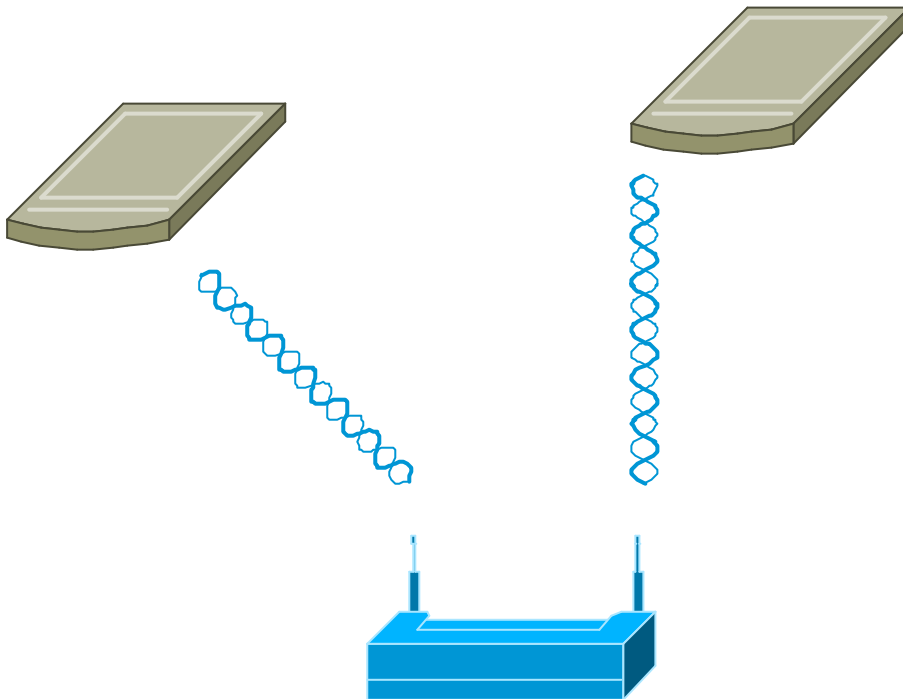


Sicherheit im Internet

WLAN – Grundlagen

Seminar Datenverarbeitung WS 2002/03



Referent: cand.-Ing. Sebastian Gajek

Betreuer: Dr.-Ing. Thomas Droste

Inhalt

1	Einleitung	2
1.1	Wire vs. wireless.....	2
1.2	Alternativen.....	3
1.2.1	IrDA	3
1.2.2	Bluetooth.....	3
1.2.3	HomeRF.....	4
1.2.4	Mobilfunkgeräte der 3. Generation	4
1.3	Interoperabilität	4
2	IEEE 802.11.....	6
2.1	Standard.....	6
2.2	Bitübertragungsverfahren	7
2.2.1	Schmalbandübertragung	8
2.2.2	Frequency Hopping Spread Spectrum (FHSS)	8
2.2.3	Direct Sequence Spread Spectrum (DSSS)	9
2.2.4	Orthogonal Frequency Division Multiplexing (OFDM)	10
2.3	Kanalzugriff	11
2.3.1	Distributed Coordination Function (DCF)	12
2.3.2	Point Coordination Function (PCF)	13
2.4	Netzwerkkonzepte	14
3	Antennentechnik.....	16
3.1	Funkausbreitung	16
3.2	Antennen.....	16
4	Workshop: Bau einer Pringles Antenne	18
5	Literatur	20
	Anhang	21

1 Einleitung

Wireless Local Area Network (WLAN) steht für eine drahtlose Netzwerktopologie nach dem IEEE Ethernet Standard in einem lizenzfreien Spektrum (ISM Band)¹. Dabei können Bandbreiten bis zu 54 MBit/s gewährleistet werden.

Im Zeitalter der mobilen Systeme und des Internets kommt einer drahtlosen Infrastruktur höchstes Interesse zu gute. Intel postuliert, dass im Jahre 2006 vier von fünf Laptops mit einem WLAN Anschluss ausgestattet sein werden. Die Analysten von Frost & Sullivan unterstreichen diese Prognose. Sie erwarten für den europäischen Markt stetig steigende Gewinnmargen (Abbildung 1-1).



Abbildung 1-1: Umsatzprognose WLAN [FRO01]

1.1 Wire vs. wireless

Das klassische, konventionelle LAN ist drahtgebunden und basiert auf Koaxial-, Twisted-Pair oder Glasfaserkabeln. Drahtgebundene Netze sind an die vorhandene Struktur anzupassen und bieten selten einen hohen Grad an Flexibilität oder Austauschbarkeit, dafür ist die Technik ausgereifter. Moderne WiredLANs stellen eine hohe Bandbreite sicher und bieten Möglichkeiten zur Netzsicherheit.

Drahtlose Netze nutzen das Medium Luft. Dieses Medium ist von seiner Beschaffenheit sensibel und omnipresent. Dies sind Risiken, die aber Vorteilen, wie z.B. einer Kostendegression durch Einsparung der Kabelverlegung oder einer erhöhten Mobilität entgegenstehen.

¹ ISM - Industrial Scientific Medical

1.2 Alternativen

Die Industrie bietet neben WLAN noch andere Möglichkeiten zur drahtlosen Datenübertragung, die ähnliche Ziele verfolgen. Bei der Konzeption eines Netzwerkes müssen also alle gängigen technischen Wege mit ihren Vor- und Nachteilen evaluiert werden. Die kommerziell interessantesten drahtlosen Techniken werden nachfolgend aufgeführt.

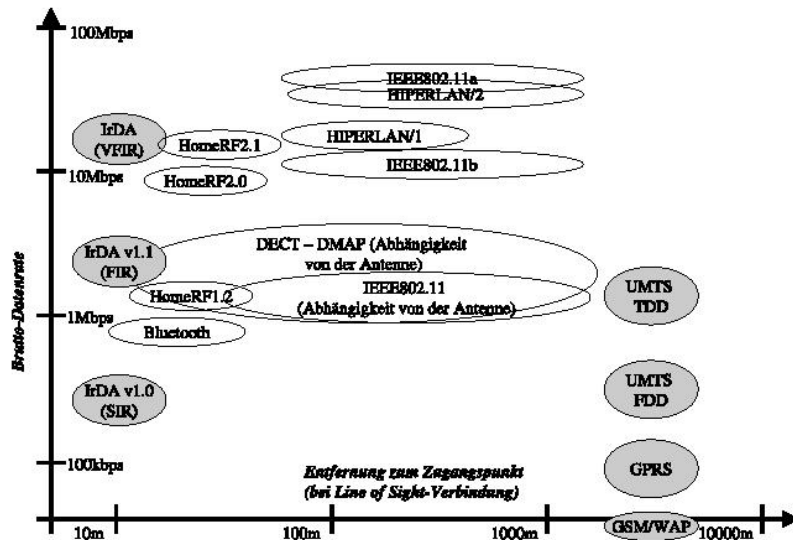


Abbildung 1-2: Alternative Technologien [SIK01]

Die Abbildung 1-2 zeigt Referenzwerte und soll einen groben Umriss über alternative Standards verschaffen. Dargestellt wird die angestrebte Brutto Übertragungsgeschwindigkeit in Abhängigkeit der Übertragungsreichweite.

1.2.1 IrDA

Infrared Data Association (IrDA) ist ein auf Infrarot basierender Standard, der mit einer Übertragungsrate von 115 KBit/s bis 4 MBit/s vorrangig zu einer lokalen Kopplung von mobilen Endgeräten konzipiert ist. Typische Distanzen liegen im Bereich von 2m. In der neusten Version IrDA 2.0 sollen auch Geschwindigkeiten von bis zu 20 MBit/s angestrebt werden.

1.2.2 Bluetooth

Bluetooth ist das bekannteste Konkurrenzprodukt. Es ist vorrangig als Kabelersatz vorgesehen und bietet dementsprechend eine niedrige Übertragungsrate von 1 MBit/s bei einer Reichweite von bis zu 10m.

Schwerpunkt dieser Technologie ist der geringe Stromverbrauch, der realisiert wird, indem die Geräte verschiedene Verbindungszustände aufnehmen.

Die Problematik von Bluetooth liegt in der Interoperabilität mit WLAN. Beide Techniken nutzen das ISM Band. Somit ist kein Schutz vor Interferenzen gewährleistet.

Die IEEE Organisation ist bemüht, Erweiterungen der Standards zu verabschieden, um diesen Konflikt zu lösen und somit beide Technologien kommerziell noch interessanter zu machen.

1.2.3 Home RF

HomeRF ist die Weiterentwicklung von Digital European Cordless Telecommunications (DECT). DECT ist der klassische Kommunikationsstandard von schnurlosen Telefonen. HomeRF ergänzt den Standard von der reinen Sprachübertragung zu der Option, auch Daten zu verschicken. In der Version 2.1 überträgt HomeRF Daten mit einer Rate von 20 MBit/s.

1.2.4 Mobilfunkgeräte der 3. Generation

Im Mobilfunk ist Universal Mobile Telecommunications System (UMTS) die aktuellste Technologie. Die so genannten Handies der 3. Generation werden im Stande sein, verstärkt multimediale Dienste auszuführen. Dabei wird der reinen Sprachübertragung ein sinkender, aber immer noch ausschlaggebender Stellenwert zugeordnet.

Die dazu recht kleine Übertragungsgeschwindigkeit von 384 KBit/s wird aber mit einer konkurrenzlosen Erreichbarkeit kompensiert.

1.3 Interoperabilität

Eine Koexistenz der Techniken für sehr unterschiedliche Versorgungsbereiche ist wahrscheinlich. Zusammenfassend lassen sich drahtlose Technologien in drei Kategorien gruppieren (vgl. Abbildung 1-3).

WPAN steht für Wireless Personal Area Network und vereint alle Funktechnologien, die auf einen beschränkten Einsatzbereich ausgerichtet sind. Dazu zählen unter anderen die besagten Standards Bluetooth und IrDA.

Wireless Wide Area Network (WWAN) bezeichnet alle globalen Wege der Datenübertragung, wie z.B. GSM² oder UMTS.

Abbildung 1-3 verdeutlicht, dass niemals eine einzelne Technologie dominieren wird. Vielmehr muss eine Zusammenarbeit aller Standards als Vision der Zukunft angestrebt

² GSM - Global System for Mobile Communication

werden, um allen individuellen Wünschen gerecht zu werden und ein flächendeckendes, drahtloses Netzwerk zur Verfügung stellen zu können.

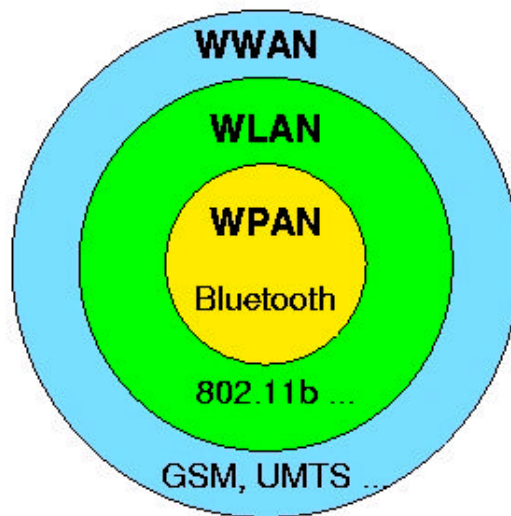


Abbildung 1-3: Gruppierung drahtloser Standards [HÜB02]

In diesem Kontext steht WirelessLAN als technisch und wirtschaftlich interessantester Kompromiss und begründet somit seine Rolle als wichtigstes Bindeglied zum drahtgebundenen Netz. WLAN wird dabei niemals das „klassische“ Netz verdrängen, es wird aber eine notwendige Erweiterung sein.

2 IEEE 802.11

2.1 Standard

Seit dem Jahr 1992 gibt es diverse proprietäre drahtlose Netzwerklösungen einzelner Hersteller, die sich mit einer Datenrate weit unter kommerziell interessanten Bandbreiten begnügten, und die nur untereinander interoperabel waren (Abbildung 2-1).

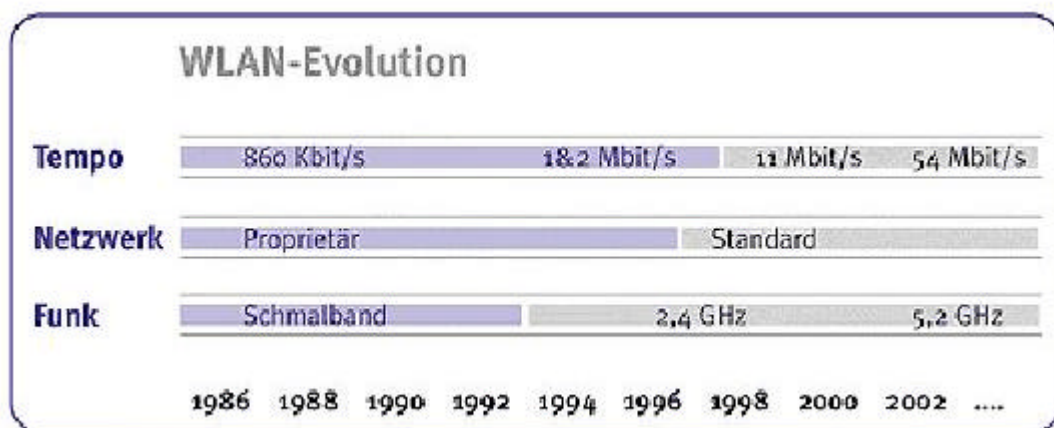


Abbildung 2-1: historische Entwicklung von WLAN [ART02]

Erst im Jahre 1997 verabschiedete die IEEE Organisation einen einheitlichen Standard. Geräte, die mit diesem Standard konform sind, und die somit eine herstellerunabhängige Interoperabilität garantieren, werden in diesem Zusammenhang auch als WiFi-kompatibel (Wireless Fidelity) bezeichnet.

Mit den Erfahrungen des IEEE 802.xx Standards, der die ersten beiden Layer des ISO/OSI³ Modells für lokale Netze definiert, wurde der IEEE 802.11 Standard für drahtlose Netze verabschiedet.

Dieser Standard konstituiert folgende Spezifikationen:

- ? 2,4 GHz – 2,485 GHz (13 Kanäle in Deutschland)
- ? lizenzfreies ISM Band
- ? Datenraten von 1 und 2 MBit/s
- ? Vielfachzugriff mit Träger- und Kollisionserkennung CSMA/CA⁴

Bis heute stehen die IEEE 802.11 Standards unter stetiger Erweiterungen, wobei IEEE 802.11a und IEEE 802.11b herausstechen. IEEE 802.11b ist heute der verbreitetste Standard, der mit einer Übertragungsrate von 11 MBit/s im 2,4GHz Bereich operiert

³ ISO/OSI – International Standardization Organisation/ Open System Interconnection

⁴ CSMA/CA – Carrier Sense Multiple Access/ Collision Avoidance

und das DSSS-Verfahren (vgl. Kapitel 2.2.3) verwendet. Um der ständigen Nachfrage nach Bandbreite gerecht zu werden, ist der IEEE 802.11a Standard entwickelt worden, um Geschwindigkeiten bis zu 54 MBit/s erreichen zu können. Realisiert wird dies in dem ebenfalls lizenzfreien 5,2 GHz Band mit dem OFDM Verfahren (vgl. Kapitel 2.2.4). Die Verwendung eines höheren Frequenzbandes hat zwei Nachteile: einerseits werden höhere Frequenzen stärker gedämpft, andererseits ist dieses Spektrum in Europa nicht vollständig zugelassen. Die Ursache liegt in der Überlappung des Frequenzbandes mit RADAR und anderen Funkdiensten. Hier muss eine weitere Entwicklung noch abgewartet werden.

Weitere wichtige Teilstandards und Erweiterungen sind in Tabelle 2-1 angegeben.

IEEE 802.11d	Aktualisierung der Regulatory Domains
IEEE 802.11e	Quality of Service (QoS)
IEEE 802.11f	Generalisierung der Verwaltungsdaten von Access Points mittels Inter Access Point Protocol (IAPP)
IEEE 802.11g	22 MBit/s im 2.4GHz Spektrum (OFDM)
IEEE 802.11h	Dynamisches Frequenz- und Leistungsmanagement bei Interferenzen (Dynamic Channel Selection, Transmission Power Control)
IEEE 802.11i	Authentifizierung und Sicherheit

Tabelle 2-1: IEEE 802.11 Erweiterungen

2.2 Bitübertragungsverfahren

Die Bitübertragungsschicht, die erste Ebene (Physical Layer) nach dem ISO/OSI Modell (vgl. Abbildung 2-2), stellt bislang die grundlegendsten Unterschiede zu der Drahtgebundenheit her, weil nun Informationen mit Hilfe von elektromagnetischen Wellen über das Medium Luft transportiert werden. Dieses Medium garantiert eine erhöhte Störanfälligkeit, die mit notwendigen Verfahren kompensiert werden muss.

Die Bitübertragungsschicht besteht aus einer mediumabhängigen (Physical Media Dependent) und einer mediumunabhängigen Schicht (Physical Layer Convergence Protocol), wobei die erstgenannte die Modulations- und Kodierungstechnik festlegt. Die ersten proprietären Übertragungen fanden schmalbandig statt, sind aber in der nächsten Generation durch Spreizspektrumtechniken (Spread Spectrum Technology)

abgelöst worden. Infrarot (IR) spielt in dem IEEE 802.11 Standard nur eine optionale Rolle, die nicht weiter kommerziell genutzt wird.

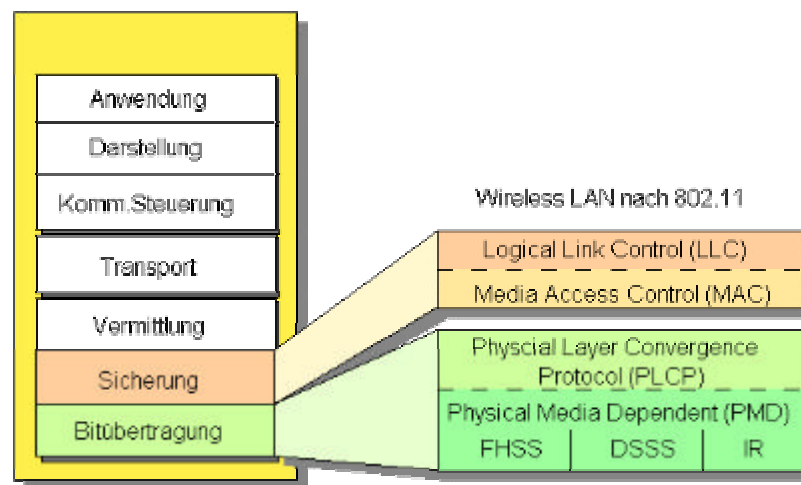


Abbildung 2-2: Einordnung von IEEE 802.11 im ISO/OSI Modell [KOW02]

2.2.1 Schmalbandübertragung

Bei einer Schmalbandübertragung (Narrowband Technology) wird die digitale Datenübertragung auf je eine spezielle Trägerfrequenz aufmoduliert. Mehrere verschiedene Kanäle werden durch mehrere verschiedene Trägerfrequenzen realisiert. Störungen auf diesen Frequenzen wirken sich auf die Datenübertragung aus. Außerdem können diese Kanäle leicht detektiert werden, es ist nur eine Frequenzabtastung wie bei der Sendersuche eines Radios nötig.

2.2.2 Frequency Hopping Spread Spectrum (FHSS)

In dem FHSS Standard sind nach IEEE 802.11 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 an Hand einer Basisfolge $b(i)$ berechnet (Tabelle 2-2), die einer Pseudozufallskette im Intervall von 0 bis 79 entspricht.

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	-

Tabelle 2-2: pseudozufällige Vergabe der Kanalnummer

Das Modulationsverfahren ist bei einer Datenrate von 1 MBit/s 2 Level Gaussian Frequency Shift Keying (2 level-GFSK), bei 2 MBit/s wird 4 level-GFSK eingesetzt. Nähere Informationen befinden sich im Anhang. Tritt ein Fehler beim Übertragen auf (Kollision, Störung...), kann das gleiche Paket auf einer anderen Frequenz versendet werden. Ein Abhören der Informationen ist nur möglich, wenn die Sendefrequenz bekannt ist. Diese Frequenz wird vor jeder Kommunikation von Sender und Empfänger vor Beginn nach Tabelle 2-3 *pseudozufällig* festgelegt.

Region	Sendefrequenzen	Kanäle	Berechnung der Kanalnummer ⁵
USA	2,402 – 2,480 GHz	2..80	$[b(i)+x] \bmod 79 + 2$
Europa	2,400 – 2,480 GHz	2..80	$[b(i)+x] \bmod 79 + 2$
Japan	2,473 – 2,495 GHz	73..95	$[(i-1) \cdot x] \bmod 23 + 73$

Tabelle 2-3: Ermittlung der Sendefrequenz (FHSS)

Nur wenige Distributoren halten noch am FHSS Verfahren fest, denn mit einer Übertragungsgeschwindigkeit von 2 MBit/s wird diese Technologie den heutigen Ansprüchen nicht mehr gerecht.

2.2.3 Direct Sequence Spread Spectrum (DSSS)

Beim DSSS-Verfahren stellt ein konstante Anzahl an Kanälen der Breite von 22 MHz zur Verfügung (in Deutschland 13 Kanäle, vgl. Anhang 1-1). Bei einem empfohlenen Kanalabstand von 25 MHz sind drei überlappungsfreie Kombinationen möglich.

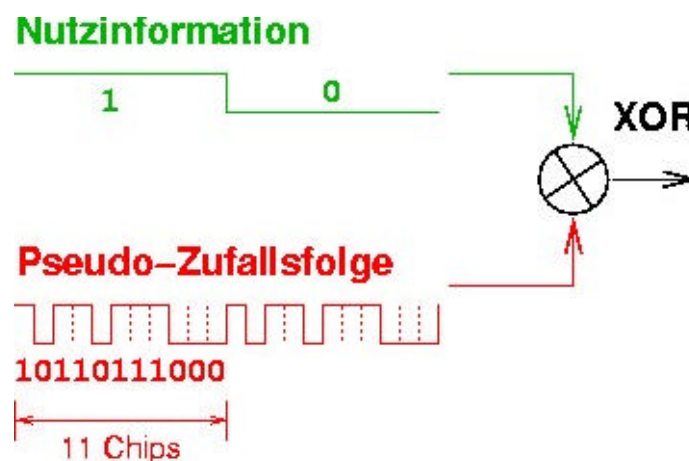


Abbildung 2-3: Modulation der Sendeinformation (DSSS) [HÜB02]

⁵ x - Offset

Jedes zu übertragende Bit wird mittels einer 11 Bit langen zufälligen Bitfolge (Chip), die sehr gute Autokorrelationseigenschaften aufweist, kodiert und mittels eines "Doubly Balanced Mixer" auf 13 MHz Bandbreite aufgespreizt gesendet (vgl. Abbildung 2-3). Dieses Signal ist somit ein weites Breitbandsignal, dessen Spektraldarstellung wie ein Rauschen wirkt. Der Demodulationsprozess wird durchgeführt, indem dasselbe, zur Modulation verwendetes Signal mit dem eingehenden Signal multipliziert wird. Das Ergebnis ist ein Signal, das sein Maximum annimmt, wenn sich die beiden Signale gleichen. Das korrelierte Signal wird gefiltert und dann an den Demodulator weitergeleitet. Als Modulationsverfahren wird die Phasenmodulation (Phase shift keying) angewendet, die zu vier möglichen Übertragungsgeschwindigkeiten führt (vgl. Tabelle 2-4).

1 MBit/s	Differential Binary Phase Shift Keying (DBPSK)
2 MBit/s	Differential Quadrature Phase Shift Keying (DQPSK)
5,5 MBit/s	Complementary Code Keying (CCK)
11 Mbit/s	Code Keying (CCK) + DQPSK

Tabelle 2-4: Modulationsverfahren (DSSS)

Aufgrund der technischen Notwendigkeit nach Bandbreitenmaximierung, hat sich das DSSS Verfahren mit bis zu 11 MBit/s durchgesetzt und ist somit die augenblicklich von der Industrie favorisierte Technik. Eine baldige Ablösung durch die Teilerweiterung IEEE 802.11g (22 MBit/s, OFDM) ist wahrscheinlich.

2.2.4 Orthogonal Frequency Division Multiplexing (OFDM)

Das OFDM-Verfahren ist im Gegensatz zu den beiden vorigen Methoden kein Spreizspektrumverfahren. Nach IEEE 802.11a wird das Spektrum in 11 nicht überlappende Kanäle aufgeteilt. Hierbei wird eine Information parallel über mehrere Frequenzen, den Unterfrequenzen (Subcarrier), gesendet (vgl. Abbildung 2-4).

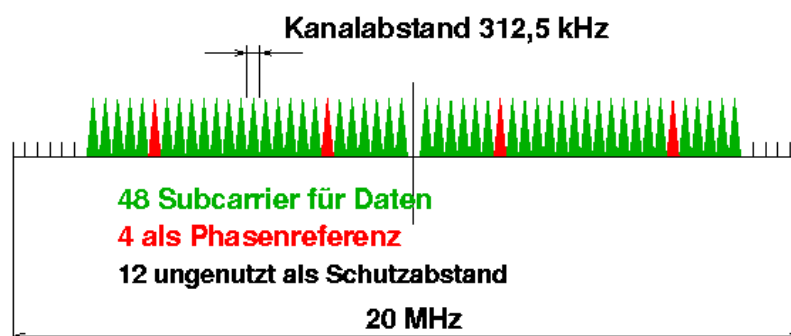


Abbildung 2-4: Frequenzaufteilung nach OFDM [HÜB02]

Durch die Aufspaltung in mehrere Sub-Kanäle wird erreicht, dass weniger Bits fehlerhaft übertragen werden, die mit einem Korrektionsalgorithmus (Forward Error Correction) behoben werden können. Außerdem lässt sich jede Unterfrequenz optimal an die Eigenschaft des Übertragungskanals anpassen. So können insbesondere Varianzen der Signallaufzeiten (Delay Spread) über variante Ausbreitungspfade (Multipath) berücksichtigt werden.

Der fundamentale Unterschied zum herkömmlichen Frequenzmultiplexverfahren, das relativ große Abstände zwischen den Unterfrequenzen aufweist und somit das komplette Spektrum ineffizient ausnutzt, ist die Interferenz der Sub-Frequenzen. Um trotzdem Störungen zu vermeiden, können nur orthogonale Unterfrequenzen genutzt werden. Dies bedeutet, dass die Signalrate entsprechend dem Abstand zweier benachbarter Unterkanäle gewählt wird. Technische Voraussetzung für eine verzerrungsfreie Überlagerung ist eine sehr hohe Genauigkeit der Trägerfrequenz.

Als Modulationsverfahren wird die Phasenmodulation (BPSK, QPSK)⁶ oder eine Kombination aus Amplituden und Phasenmodulation (QAM)⁷ verwendet. Durch Hinzunahme der Amplitude können 64 mögliche Zustände pro Frequenz (64-QAM) realisiert werden und erreichen eine Übertragungsgeschwindigkeit von 54 MBit/s. Eine Zusammenfassung der Modulationen befindet sich im Anhang (A 2-1).

2.3 Kanalzugriff

Der Datentransport über Funk lässt Analogien zum traditionellen IEEE Ethernet Standard zu. Auch hier konkurrieren mehrerer Stationen um den Zugriff auf ein Medium, wobei der aus den drahtgebundenen Standards bekannte CDMA/CD-Algorithmus nicht eingesetzt werden kann, weil die Feststellung einer Reihenfolge der Sender unmöglich ist. Eine Vermeidung von Kollisionen ist somit nicht gegeben, allerdings werden die Zeitspannen, in denen Kollisionen auftreten können, durch geschickte Algorithmen vermieden (CA)⁸. Der Zugriff erfolgt mit zwei unterschiedlichen Mechanismen (vgl. Abbildung 2-5), der Point Coordination Function (PCF) und der Distributed Coordination Function (DCF).

⁶ BPSK, QPSK - Binary Phase Key Shifting, Quadrature Phase Key Shifting

⁷ QAM - Quadrature Amplitude Modulation

⁸ Collision Avoidance

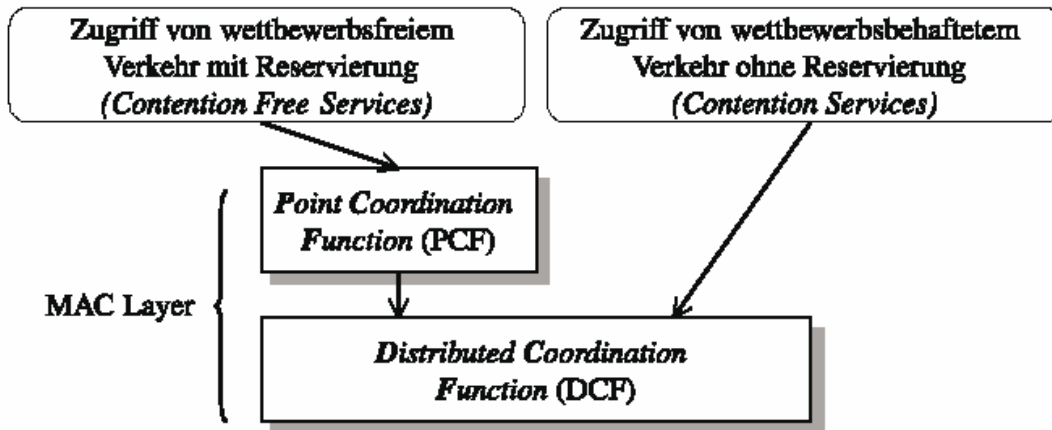


Abbildung 2-5: Zugriffsmechanismen auf einen Kanal [SIK01]

2.3.1 Distributed Coordination Function (DCF)

Bevor eine Übertragung stattfinden kann, muss das Medium abgehört werden (Carrier Sense). Zwei Fälle sind möglich. Ist das Medium nicht belegt, kann nach einer Abhörzeit (DIFS)⁹ das Senden auf diesem Kanal beginnen (Station A sendet an B, Abbildung 2-6). Die Versendung der Quittung (ACK)¹⁰ erfolgt nach einer weiteren Wartezeit (SIFS)¹¹. Diese Wartezeiten haben eine konstante Länge, so dass alle Stationen in einem gleichen „Takt“ arbeiten. Die Verständigung wird über Broadcasting aller relevanten Stations- und Kanalinformationen erreicht. Ist das Medium belegt, wird die Übertragung in einen Wartezyklus (Backoff) gesetzt. Nach Ablauf der Wartezeit wird das Medium erneut kontrolliert (Station C, vgl. Abbildung 2-6).

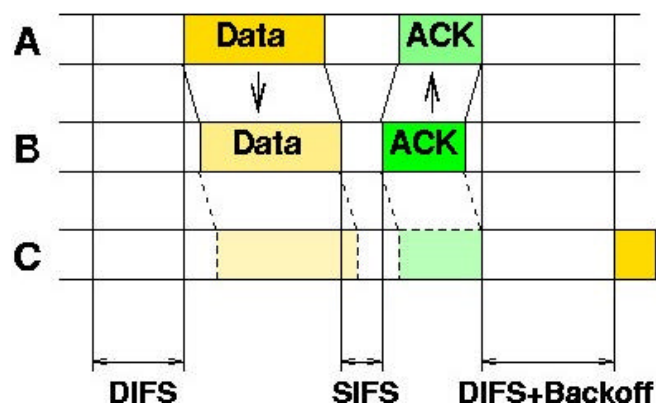


Abbildung 2-6: Stationen A, B und C greifen auf einen gemeinsamen Kanal zu [HÜB02]

⁹ DCF Interframe Space

¹⁰ Acknowledgement

¹¹ Short Interframe Space

Das Verfahren funktioniert zuverlässig, wenn alle Stationen direkt miteinander kommunizieren. Normalerweise gefährden Hindernisse (hidden nodes) einen direkten Kontakt, so dass ein weiterer Zugriffsmechanismus (RTS/CTS)¹² verwendet wird.

Abbildung 2-7 zeigt den gemeinsamen Kanalzugriff der Stationen A und B unter der Nebenbedingung, dass kein Informationskontakt zwischen der Station A zu der Station D besteht.

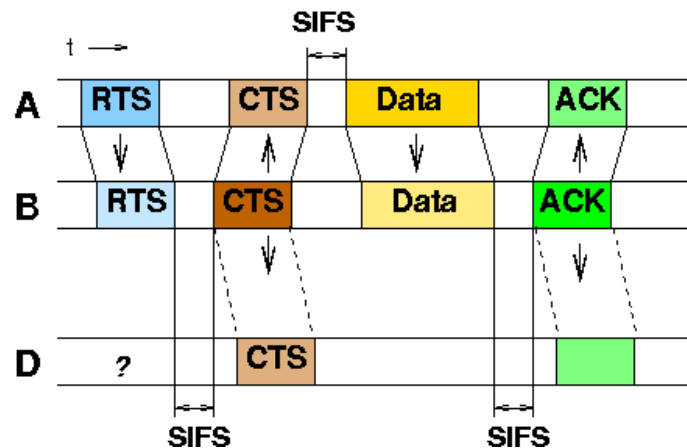


Abbildung 2-7: Kommunikation der Stationen A,B ohne direkten Kontakt zu Station D [HÜB02]

Ein RTS-Frame wird an alle sendewilligen Stationen gesendet. Dieser Rahmen enthält Informationen über die Dauer der Datenübertragung. Der adressierte Sender quittiert den Erhalt mit einem CTS-Frame ebenfalls an alle vorhandenen Stationen, die übrigen Empfänger schalten für die angegebene Zeit in einen unabhängig vom Backoff-Prozess vorgegebenen Wartemodus. Die Verwendung der SIFS-Zeit sichert der CTS-Antwort eine höhere Priorität gegenüber der normalen Übertragung. Schlägt die Sendung eines CTS-Frames fehl, erfolgt ein erneutes Senden des RTS-Frames nach Ablauf des Backoff-Zyklus.

2.3.2 Point Coordination Function (PCF)

Die PCF ist ein optionales Verfahren, zeitkritischen Diensten priorisierten Zugriff zu gewähren. Die PCF steuert die Übertragung der Rahmen während einer wettbewerbsfreien Zeit (CFP)¹³, die sich mit der durch die DCF gesteuerten Wettbewerbsperiode abwechselt (CP)¹⁴. Die CFP wird in regelmäßigen Zeitabständen

¹² Ready to Send / Clear to Send

¹³ CFP - Contention Free Period

¹⁴ CP - Contention Period

mit der CFP-Rate wiederholt und startet mit der Übertragung eines Beacon-Rahmens, der die maximale Dauer der CFP enthält (Abbildung 2-8).

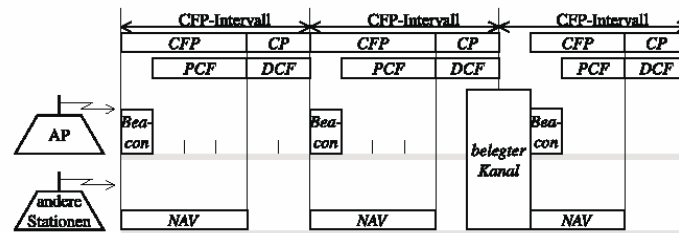


Abbildung 2-8: Priorisierter Zugriff auf einen Kanal (PCF) [SIK01]

2.4 Netzwerkkonzepte

Der IEEE 802.11 Standard lässt verschiedene Kombinationen offen, wie ein drahtloses Netzwerk aufgebaut werden kann. Diese sollen nachfolgend kurz erwähnt werden.

2.4.1 Ad-Hoc

Das Ad-Hoc Netz (vgl. Abbildung 2-9) ist eine direkte Verbindungen von mobilen Stationen ohne Zugangspunkt.

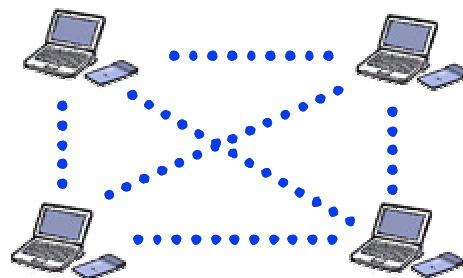


Abbildung 2-9: Ad-Hoc Netz

Somit ist dies der einfachste Weg, eine drahtlose Kommunikation aufzubauen.

2.4.2 Infrastruktur-Netze

Das Infrastruktur-Netz (vgl. Abbildung 2-10) ist die Kombination aus drahtlosem und drahtgebundenem Netz. Notwendig für solch eine Anbindung ist ein Zugangspunkt (Access-Point). Der Access-Point koordiniert den gesamten Datenverkehr. Er vermittelt zwischen LAN und WLAN sowie auch zwischen den mobilen Stationen (z.B. laptop-to-laptop connection).

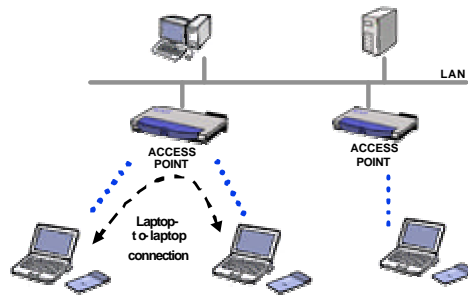


Abbildung 2-10: Infrastruktur

2.4.3 Roaming

Das aus dem Mobilfunk bekannte Verfahren des Roamings (vgl. Abbildung 2-11) ermöglicht eine erweiterte, drahtlose Erreichbarkeit.

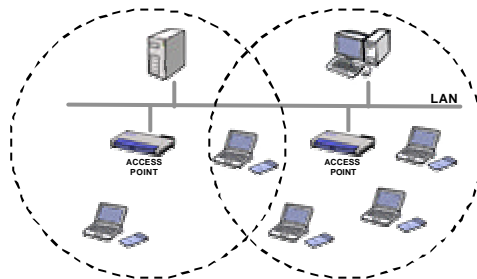


Abbildung 2-11: Roaming

Vorraussetzung hierfür ist, dass sich die Mobilstation im gleichen Sub-Netz befindet. Der WLAN Benutzer hat den Vorteil einer größeren Mobilität, ohne Veränderungen an seiner Konfiguration tätigen zu müssen.

3 Antennentechnik

3.1 Funkausbreitung

Drahtloser Datenaustausch nach IEEE 802.11b findet im regulierungsfreien 2.4 GHz Spektrum statt. Elektromagnetische Wellen haben somit nach der Wellengleichung:

$$c = \lambda \cdot f$$

eine Wellenlänge von 12.5 cm. Sie werden auch als *quasioptisch* bezeichnet, weil ihr Verhalten dem Licht gleicht. Nach Möglichkeit sollte eine hindernisfreie Sicht zwischen Empfänger und Sender bestehen (Line of Sight). Außerhalb von Gebäuden sollten auch saisonale Wetterschwankungen berücksichtigt werden. Die markanteste Beeinträchtigung auf die Übertragung hat der Feuchtigkeitsanteil der Luft. Wassermoleküle sind die simpelsten natürlichen Antennen (Dipole) und absorbieren somit die gesendete Leistung.

Um Antennen vergleichen zu können, werden unterschiedliche Maße angegeben:

? dB - logarithmisches Dämpfungs- oder Verstärkungsmaß

$$P [\text{dB}] = 10 \log P [\text{W}]$$

? dBi - Antennengewinn gegenüber einem Isotropstrahler (Punktantenne)

? dBm - logarithmisches Leistungsmaß

$$P [\text{dBm}] = 10 \log P [\text{mW}]$$

? Ausbreitungsdämpfung (path loss)

$$L = 20 \log(d) + 20 \log(f) + 32.44$$

d - Entfernung [km]

f - Frequenz [MHz]

L - Ausbreitungsdämpfung im Freiraum [dB]

3.2 Antennen

Um einen Einblick in die Welt der für den 2,4 GHz Bereich geeigneten Antennen zu erhalten, werden in Tabelle 3-1 vier charakteristische Antennen mit ihren horizontalen und vertikalen Abstrahleigenschaften aufgeführt. Sie sollen nur einen kurzen Einblick in die Welt der Antennentechnik geben, auf die hier nicht näher eingegangen werden kann. Dieses Thema darf im Zusammenhang mit WLAN nicht missachtet werden, weil die Antenne über die Qualität und Quantität der Übertragung entscheidet und wie in Kapitel 4 gezeigt wird, am einfachsten moduliert werden kann.


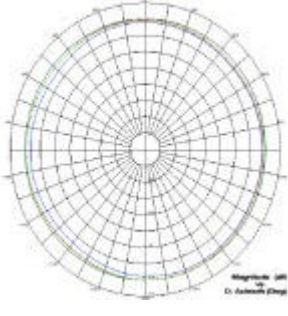
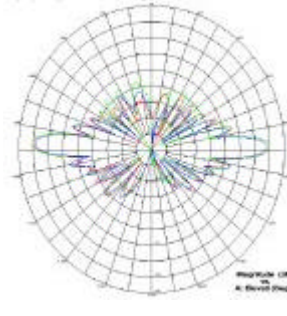
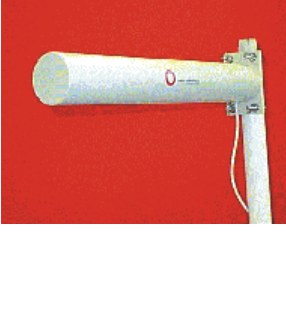
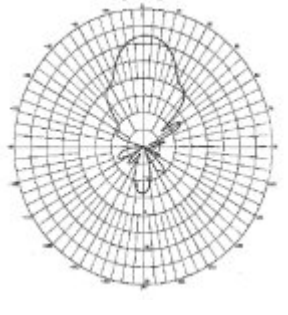
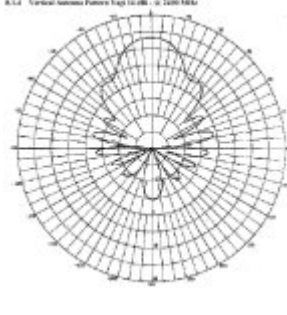
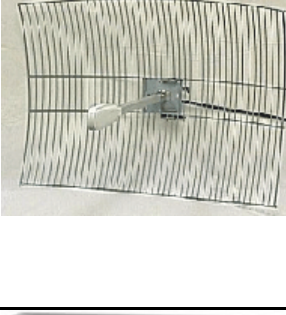
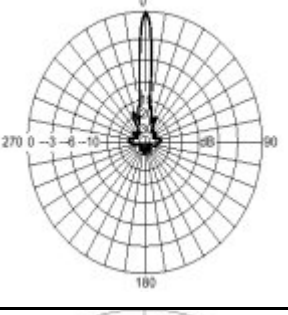
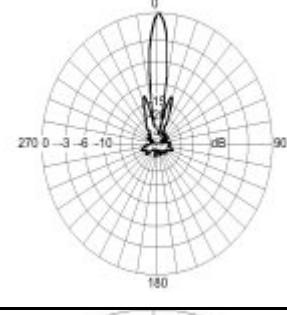

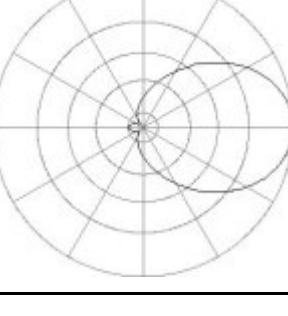
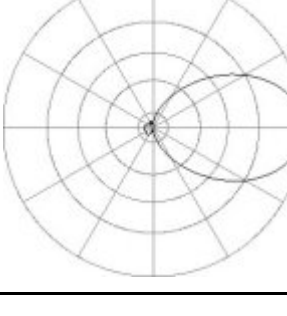
Rundstrahl Antenne, Omni directional , 10 dBi, 360 Grad Horizontal / 8 Grad Vertikal, 5.5 km Reichweite.			
Stabantenne, 14 dBi, Abstrahlung 30 Grad, max. Reichweite 7 km mit 1 MBit/s (bei freier Sicht- verbindung)			
Parabolantenne, 24 dBi, Abstrahlung 10 Grad, max. Reichweite 11 km (bei freier Sichtverbin- dung)			
Planar Antenne, 8,5 dBi,, horizontal - 75°, vertikal - 60°, Polarisation linear, vertikal			

Tabelle 3-1: Antennen

4 Workshop: Bau einer Pringles Antenne

Die integrierten Antennen in den handelsüblichen WLAN - Komponenten sind Hertzsche Dipole. Damit können outdoor Distanzen von nicht mehr als 100m überbrückt werden. Motivation war der Bau einer effizienteren Antenne mit einfachen und gängigen Mitteln.



Abbildung 4-1: Antenne vor dem Bau

Die Antenne besteht aus drei Teilen: Reflektor, Kollektor und Injektor.

Die metallische Ummantelung und die zylindrische Symmetrie begründen, wieso die Wahl auf eine Pringlesdose als Reflektor gefallen ist. Die zylindrische Form sorgt für eine Bündelung der Wellen auf dem Kollektor. Es bildet sich eine stehende Welle der Länge λ aus, die vom Injektor an der Stelle des Maximums, also bei $\lambda/4$, abgegriffen wird.

Bauteil	Anzahl	Masse	Beschreibung
Pringles Chipsdose	1		Reflektor
Aluminiumrohr	4	3cm($\lambda/4$)	Kollektor
Gewindestange	1	M3.3	Verbindet Aluröhre mit Muttern
Unterlegscheiben	5		Koaxialfilter
Muttern	2	M4	
Pringles Deckel	2		Träger

Tabelle 4-1: Bauteile

Der Injektor wird über ein Kupferkabel mit einem passenden Koaxialstecker verbunden, und bildet mit einem passenden, dämpfungsarmen Kabel den Anschluss an die WLAN Karte. Die Wahl des Koaxialsteckers und des Kabels ist individuell zu treffen, weil es keinen bislang einheitlichen Weg zur Anbindung einer externen Antenne gibt.

Mit den Mitteln nach Tabelle 4-1 zu dem Ergebnis in Abbildung 4-2.



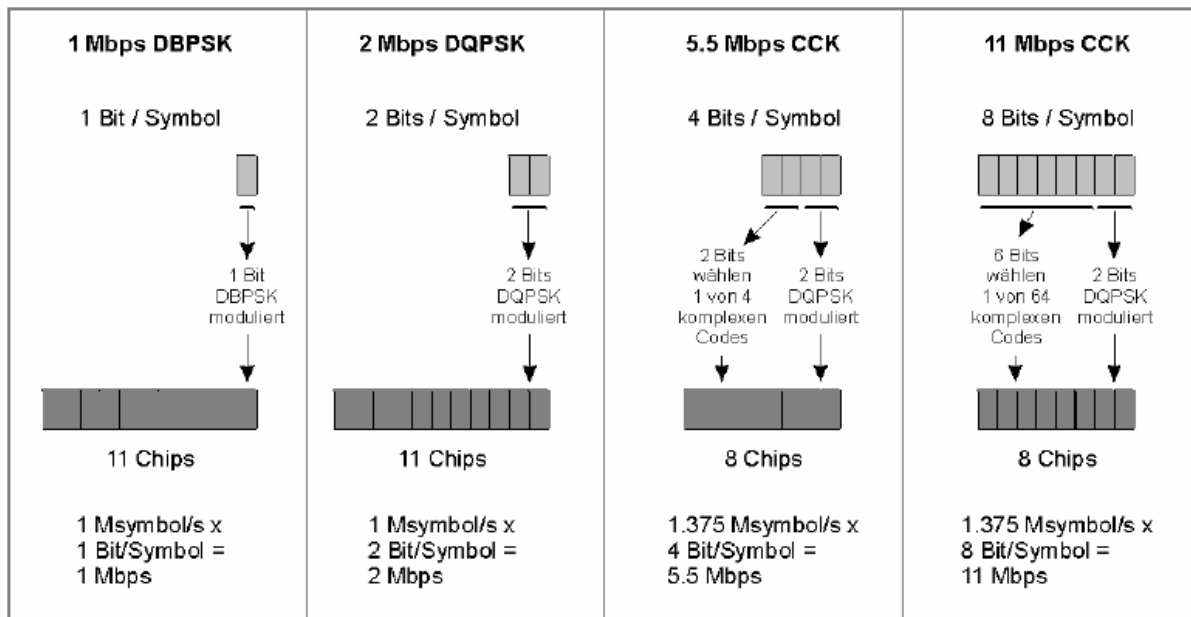
Abbildung 4-2: Antenne (Kollektor, Reflektor und Injektor)

Weitere Informationen befinden sich im Internet unter [FLI02].

5 Literatur

- [ART02] Artem
Whitepaper März 2002
<http://www.artem.com>
- [FLI02] Flickenger, Rob
Antenna on the Cheap (er, Chip)
O'Reilly Network Web logs
- [FRO02] Frost & Sullivan
<http://www.frost.com>
- [GER02] Gergeleit, M. / Trikaloitis, S.R.
Wireless Networks
Universität Magdeburg, Magdeburg 2002
- [HÜB02] Hübner, Uwe
Wireless Local Area Networks
TU Chemnitz, Chemnitz 2002
- [IEEE] IEEE Organisation
<http://www.ieee.org>
- [KOW02] Kowalk, W.
Rechnernetze
Universität Oldenburg, Oldenburg 2002
- [MYR02] Myrach, Thomas
Mobile Computing
RWTH Aachen, Aachen 2002
- [SIK01] Sikora, Axel
Wireless LAN – Protokolle und Anwendungen
Addison-Wesley Verlag, München 2001

Anhang



A 1-1: Modulationsverfahren (DSSS) [GER02]

0	1	2	3	4	5	6
Modulation	Codierte Bits pro Unterkanal	Codierte Bits pro OFDM-Symbol (1) * 48	Codierungsrate	Daten-bits pro OFDM-Symbol (2) * (3)	Symbol-Rate [Msymbol/s]	Daten-Rate [Mbps] (4) * (5)
BPSK	1	48	1/2	24	0.25	6
BPSK	1	48	3/4	36	0.25	9
QPSK	2	96	1/2	48	0.25	12
QPSK	2	96	3/4	72	0.25	18
16-QAM	4	192	1/2	96	0.25	24
16-QAM	4	192	3/4	144	0.25	36
64-QAM	6	288	2/3	192	0.25	48
64-QAM	6	288	3/4	216	0.25	54

A 2-1: Modulationsverfahren (OFDM) [GER02]