel.de/hardware/511/index.html*

(3) Sikora, A., »Programmierbare Logikbauelemente – Architekturen und Anwendungen«, Hanser Verlag, 2001

(4) Sikora, A., "Embedded Applikationen im Internet, Teil 1: Übersicht über Vor- und Nachteile von vernetzten Anwendungen", Elektronik 22/2000, S.90–102, »Teil 2: Implementierungen«, Elektronik 23/2000, S.164–169

(5) Sikora, A., "CMOS goes to Gigahertz – Embedded Technologien werden schneller", Markt & Technik, Nr. 22/00, S.39–40

(1) Solectek Corp., »Tech Talk – DSSS vs. FHSS, The Skinny«, verfügbar unter: *http://www.solectek.com/tech-center/index.html*

(2) Solectek Corp., »Tech Talk – What's in Your Microwave«, verfügbar unter: *http://www.solectek.com/tech-center/index.html*

Spurgeon, C.E., »Ethernet – The Definitive Guide«, O'Reilly, 2000, ISBN 1-56592-660-9

Texas Instruments, »TI's Optical Wireless Solutions™ Technology – Moving Data at Light Speed«, verfügbar unter: *http://www.ti.com/sc/docs/products/msp/telecom/alp/ows_brochure.pdf*

(1) Tourrilhes, C.R.J., »Linux Wireless LAN Howto«, verfügbar unter: *http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.pdf*

(2) Tourrilhes, C.R.J., »A Medium Access Protocol for Wireless LANs which supports Isochronous and Asynchronous Traffic«, verfügbar unter: *http://www.hpl.hp.com/personal/Jean_Tourrilhes/Papers/pimrc98.html*

(3) Tourrilhes, C.R.J., »*PiggyData: Reducing CSMA/CA collisions for multimedia and TCP connections*«, Proc. of VTC `99. HP external report HPL-1999-58

Vinayak, V., O'Keese, W., Lam, C., »Ein Chip für die Übertragung im 2,4 GHz-Band – Eine gemeinsame Lösung für Bluetooth und Funk-Datennetze«, Teil 1, Elektronik 7/2001, S. 70–77

Walke, B., »Mobilfunknetze und ihre Protokolle«, Teubner 2000, Band 1, ISBN 3-519-16430-2 und Band 2, ISBN 3-519-16431-0

Wireless Ethernet Compatibility Alliance, »802.11b Wired Equivalent Privacy (WEP) Security, 19. Februar 2001, verfügbar unter: *http://www.wi-fi.com/pdf/Wi-FiWEPSecurity.pdf*

Wolisz, A. »Wireless Internet Architectures: Selected Issues. Mobile Networks, S.1–16, 2000, (invited paper) in: J.Wozniak, J. Konorski, editors "Personal Wireless Communications" Kluver Academic Publishers, Boston / Dordrecht / London, verfügbar unter: *http://www-tkn.ee.tu-berlin.de/publications/wolisz/pwc_wolisz_cor.pdf*

Wuschek, M., »Elektrosmog: Gefahren durch Mobilfunk?«, Artikel vom 12.1.01, verfügbar unter: *http://www.tecchannel.de/hardware/628/index.html*

(1) Zyren, J., Petrick, A., »Brief Tutorial on IEEE 802.11 Wireless LANs«, Intersil Application Note 9829, Februar 1999, verfügbar unter: *http://www.intersil.com/data/an/an9/an9829/an9829.pdf*

(2) Zyren, J., »Reliability of IEEE802.11 Hi Rate DSSS WLANs in a High Density Bluetooth Environment«, Intersil, 8.6.1999

(3) Zyren, J., Godfrey, T., Eaton, D.,»Does Frequency Hopping Enhance Security«, 19. April 2001, verfügbar unter: *http://www.wi-fi.com/pdf/20010419_frequencyHopping.pdf*

C Abkuerzungen

ACK	**Ack**nowledgement
ACL	**A**synchronous **C**onnectionless Link
ACS	**A**ccess **C**ontrol **S**erver
ADSL	**A**symmetric **D**igital **S**ubscriber **L**ine
AID	**A**ssociation **Id**entifier
AM_ADDR	**A**ctive **M**ember **Addr**ess
AP	**A**ccess **P**oint
APC	**A**ccess **P**oint **C**ontroller
API	**A**pplication **P**rogram **I**nterfaces
AR_ADDR	**A**ccess **R**equest Member **Addr**ess
ARIB	**A**ssociation of **R**adio **I**ndustries and **B**roadcasting
BD_ADDR	**B**luetooth **D**evice **Addr**ess
BER	**B**it **E**rror **R**ate
BPSK	**B**inary **P**hase **S**hift **K**eying
BRAN	**B**roadband **R**adio **A**ccess **N**etwork
BSIG	**B**luetooth **S**pecial **I**nterest **G**roup
BSS	**B**asic **S**ervice **S**et
BT	**B**andwidth-**T**ime
CA	**C**ollision **A**voidance
CC	**C**entral **C**ontroller
CCA	**C**lear **C**hannel **A**ssignment
CCK	**C**omplimentary **C**ode **K**eying
CD	**C**ollision **D**etection
CDMA	**C**ode **D**ivision **M**ultiple **A**ccess
CEM	**C**lient **E**ncryption **M**anager
CEPT	**E**uropean **C**onference for **P**ost and **T**elecommunications
CFP	**C**ontention **F**ree **P**eriod
CL	**C**onvergence **L**ayer
CM	**C**entral **M**ode
CODEC	**Co**dierer/**Dec**odierer

CP	**C**entral **P**oint
CRC	**C**yclic **R**edundancy **C**heck
CS	**C**arrier **S**ense
CSMA/CD	**C**arrier **S**ense **M**ultiple **A**ccess
CTS	**C**lear-**T**o-**S**end
CVSD	**C**ontinuous **V**ariable **De**lta **M**odulation
CW	**C**ontention **W**indow
DAB	**D**igital **A**udio **B**roadcasting
DAC	**D**evice **A**ccess **C**ode
DCF	**D**istributed **C**oordination **F**unction
DCS	**D**ynamic **C**hannel **S**election
DECT	**D**igital **E**uropean **C**ordless **T**elecommunication
DECT-MMC	**DECT M**ulti**m**edia **C**onsortium
DFS	**D**ynamic **F**requency **S**election
DH	**D**ata–**H**igh Rate
DIAC	**D**edicated **I**nquiry **A**ccess **C**ode
DLA	**D**irect **L**ink **A**ccess
DLC	**D**ata **L**ink **C**ontrol
DM	**D**ata–**M**edium Rate
DM	**D**irect **M**ode
DMAP	**DE**CT **M**ultimedia **A**ccess **P**rofile
DPRS	**DE**CT **P**acket **R**adio **S**ervice
DQPSK	**D**ifferential **Q**uadrature **S**hift **K**eying
DRM	**D**ynamic **R**esource **M**anagement
DS	**D**istribution **S**ystem
DSSS	**D**irect-**S**equence **S**pread **S**pectrum
DV	**D**ata **V**oice Combined
EC	**E**rror **C**ontrol
ERIP	**E**ffective **I**sotropically **R**adiated **P**ower
ESS	**E**xtended **S**ervice **S**et
ETSI	**E**uropean **T**elecommunications **S**tandard **I**nstitute
FCC	**F**ederal **C**ommunications **C**ommission
FDMA	**F**requency **D**ivision **M**ultiple **A**ccess
FEC	**F**orward **E**rror **C**orrection
FFT	**F**ast **F**ourier **T**ransform
FHSS	**F**requency **H**opping **S**pread **S**pectrum

FP	**F**ixed **P**art
FSK	**F**requency **S**hift **K**eying
FTP	**F**ile **T**ransfer **P**rotocol
GAP	**G**eneric **A**ccess **P**rofile
GFSK	**G**aussian **P**hase **S**hift **K**eying
GIAC	**G**eneral **I**nquiry **A**ccess **C**ode
GIP	DECT/**G**SM **I**nterworking **P**rofile
GP	**P**rocessing **G**ain
GPRS	**G**eneral **P**acket **R**adio **S**ervice
GSM	**G**eneral-**S**ystem-for-**M**obile-Communication
H2GF	**H**iperLAN/**2** **G**lobal **F**orum
HCI	**H**ost **C**ontroller **I**nterface
HIPERLAN/2	**Hi**gh **Pe**rformance **R**adio **L**ocal-**A**rea **N**etwork Type **2**
HiSWANa	**Hi**gh **S**peed **W**ireless **A**ccess **N**etwork
HomeRF	**Home** **R**adio **F**requency
HomeRF WG	**Home** **R**adio **F**requency **W**orking **G**roup
HR	**H**igh **R**ate
HV	**H**igh Quality **V**oice
IAPP	**I**nter **A**ccess **P**oint **P**rotocol
IBSS	**I**ndependent **B**asic **S**ervice **S**et
ICNIRP	**I**nternational **C**ommission for **N**on-**I**onizing **R**adiation **P**rotection
ICV	**I**ntegrity **C**heck **V**alue
IEEE	**I**nstitute of **E**lectrical and **E**lectronic **E**ngineers
IFFT	**I**nverse **FFT**
IFS	**I**nter**f**rame **S**pace
IN	**I**ntelligente **N**etze
IP	**I**ntellectual **P**roperty
IP	**I**nternet **P**rotocol
IrDA	**I**nfrared **D**ata **A**ssociation
ISI	**I**nter**s**ymbol **I**nterference
ISM	**I**ndustrial, **S**cientific, **M**edical
ISO	**I**nternational **S**tandards **O**rganisation
ISP	**I**nternet **S**ervice **P**rovider
ITU	**I**nternational **T**elecommunication **U**nion
IV	**I**nitialisierungs**v**ektor

KSA	**K**ey **S**cheduling **A**lgorithm
L2CAP	**L**ogical Link **C**ontrol and **A**daptation **P**rotocol
LAN	**L**ocal **A**rea **N**etwork
LBT	**L**isten **B**efore **T**alk
LLC	**L**ogical **L**ink **C**ontrol
LMP	**L**ink **M**anager **P**rotocol
LOS	**L**ine **o**f **S**ight
MA	**M**ultiple **A**ccess
MAC	**M**edium **A**ccess **C**ontrol
MBOK	**M**-ary **B**i-**O**rthogonal **K**eying
MC	**M**ulti **C**arrier
MLS	**M**ulti-**L**evel **S**ignaling
MMAC	**M**ultimedia **M**obile **A**ccess **C**ommunications
MMAP	**M**ulti**m**edia **A**ccess **P**rofile
MSK	**M**inimum **S**hift **K**eying
MT	**M**obile **T**erminal
NAV	**N**et **A**llocation **V**ector
NPO	**N**on-**P**rofit-**O**rganisations
OBEX	**Ob**ject-**Ex**change
OFDM	**O**rthogonal **F**requency **D**ivision **M**ultiplex
OSI	**O**pen **S**ystems **I**nterconnection
P2P	**P**oint-**to**-**P**oint
PAN	**P**ersonal **A**rea **N**etwork
PC	**P**oint **C**oordinator
PCF	**P**oint **C**oordination **F**unction
PCM	**P**ulse **C**ode **M**odulation
PDA	**P**ersonal **D**igital **A**ssistant
PDU	**P**rotocol **D**ata **U**nit
PHS	**P**ersonal **H**andy-Phone **S**ystem
PLCP	**P**hysical **L**ayer **C**onvergence **P**rotocol
PM_ADDR	**P**arked **M**ember **Addr**ess
PMD	**P**hysical **M**edium **D**ependant
PMP	**P**oint-to-**M**ulti**p**oint
PP	**P**ortable **P**art
PPM	**P**ulse **P**osition **M**odulation
PPP	**P**oint-to-**P**oint-**P**rotocol

PRS	**P**seudo **R**andom **S**equence
PSK	**P**hase **S**hift **K**eying
QAM	**Q**uadratur-**A**mplituden-**M**odulation
QoS	**Q**uality **o**f **S**ervice
QPSK	**Q**uadrature **P**hase **S**hift **K**eying
RADIUS	**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice
RAP	**R**adio Local Loop **A**ccess **P**rofile
RegTP	**Reg**ulierungsbehörde für **T**elekommunikation und **P**ost
RLC	**R**adio **L**ink **C**ontrol
RSSI	**R**eceived **S**ignal **S**trength **I**ndication
RTS	**R**equest-**T**o-**S**end
SA	**S**tandards **A**ssociation
SAP	**S**ervice **A**ccess **P**oint
SAR	**S**egmentation **A**nd **R**eassembly
SCO	**S**ynchronous **C**onnection-**O**riented Link
SDMA	**S**pace **D**ivision **M**ultiple **A**ccess
SDP	**S**ervice **D**iscovery **P**rotocol
SN	**S**ervice **N**egotiation
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
SNR	**S**ignal-To-**N**oise-**R**atio
SOHO	**S**mall **O**ffice **H**ome **O**ffice
SSID, ESSID	**E**lectronic **Sy**stem **ID**
SST	**S**pread **S**pectrum **T**echniques
SWAP-CA	**S**hared **W**ireless **A**ccess **P**rotocol – **C**ordless **A**ccess
TBTT	**T**arget **B**eacon **T**ransmission **T**ime
TCP	**T**ransport **C**ontrol **P**rotocol
TCS-Binary	**T**elephony **C**ontrol **S**ervice-**Binary**
TDD	**T**ime **D**ivision **D**uplex
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess
TPC	**T**ransmit **P**ower **C**ontrol
TSF	**T**iming **S**ynchronisation **F**unction
UDP	**U**ser **D**atagramm **P**rotocol
UNII	**U**nlicensed **N**ational **I**nformation **I**nfrastructure
USB	**U**niversal **S**erial **B**us
WECA	**W**ireless **E**thernet **C**ompatibility **A**lliance
WEP	**W**ired **E**quivalent **P**rivacy

Wi-Fi	**Wi**reless **Fi**delity
WLAN	**W**ireless **L**ocal **A**rea **N**etworks
WLANA	**W**ireless **LAN A**ssociation
WLIF	**W**ireless **L**AN **I**nteroperability **F**orum
WLL	**W**ireless **L**ocal **L**oop

Stichwortverzeichnis

A
Absorption 49
Access Point (AP) 167
Ad-Hoc Networks 119
Ad-Hoc-Modus 82, 164
Ad-Hoc-Networking 18, 22
Ad-Hoc-Netzwerk 100
ADSL 65
Aloha-Netz 22, 36
Antennen 66
API 40, 123
Application Program Interface 40, 123
ARIB 154
Arpanet 36
Assocation of Radio Industries and Broadcasting 154
Asymmetrical Digital Subscriber Line 65
Asymmetrische Kommunikation 45
Asynchrone Übertragung 45, 148
Asynchrone verbindungslose Kommunikation 126
Asynchronous Connectionless Link (ACL) 126
Authentifizierung 101, 136

B
Backoff-Algorithmus 37
Backoff-Prozess 86
Barker-Code 204
Basic Service Set 82
Beacon 149
Beacon-Rahmen 100
BER 55
Binäre PSK-Modulation 56
Binary Phase Shift Keying 114
Bit Error Rate 55
Bluetooth 13, 26f., 76, 119, 150
Bluetooth Special Interest Group 33, 119
BPSK 56, 114
BSIG 33, 119
BSS 82

C
CA 85
Carrier Sense 36, 85
Carrier Sense Multiple Access Collision Detection 88
Carrier Sensing 154, 160
CCA 83
CEPT 31
Circuit Switching 43
Clear To Send 90, 178
Clear-Channel-Assignment 83
Client-Server 45
Code Division Multiple Access (CDMA) 59
Codemultiplexverfahren 59
Collision Avoidance (CA) 37, 85
Collision Detection(CD) 37
Complimentary Code Keying (CCK) 204
Connection Less Mode 45
Connection-Oriented Mode 44
Contention Window 86
CRC 42, 186
CS 85
CSMA / CA-Algorithmus 85, 153
CSMA / CD 88
CSMA-CA 195
CTS 90, 178
CW 86
Cyclic Redundancy Check 42, 186

D
Dämpfung 49
DCF 84
DCF IFS 90
DECT 13, 26, 59, 70, 76, 139, 145, 150, 165, 191
DECT Multimedia Consortium 33, 139
DECT-MMC 33, 139
Differential Quadrature Shift Phase Shift Keying (DQPSK) 109
DIFS 90
Digital Audio Broadcasting – DAB 65
Direct Sequence 191
Direct Sequence Spread Spectrum 107
Direct-Sequence-Spread-Spectrum-Verfahren 62f., 80, 191
Distributed Coordination Function 84f.
Distribution Service 110
Distribution System 82
Diversizität 67, 166
DPRS 59

Drahtloses Kabel 122
DS 82
DSSS 80, 107
DSSS-Verfahren 62f., 71, 114, 191

E
Effective Isotropically Radiated Power 205
EIFS 90
EIRP 205
Electronic System ID 104, 111
EMV 19, 193
ERIP 160
ESS 82, 110, 171
ESSID 102, 104, 111
Ethernet 36f., 54, 79, 85, 104, 146
ETSI 31f., 139, 153
European Conference for Post and Telecommunication 31
European Telecommunication Standard Institute 31f.
Extended IFS 90
Extended Service Set 82, 110, 171

F
Fast-Fourier Transform (FFT) 66
FCC 31, 150
FEC 42, 161
Federal Communications Commission 31
FHSS 80, 105, 114
FHSS-Verfahren 32, 62, 71, 134, 150, 191
Firewire-Bus 33
Forward Error Control 161
Forward Error Correction 42
Fragmentierung 92
Frequency Division Multiple Access (FDMA) 58f.
Frequency Hopping Spread Spectrum 105
Frequency Shift Keying 57
Frequenzmultiplexverfahren 58f.
Frequenzspektrum 53
Frequenzspreiz 191
Frequenzspreizverfahren 59, 191
Frequenzsprung-Spread-Spectrum-Verfahren 32, 62, 80, 134, 150, 191
FSK 57

G
GPRS 59
GSM 26, 59, 191

H
H2GF 33
HCI 121
Hertz, Heinrich 36
Hidden-Station-Problem 70
High Speed Wireless Access Network 154
HiperACCESS 154
HiperLAN/2 13, 26, 76, 153, 182
HiperLAN/2 Global Forum 33
HiperLINK 154
HiSWANa 154
Home Radio Frequency Working Group 33
HomeRF 13, 27, 32, 76, 145
HomeRF WG 33
Hop 62
Host Controller Interface 121
Hot Spot 21, 26

I
IBSS 82
IEEE 79
IEEE1394 33
IEEE802.11 13, 26f., 52, 76, 79, 136
IEEE802.11a 81, 113
IEEE802.11b 24, 81
IEEE802.15 26
IEEE802.3 37
IN 18
In-Channel Administration 47
Independent Basic Service Set 82
Industrial, Scientific, Medical 71
Infrastruktur-Modus 82
Infrastruktur-Netzwerk 100
Initialisierungsvektor 112, 186
Inquiry 130
Institute of Electrical Electronic Engineers, Inc. (IEEE) 33
Intellectual Property 138
Intelligente Netze 18
Internatinal Standard Organisation 32
International Standardisation Organisation 38
International Telecommunication Union 32
Internet Service Provider 30
Intersymbol Interference (ISI) 58
Inverse FFT (IFFT) 66
IP 138
IrDA-Standard 53
ISM 71
ISO 32, 38
ISO/OSI-Referenzmodell 38, 80, 123
Isochrone Übertragung 45, 148
ITU 32
IV 112, 186

J
Jitter 46
Joint Standard Committee 52
JTC 52

L
L2CAP 121
LAN 17
Latenzzeit 46
LBT 85
Leitungsvermittlung 43
Line of Sight (LOS) 77, 206
Link Manager Protocol 121
Linux 163
Listen before Talk 85
LLC 80
LMP 121
Local Area Network (LAN) 74
Logical Link Control 80
Logical Link Control and Adaptation Protocol 121
LOS 206

M
MA 85
MAC 80
Marconi, Guglielmo 36
M-ary Bi-Orthogonal Keying 114
M-ary PSK 57
Matched Filter 202
Maxwell, James C. 47
Maxwellsche Gleichungen 47, 201
MBOK 114
MC 140
Medium Access Control 80
Mehrwegeausbreitung 50
Minimum Shift Keying 58
MKK 31
MLS 55
MMAC 154
Mobilfunknetz 17
Mobilität 18
Modulationstechnik 53
MSK 58
Multi Carrier 140
Multilevel Signaling 55
Multimedia Mobile Access Communication 154
Multiple Access 36, 85
M-wertiges PSK 57

N
Near-Far-Problem 70
Non-Profit-Organisation 33

O
OFDM 161
OFDM-Modulationsverfahren 117, 155
Omni 205
Orthogonal Frequency Division Multiplex (OFDM) 59, 64, 161
Orthogonales Frequenzmultiplexverfahren 59, 64

P
P2P 17
Packet Switching 43
Paging 132
Paketvermittlung 43
PAN 73
Patch 205
PC 94
PCF 84, 94
PCF IFS 90
PDA 29, 73
Personal Area Networks 73, 119
Personal Digital Assistant 29, 73
Personal Handy-Phone System 139
Phase Shift Keying 56
Phasenumtastverfahren 56
PHS 139
Physical Layer Convergence Procedure 106
Physical Layer Convergence Protocol 83
Physical Medium Dependent 83
Piconet 124
PIFS 90
PLCP 83, 96, 106
PMD 83
PMP 17
Point Coordination Function 84, 94
Point Coordinator 94
Point-to-Multipoint 17
Point-to-Point 17
Polarisation 67
PPM 114
Protocol Data Unit (PDU) 157
Pseudo Random Sequence (PRS) 62
PSK 56
Pulse Position Modulation 114

Q
QAM 57
QPSK 57, 114
Quadratur-Amplituden-Modulation 57
Quadrature Phase Shift Keying 114
Quarternary PSK 57
Quellkodierung 42

R
Radio Equipment Inspection and Certification Institute 31
RADIUS 111, 173
Raummultiplexverfahren 60
Received Signal Strength Indication 141
Reflexion 49
RegTP 31
Regulierungsbehörde für Telekommunikation und Post 31
Remote Authentication Dial-In User Service 111, 173
Request To Send 90, 178
RFCOMM 122
Roaming 82, 145
RSSI 141
RTS 90, 178
RTS-CTS 90

S
Scatternet 124
SDP 121
Segmentation And Reassembly (SAR) 157
Service Discovery Protocol 121
Shannon 61
Shared Medium 19
Shared Wireless Access Protocol – Cordless Access 147
Short IFS 90
Sicherheit 20, 28, 136, 185
elektromagnetischer Verträglichkeit 14
SIFS 90
Signal-Rausch-Abstand 55, 115
Signal-To-Noise-Ratio 55
Simple Network Management Protocol 188
Sniffer 177
SNMP 188
SNR 55, 61, 115
Space Division Multiple Access (SDMA) 59f.
Spektrale Effizienz 54
Spread Spectrum Techniques (SST) 59, 61
SSID 102, 104, 111, 165, 188
Station 38
Streuung 49
SWAP-CA 147
Symmetrische Kommunikation 45
Synchrone Übertragung 45, 148
Synchrone verbindungsorientierte Kommunikation 125
Synchronisation 110
Synchronous Connection-Oriented Link (SCO) 125

T
Target Beacon Transmission Time 100, 110
TBTT 100, 110
TCP 45
TDD 140, 149
TDMA 140
Time Division Duplex (TDD) 59, 140
Time Division Multiple Access (TDMA) 58, 140
Timing Synchronisation Function 110
Transport Control Protocol 45
TSF 110

U
UDP 45
UMTS 17, 26, 162
UMTS-Netz 26
UNESCO 32
UNII 70
UNII-Band 155
Unlicensed National Information Infrastructure 70
User Datagram Protocol 45

V
Verbindungslose Kommunikation 45
Verbindungsorientierte Kommunikation 44
Verzerrung 53

W
WAP 122
WECA 80, 151, 187, 219
WEP 111, 172, 185, 188
WEP-Algorithmus 101
Wi-Fi 80
Wired Equivalent Privacy 111, 185
Wireless Application Protocol 122
Wireless Ethernet Compatibility Alliance 33, 80
Wireless Fidelity 80
Wireless LAN Association 33, 80
Wireless Local Area Network (WLAN) 17
Wireless Local Loop 22, 154
WLAN 13
WLANA 33, 80
WLL 22, 154

Y
Yagi 205

Z
Zeitmultiplexverfahren 58f.
Zelle 52, 99
Zugangspunkt 82, 167