IEEE 802.11b

Ronald Nitschke

Potsdam, 11. Juli 2003

*http://www.**802.11b**.de.ms*

Inhalt

Einleitung 3
Der Standard IEEE 802.11b 3
Technische Daten 4
  Frequenzbereich: 4
  Technologien: 4
  Modulationsverfahren: 4
  Reichweite: 4
  Bandbreite 5
Der Physical Layer 6
  Architektur des PHY-Layer 6
  Die Spread Spectrum Technologien 7
    Frequency Hopping Spread Spectrum (FHSS) 7
    Direct Sequence Spread Spectrum (DSSS) 7
Multiple Access Probleme (MA-Problem) 9
Der MAC-Layer 10
  CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) 10
Roaming 12
Betriebsmodi von 802.11b 13
  Ad-hoc 13
  Infrastruktur 13
802.11-Zusatzfeatures 13
Sicherheit im Funknetz 14
  Authentifizierung auf Link- und Benutzerebene 14
Abbildungsverzeichnis 15

Einleitung

Es gibt eine Vielzahl von Anwendungsfällen, in denen der Einsatz der drahtlosen Kommunikation in Betracht gezogen werden kann. So ist es beispielsweise vorstellbar, während einer Beratung oder Konferenz schnell ein Netzwerk einzurichten und somit jedem Teilnehmer bestimmte Daten zur Verfügung zu stellen. Das dürfte der typische Anwendungsfall für ein Ad-hoc Netzwerk sein.
Andererseits kann es durchaus wünschenswert sein, mit einem mobilen Gerät auf Serverdaten oder gar das Internet zuzugreifen. Dafür kommt ein Infrastruktur Netzwerk mit einem oder mehreren Access Points (Zugangspunkten) in Frage.

Der Standard IEEE 802.11b

Als erstes ein Überblick über IEEE 802.11. Es haben sich verschiedene Arbeitsgruppen gebildet, die sich mit den verschiedenen Gebieten der drahtlosen Kommunikation beschäftigen (siehe Tabelle). Bei den WLAN-Technologien lassen sich zwei Hauptgruppen nach den Frequenzbereichen unterscheiden. Im klassischen 2,4-GHz-Band arbeitet 802.11b und sein rückwärtskompatibler Nachfolger 802.11g. Das 5-GHz-Band wird von 802.11a und 802.11h genutzt. Dann gibt es noch einige ergänzende Standards. IEEE 802.11c behandelt die Kopplung verschiedener Netzwerktopologien, 802.11e soll Quality of Service definieren und mit 802.11i sollen die Sicherheitslücken, die bei drahtlosen Netzten bis heute bestehen, geschlossen werden.

Arbeitsgruppe	Arbeitsgebiet
802.11a	54-Mbit/s-WLAN im 5 GHz-Band
802.11b	11-Mbit/s-WLAN im 2,4-GHz-Band
802.11c	Wireless Bridging
802.11d	"World Mode", regionsspezifische Anpassung
802.11e	QoS- und Streaming-Erweiterung für 802.11a/g/h
802.11f	Roaming für 802.11a/g/h (Inter Access Point Protocol IAPP)
802.11g	54-Mbit/s-WLAN im 2,4-GHz-Band
802.11h	54-Mbit/s-WLAN im 5-GHz-Band mit DFS und TPC
802.11i	Authentifizierung/Verschlüsselung für 802.11a/b/g/h (AES, 802.1x)

Abbildung 1 : Überblick über IEEE 802.11

Der Standard 802.11b ist eine abwärtskompatible Erweiterung des 802.11DS Standards, der 1997 von der IEEE als herstellerunabhängiger Standard für Wireless LANs (WLANs) verabschiedet wurde. In seiner momentanen Definition erreicht ein drahtloses Netzwerk nach dem Standard 802.11b eine Brutto-Datenrate von 11Mbit/s.
Es gibt auch 802.11b+, hierbei soll eine Verdopplung der Übertragungsrate erreichen werden. Bei 802.11b+ handelt es sich aber nicht um einen offiziellen Standard.

Technische Daten

Frequenzbereich:

Der verfügbare Frequenzbereich ist in den einzelnen Ländern unterschiedlich. Er ist in Nordamerika auf 900MHz und 2,4GHz im ISM-Band mit max. 1W Sendeleistung festgelegt. In Europa hat die ETSI den Frequenzbereich auf 2,4 GHz im ISM-Band mit max. 100mW Sendeleistung festgelegt. Die Bandbreite beträgt dabei 80MHz (2,4GHz-2,48GHz).

Region	Frequenzband (GHz)	Sendeleistung
USA	2,4000 – 2,4835	1000 mW
Europa	2,4000 – 2,4835	100 mW (EIRP)
Japan	2,4710 – 2,4970	10 mW/MHz
Frankreich	2,4465 – 2,4835	100 mW (EIRP)
Spanien	2,4450 – 2,4750	100 mW (EIRP)

Abbildung 2 : Verfügbare Frequenzbereich nach IEEE 802.11

Technologien:

Die für 802.11 verwendeten Technologien sind:
Frequenz Hopping Spread Spektrum (FHSS)
Direct Sequence Spread Spectrum (DSSS)
Infrarot (IR)

Modulationsverfahren:

Für FHSS und DSSS werden je nach Datenübertragungsrate verschiedene Modulationsverfahren eingesetzt.
FHSS:
2GFSK (2-Level Gaussian Frequency Shift Keying) 1MBit/s
4GSFK (4-Level Gaussian Frequency Shift Keying) 2MBit/s
DSSS:
DBPSK (Differential Binary Phase Shift Keying) 1MBit/s
DQSP (Differential Quadrature Phase Shift Keying) 2MBit/s, 5,5MBit/s, 11MBit/s

Reichweite:

Eine allgemeine Aussage über die Reichweite eines WLAN-Links (d.h. einer Punkt-zu-Punkt-Verbindung) lässt sich kaum machen, da die örtlichen Gegebenheiten einen großen Einfluss haben und es selbst von Hersteller zu Hersteller Unterschiede bis zum Faktor fünf gibt. Im Allgemeinen ist sie aber mit DECT (Digital Enhanced Cordless Telephone) vergleichbar: 300m mit Sichtkontakt und 30m im Gebäude.

Um eine hohe Flächendeckung zu erreichen, können mehrere Funkzellen eingerichtet werden, welche mittels eines Handovers die Möglichkeit bieten von einer Zelle zur nächsten zu wandern, ohne dass die Kommunikation abbricht.

Bandbreite

Die Bandbreite variiert zwischen 1 Mbit/s bei schlechter und bis zu 11 Mbit/s bei sehr guter Empfangsqualität. Die reale Bandbreite, d.h. die Bandbreite, die mit einer kabelgebundenen Verbindung vergleichbar ist, dürfte zwischen 512 kbit/s und 4 Mbit/s liegen. Nicht zu vergessen ist, dass ein AP wie ein Hub arbeitet, d.h. alle angemeldete Endgeräte teilen sich die theoretisch maximalen 11 Mbit/s.

Der Physical Layer

Architektur des PHY-Layer

Die Abbildung zeigt die verschiedenen Realisierungsmöglichkeiten der physikalischen Ebene des IEEE 802.11 Standards einschließlich der Erweiterungen aus IEEE 802.11a und 802.11b.

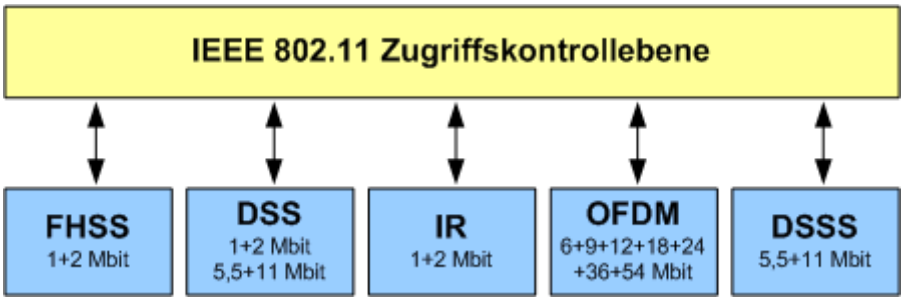

Abbildung 3 : Physikalische Ebenen im IEEE 802.11 Standard

Auf Grund der Tatsache, dass die Charakteristika der möglichen Übertragungsverfahren speziell in ihrem Zeitverhalten sehr unterschiedlich sein können, sieht 802.11 eine weitere Aufteilung der Protokolle in den einzelnen Schichten vor, die in der folgenden Abbildung dargestellt ist.

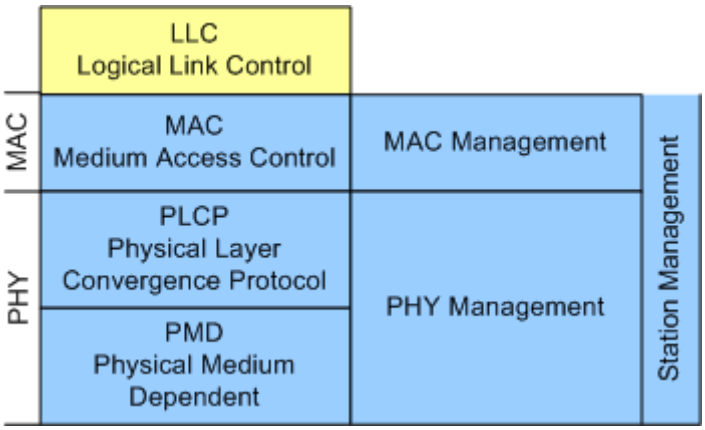

Abbildung 4 : 802.11-PHY Layer

In dieser Konfiguration übernimmt das Physical Medium Dependant Sublayer (PMD) die Modulation und Kodierung, während das Physical Layer Convergence Protocol (PLCP) eine für alle physikalischen Ebenen gleiche Schnittstelle zur Zugriffskontrollebene (MAC Sublayer) zur Verfügung stellt.

Die Spread Spectrum Technologien

IEEE 802.11 WLANs benutzen Spread Spectrum Technologien zur Erhöhung der Übertragungssicherheit. Das Spreizen eines Signals durch FHSS oder DSSS bewirkt, dass ein größerer Frequenzbereich benutzt wird als für die eigentliche Datenübertragung benötigt wird. Da das ISM-Band, in dem die WLANs nach IEEE 802.11 operieren, für industrielle, wissenschaftliche und medizinische Anwendungen reserviert ist und keinerlei amtlicher Genehmigung bedarf, tritt das Problem des *Multiple Access* auf. Das heißt, dass die physikalische Ebene von WLANs für einen geordneten und möglichst störungsfreien Betrieb zu sorgen hat.

Frequency Hopping Spread Spectrum (FHSS)

Bei FHSS wechseln Sender und Empfänger zyklisch die benutzte Frequenz, wobei sie die gleiche Reihenfolge einhalten (Hopping Sequence). Die durch andere Sender verursachten Störungen werden minimalisiert, da nur Sender und Empfänger, die mit gleicher Hopping Sequence arbeiten, kommunizieren können.
Andererseits ist jedoch bei FHSS der Aufwand auf der MAC-Ebene hoch, da die Frequenzwechsel gesteuert und synchronisiert werden müssen. Aufgrund besserer Leistungswerte hat sich DSSS durchgesetzt und wird in 802.11b ausschließlich verwendet, weshalb an dieser Stelle auf eine nähere Beschreibung von FHSS verzichtet wird.

Direct Sequence Spread Spectrum (DSSS)

DSSS: Funktionsprinzip

Im Gegensatz zu FHSS wird bei der Direct Sequence Spread Spectrum Technologie das Signal nicht zeitlich versetzt auf verschiedenen Kanälen versendet, sondern das schmalbandige Signal durch Multiplexen mit einem PN (Pseudo-Noise)- Code direkt in ein breitbandiges Signal umgewandelt. Da dadurch die Sendeintensität unter die Rauschgrenze abgesenkt wird, kann das Signal nur noch von Stationen Empfangen werden, die mit dem gleichen PN-Code arbeiten (vgl. CDMA).
Bei der Spreizung der 2Mbit/s Signalrate mit einem elfstelligen Chip-Code ergibt sich eine Bandbreite von 22MHz pro Sequenz .

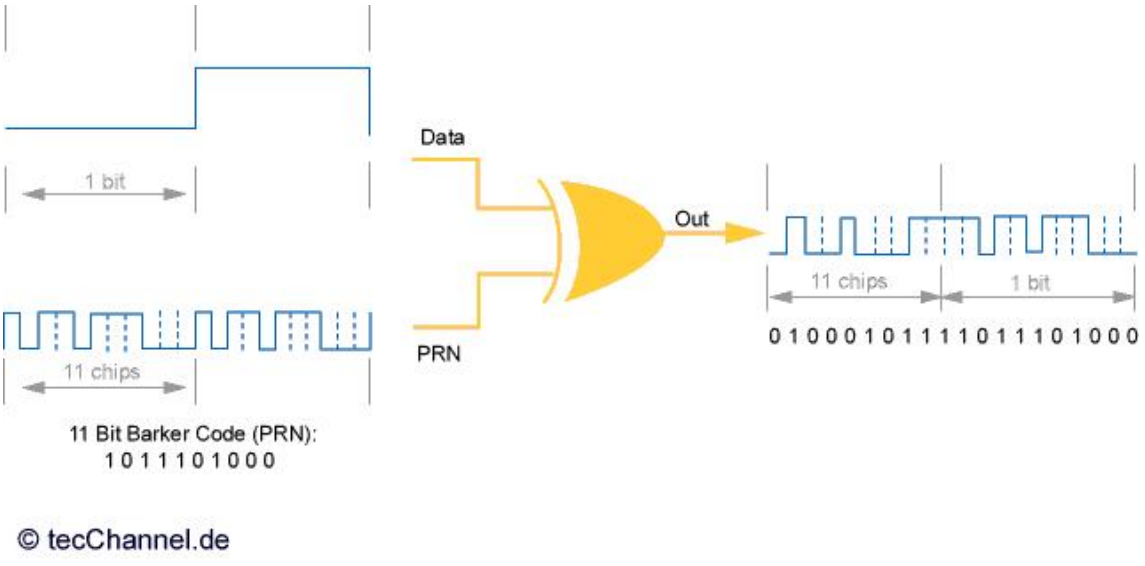

Abbildung 5 : Direct Sequence

Auf der Empfängerseite dient ein angepasster Korrelator zum Ausfiltern der Nutzdaten aus der überlagerten PN-Folge. Dabei wandelt er automatisch schmalbandige Störungen hoher Intensität in ein breitbandiges Rauschen niedriger Intensität um.

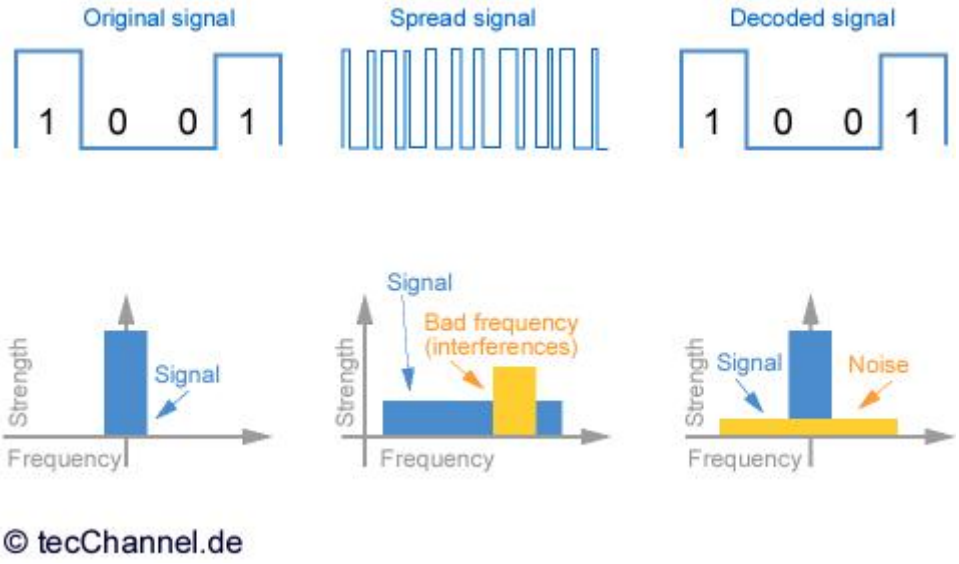

Abbildung 6 : Störunterdrückung bei DSSS

DSSS: Frequenznutzung

Das Frequenzband (2,4 – 2,4853 GHz) wird in 11 (USA) bzw. 13 (Europa) Kanäle unterteilt. Die Mitten-Frequenzen dieser Kanäle haben den Abstand von jeweils 5 MHz.

Kanal	Frequenz	Kanal	Frequenz
1	2412 MHz	8	2447 MHz
2	2417 MHz	9	2452 MHz
3	2422 MHz	10	2457 MHz
4	2427 MHz	11	2462 MHz
5	2432 MHz	12	2467 MHz
6	2437 MHz	13	2472 MHz
7	2442 MHz		

Abbildung 7 : DSSS-Kanäle im 2,4 GHz Band

Aus der Signalbreite von 22 MHz folgt, dass sich im ISM-Band lediglich drei DSSS-Kanäle überlappungsfrei nebeneinander anordnen lassen.

Multiple Access Probleme (MA-Problem)

Überschneiden sich die Sende- und Empfangsbereiche von verschiedenen Benutzern des 2,4 GHz Bandes, so tritt ein MA-Problem auf. Die physikalische Ebene von DSSS-Systemen hat die Aufgabe, für eine möglichst störungsfreie Verbindung der Teilnehmer untereinander zu sorgen. Dazu wird eine Kombination von CDMA (Code Division Multiplexing), FDMA (Frequency Division Multiplexing) und TDMA (Time Division Multiplexing) verwendet.
Das CDMA Verfahren benutzt dabei den PN-Code, um sich von anderen Benutzern des ISM-Bandes abzugrenzen.
Um Störungen von anderen IEEE-DSSS Systemen aus sich überschneidenden Sende- und Empfangsbereichen zu eliminieren, wird FDMA benutzt. Das heißt, dass benachbarte Systeme verschiedene Kanäle benutzen, um die gegenseitige Beeinflussung zu minimieren. Bis zu drei DSSS Systeme können gemeinsam in einem Empfangsbereich arbeiten, ohne sich gegenseitig zu stören.
Mittels TDMA wird der Zugriff der Teilnehmer eines Kanals geregelt.

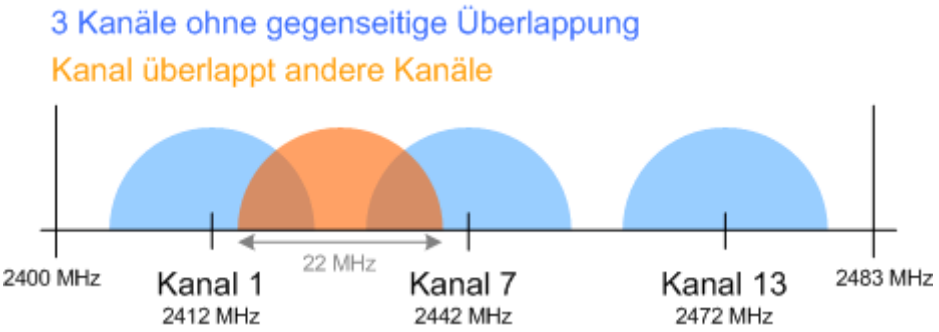

Abbildung 8 : IEEE 802.11b sieht für das ISM-Frequenzband bis zu 13 Kanäle vor.

Der MAC-Layer

Der MAC-Layer von 802.11b weist eine enge Verwandtschaft mit der kabelgebundenen Variante 802.3 auf. Allerdings muss der drahtlose Standard auf die Besonderheiten der Übertragungsstrecke Rücksicht nehmen. Selbst wenn das Senden und Empfangen gleichzeitig möglich wäre, würde das gesendete Signal alle anderen Signale maskieren. Es entfällt die Möglichkeit zum Erkennen von Kollisionen und 802.11b greift deshalb auf eine Zugangskontrolle (Access Control) nach dem CSMA/CA-Verfahren zurück.
CSMA/CA steht für Carrier Sense Multiple Access with Collision Avoidance. Es beschreibt den Zugriff auf einen gemeinsamen Kanal, indem dieser auf das Vorhandensein eines Trägersignals getestet wird. Der Unterschied zu IEEE 802.3 besteht in der Collision Avoidiance (Kollisions-Vermeidung), deren Implementierung als DCF (Distributed Coordination Function) oder PCF (Point Coordination Function) noch näher erläutert wird.
Weitere Mechanismen die die Zugriffskontrollebene zur Verfügung stellt sind:

- Unterscheidung zwischen Ad-hoc- und Infrastrukturnetzwerken
- Roaming
- Verschlüsselungs- und Authentifizierungsmechanismen
- Stromsparfunktionen für mobile Stationen

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

IFS (Interframe Space)

Eine zentrale Rolle bei der Funktionsweise des Zugriffsmechanismus spielt die Zeit zwischen zwei Datenpaketen, der so genannte Interframe Space (IFS). Der 802.11-Standard definiert vier verschiedene IFS-Zeiten, die unterschiedliche Prioritätsstufen für den Zugriff widerspiegeln. Dabei gilt: Je kürzer der IFS, desto höher die Priorität.

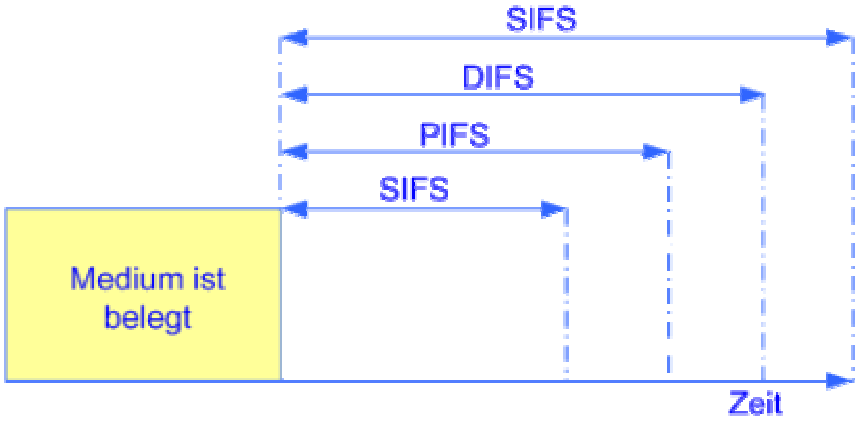

Abbildung 9 : CSMA/CA

EIFS: Extended Interframe Space
DIFS: Distributed Interframe Space
PIFS: Point Coordination Function Interframe Space
SIFS: Short Interframe Space
Die Verwendung der IFS-Zeiten wird später noch genauer erläutert.

NAV (Network Allocation Vektor)

Der NAV ist ein Timer auf MAC-Ebene der angibt, wie lange das Netzwerk voraussichtlich belegt sein wird.

DCF (Distributed Coordination Function)
Die Distributed Coordination Funktion ist ein Zugriffsmechanismus, der in einem Netzwerk ohne Manager (Ad-hoc) die Zuteilung des Funkkanals an die einzelnen Stationen (Nodes) regelt.
Um Zugriff auf den Kanal zu erhalten, testet die sendewillige Station auf Vorhandensein eines Trägers (Listen Before Talk). Ist der Kanal mindestens für die DIFS-Zeit frei, kann gesendet werden. Ist der Kanal belegt, so wird mit einem Backoff-Prozess ein Wert für den NAV bestimmt. Für diese Zeit unterbricht die Station den Übertragungsversuch. Ist der NAV abgelaufen und der Kanal mindestens für die DIFS-Zeit frei, kann gesendet werden. Andernfalls wird wieder der NAV gesetzt.

PCF (Point Coordination Funktion)
Wird das Zugriffsverfahren PCF verwendet, übernimmt ein Koordinator (z.B. ein Access-Point) die Vergabe des Kanals. Es muss allerdings gewährleistet sein, das Übertragungen von Stationen, die nach dem DCF Verfahren auf den Kanal zugreifen nicht mit Übertragungen von Stationen, die mit PCF arbeiten kollidieren.
Dazu richtet der Koordinator eine Contention Free Period (CFP - "Streitfreie Zeit") ein, die sich zeitlich mit einer Contention Period (CP - mehrere Stationen versuchen Zugriff auf den Kanal zu erhalten) abwechselt. Realisiert wird diese CFP, indem der Koordinator ein Management-Frame sendet in dessen Header ein 2Byte-Feld für alle Teilnehmer bestimmt ist. Die Teilnehmer setzen ihren NAV auf diesen Wert, so dass der Koordinator für die CFP alleinigen Zugriff auf den Kanal hat. Damit die CFP überhaupt beginnen kann, greift der Koordinator bereits nach einer PIFS-Zeit auf den Kanal zu, die innerhalb der Contention Period eine höhere Priorität hat als die DIFS. Nun wird nacheinander jedem beim Koordinator gemeldete Teilnehmer (er führt sie in einer Polling Liste) die Möglichkeit gegeben, ein Frame zu versenden. Dazu sendet der Koordinator der Station eine Poll-Frame. Nur Stationen, die ein solches Poll-Frame erhalten haben sind berechtigt, ein Daten-Frame zu senden. Diese Daten-Frames werden innerhalb der CFP nach einer SIFS-Zeit gesendet. Durch die hohe Priorität von SIFS wird der Zugriff auf den Kanal auch für den Fall gewährleistet, dass eine Station den Beginn der CFP nicht mitbekommen hat.

MAC-Retransmission (Bestätigungsmechanismen)
Weder DCF noch PCF garantieren jedoch die kollisionsfreie Übertragung. Damit höhere Protokollschichten entlastet werden, wird bereits auf MAC-Ebene mit einer Rahmenbestätigung gearbeitet. Die Ack's (Acknowledgements) werden bereits nach einer SIFS-Zeit gesendet, die den kurzen Frames eine hohe Priorität geben. Erhält der Sender keine Bestätigung, so überträgt er den Frame erneut.

RTS/CTS (Versteckte Stationen)
Solange sich alle Stationen innerhalb einer Reichweitenzone befinden, funktioniert die Kollisionsvermeidung mit den bisher beschriebenen Verfahren ganz ordentlich. Was uns jetzt aber einen Strich durch die Rechnung machen kann, ist das "Hidden Station Problem". Wie die Abbildung zeigt ist es gar nicht so unwahrscheinlich, dass es eine Station gibt, die mit zwei anderen Stationen in Kontakt steht, welche sich jedoch gegenseitig nicht erreichen können.
Was nun Probleme bereiten kann ist folgendes Szenario: Station S2 erhält Zugriff auf den Kanal und sendet an Station S1. Gleichzeitig erkennt Station S3 den Kanal als frei und sendet an S1. Das ist durchaus möglich, da ja S3 von S1 nichts mitbekommt. Da sich jedoch bei S2 die beiden Übertragungen überlagern, ist davon nichts mehr

zu gebrauchen. Nun kommt RTS/CTS zum Einsatz. "Ready To Send/Clear To Send" ist ein Handshake-Verfahren, das alle Stationen im infragekommenden Empfangsgebiet über eine bevorstehende Transmission informiert. Dazu sendet die sendewillige Station ein *Ready To Send* an den gewünschten Empfänger. Dieser antwortet, so er dem Verbindungswunsch nachkommt, mit *Clear To Send*. Der Clou an diesem Handshake ist, dass diese kurzen Frames einen NAV Wert im Header haben, der von allen nicht an dieser Übertragung beteiligten Stationen übernommen wird. Da zwischen RTS, CTS und dem Daten-Frame nur eine SIFS-Zeit liegt, kann die Übertragung dieser drei Frames unmittelbar nacheinander erfolgen. Tritt eine Kollision während des Handshakes auf, so beginnt die Übertragung des im Vergleich zu diesem Management-Frame möglicherweise viel größeren Daten-Frame erst gar nicht. Allerdings fügt das RTS/CTS Verfahren etwas mehr Overhead zur Übertragung bei, weshalb es abgeschaltet werden kann.

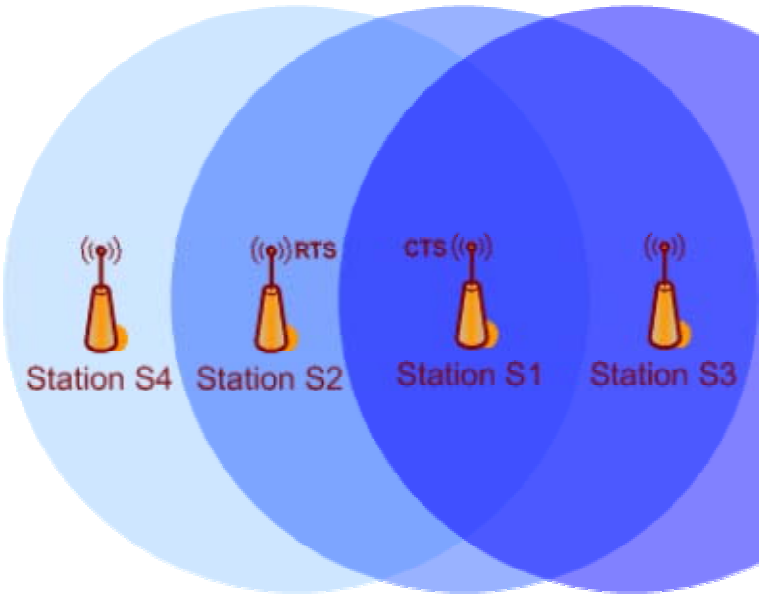

Abbildung 10 : Hidden-Station-Problem

Roaming

Da die Reichweite eines einzelnen Access Points beschränkt ist, benötigt man oft ein Netz aus mehreren Access Points, um eine ausreichende Abdeckung zu gewährleisten. Sobald sich ein Benutzer mit seinem Endgerät bewegt, muss es automatisch von einem Access Point zum anderen wechseln können. Dieser Wechsel wird Roaming genannt.

Im Gegensatz zur Verbindungsübergabe wird unter Roaming meist ein umfangreicher, komplexer Wechsel des Netzzuganges verstanden.

Ablauf des Roamings:

1	Eine Station stellt fest, dass das Signal von Access Point1 zu schwach wird und sucht einen neuen AP bei dem der Empfang besser ist (Scanning).

2	Bei der Suche wird nach aktiver und passiver Suche unterschieden. Bei einer passiven Suche (passives Scanning) hört die Station zum Finden anderer Netze in das Medium hinein. Beim aktiven Suchen (active scanning) wird eine Probe auf jedem Kanal gesendet und auf eine Antwort abgewartet. Die Antwort auf eine Probe sowie ein Beacon-Frame enthalten alle nötigen Informationen, um an einem neu gefundenen BSS teilzunehmen.
3	Nun wählt die Station den für sie besten Access Point, beispielsweise auf der empfangenen Signalstärke basierend, und sendet eine Anfrage zur Aufnahme an den gewählten Zugangspunkt.
4	Der neue Zugangspunkt antwortet mit association response. Fällt diese positive aus, war das Roaming erfolgreich. Sonst geht die Suche weiter.
5	Nimmt der neue Access Point die Station auf meldet sich diese noch bei dem alten AP ab, damit dieser noch die entsprechenden Ressourcen für weitere Stationen wieder frei geben kann.

Betriebsmodi von 802.11b

Ad-hoc

Im Ad-hoc Modus werden einfach zwei oder mehr Rechner per WLAN miteinander verbunden (Peer-to-Peer). Dieser Modus ist in letzter Zeit von den Herstellern so implementiert worden, dass die Zusammenarbeit der Karten verschiedener Hersteller problemlos funktionieren sollte.

Infrastruktur

Die zweite Betriebsart ist der Infrastruktur-Modus. Hier kümmert sich ein Access-Point (AP) um die Verwaltung des Netzwerkes. Auch stellen die meisten APs eine Bridge in ein Ethernet zur Verfügung. Mehrere APs können miteinander verbunden werden (Funk oder Ethernet) und ermöglichen damit den Aufbau eines Infrastruktur-Netzwerkes und das Roaming zwischen verschiedenen Funkzellen.

802.11-Zusatzfeatures

Neben den für MAC- und PHY-Layer beschriebenen Eigenschaften kennt IEEE 802.11 weitere Gerätemerkmale. Dazu zählen beispielsweise Synchronisation und ein Energiesparmodus.
Die Timing Synchronisation Function (TSF) dient zum Abgleichen der Systemzeit aller Stationen. Sie wird durch regelmäßiges Versenden des TSF-Zeitgebers zu den durch Target Beacon Transmission Times (TBTT) festgelegten Zeiten in einem so genannten Beacon gewährleistet. In Infrastrukturnetzen zeichnet der Access Point für dessen Aussendung verantwortlich, in Ad-hoc-Netzen teilen sich alle Stationen diese Aufgabe.
Da viele der drahtlosen Geräte mobil und somit batteriebetrieben arbeiten, sieht der Standard auch einen Energiesparmodus vor. Dessen Einsatz muss allerdings mit den anderen Stationen im Netz "abgesprochen" werden. Auch im so genannten Doze-Modus bleiben die Stationen weiter ansprechbar. Dafür sorgen spezielle Monitoring-Algorithmen, die sich im Infrastruktur- und Ad-hoc-Modus unterscheiden.

Sicherheit im Funknetz

Drahtlose Netzwerke stellen ein gewisses Sicherheitsrisiko dar. Die Ausbreitung der Funkwellen beschränkt sich ja nicht auf das Netzwerk im engeren Sinn, die Konversation kann von jedem innerhalb der Funkreichweite befindlichen IEEE 802.11-Empfänger abgehört werden. Daher sieht der Standard die Implementierung einer Reihe von Sicherheitsmerkmalen vor.

Auf der niedrigsten Ebene erfolgt die Zulassung der Teilnehmer über einen als Electronic System ID (SSID, ESSID) bezeichneten Schlüssel. Die für alle Systeme im Netz identische SSID legt der Administrator bei der Konfiguration der Clients und Access Points fest.

Daraus resultieren zwei gravierende Einschränkungen. So zeigt die SSID zwar das allgemeine Zugangsrecht des Teilnehmers an, eine eindeutige Identifikation erlaubt sie aber nicht. Zudem ist es häufig kein Problem, die SSID eines WLANs herauszufinden. Dazu trägt nicht zuletzt bei, dass die meisten Hersteller erlauben, in den Konfigurationsdateien für die SSID die Option "any" anzugeben: Dies authentisiert den Einsatz in allen Funknetzwerken.

Ein optionales Verschlüsselungsverfahren zur Erhöhung der Sicherheit ist das im Standard IEEE 802.11 definierte *Wired Equivalent Privacy (WEP)*. Im Kontrollfeld eines verschlüsselten Daten- oder Management-Frames wird das Bit WEP gesetzt und der Datenteil verschlüsselt übertragen. Zurzeit sind Schlüssellängen von 40Bit und 128Bit gebräuchlich.

Authentifizierung auf Link- und Benutzerebene

In Infrastruktur-Netzen lässt sich der Zugang zum Netz auf zugelassene Stationen beschränken. Die Identität der Endgeräte wird bei der im Rahmen des 802.11 möglichen Link Level Authentification zwischen den beteiligten Stationen ausgetauscht. Dazu muss der Administrator die MAC-Adressen der Geräte in die Zugangslisten der Access Points eintragen.

Hier bleibt jedoch ebenfalls ein gewisses Sicherheitsrisiko bestehen. Bei den meisten auf dem Markt verfügbaren Produkten lässt sich die MAC-Adresse des Rechners verändern, so dass auch hier ein missbräuchlicher Einsatz möglich erscheint. Zudem ergibt sich, zumindest in größeren Netzen, ein Problem praktischer Natur: Bislang bieten nur wenige Hersteller komfortable Werkzeuge zum Verwalten ausgedehnter WLANs an. Daher kommt in Netzen mit vielen Teilnehmern und Access Points ein erheblicher Administrationsaufwand auf den Systemverwalter zu, wenn er den Benutzern ein komfortables Roaming ermöglichen will.

Um die Authentifizierung nicht nur auf Geräteebene, sondern auch benutzerbezogen zu unterstützen, implementieren daher fast alle Hersteller inzwischen den Remote Authentification Dial-In User Service (RADIUS). Er ermöglicht die zentrale Verwaltung von Benutzeridentifikationen und Passwörtern.

Um einen effektiven Schutz zu erreichen, kann aber zwischen dem Endgerät und dem AP auch ein VPN implementiert werden. Moderne, aber auch teure, APs habe diese Option bereits enthalten.

Abbildungsverzeichnis

Abbildung 1 : Verfügbare Frequenzbereich nach IEEE 802.11 4
Abbildung 2 : Physikalische Ebenen im IEEE 802.11 Standard 6
Abbildung 3 : 802.11-PHY Layer 6
Abbildung 4 : Direct Sequence 7
Abbildung 5 : Störunterdrückung bei DSSS..... 8
Abbildung 6 : DSSS-Kanäle im 2,4 GHz Band 8
Abbildung 7 : IEEE 802.11b sieht für das ISM-Band bis zu 13 Kanäle vor. 9
Abbildung 8 : CSMA/CA 10
Abbildung 9 : Hidden-Station-Problem 12