Wireless Local Area Network nach IEEE 802.11

Ulrich Bareth, Matthias Röckl

Hauptseminar „Dienste & Infrastrukturen mobiler Systeme“
Wintersemester 03/04
Institut für Informatik
Ludwig Maximilians Universität München
{bareth,roeckl}@informatik.uni-muenchen.de

Zusammenfassung Mobilität gewinnt in der heutigen Gesellschaft zunehmend an Bedeutung. Im Bereich lokaler Vernetzung werden drahtlose Technologien eingesetzt, um diese zu realisieren. Ein Konzept wurde durch den IEEE 802.11 Standard spezifiziert. Das folgende Dokument gibt einen allgemeinen Überblick zu diesem Standard und geht dabei auf technische Details, sowie generelle Aspekte zum Thema Wireless LAN ein.

1 Allgemein

1.1 Geschichte und Entwicklung des WLAN

In der heutigen Zeit besitzt beinah jedes Unternehmen eine Vielzahl an Computern, die als Arbeitsplatzrechner, Webserver, Router, etc. fungieren. Um Interaktionen zwischen diesen Systemen zu ermöglichen, müssen die Systeme untereinander vernetzt werden. Dabei handelt es sich bei kleinen bis mittelgroßen Unternehmen im Normalfall um lokale Netze, so genannte *Local Area Networks (LANs)*. Ein LAN hat im Gegensatz zu einem *Metropolitan Area Network (MAN)* oder *Wide Area Network (WAN)* eine maximale Reichweite von wenigen hundert Metern. Die einzelnen Systeme sind dabei meist über Koaxialkabel, Twisted Pair oder Glasfaser verbunden. In manchen Fällen ist eine Verkabelung aber nicht möglich (z.B. wegen Denkmalschutz) oder unrentabel. Deshalb ist seit einigen Jahrzehnten der Datenaustausch zwischen Computersystemen über das Medium Luft ein wichtiges Thema in der Industrie und seit einigen Jahren auch in Privathaushalten. Man nennt ein derartiges drahtloses Netz auch *Wireless Local Area Network (WLAN)*.
Neben dem Nachteil der aufwändigen und teuren Verkabelung drahtgebundener Netze ist Mobilität in derartigen Netzen schwer zu realisieren. Dies ist ein weiterer Vorteil für drahtlose Netze, da das Übertragungsmedium überall und jedem zur Verfügung steht. Einzige Einschränkung sind regulatorische Restriktionen, die nur eine Nutzung spezieller Frequenzbänder ohne Lizenzen zulassen. Einen Überblick über alle möglichen Frequenzbänder ist in Abbildung 1 dargestellt. Für den WLAN-Bereich eignen sich dabei vor allem Übertragungen per Funk

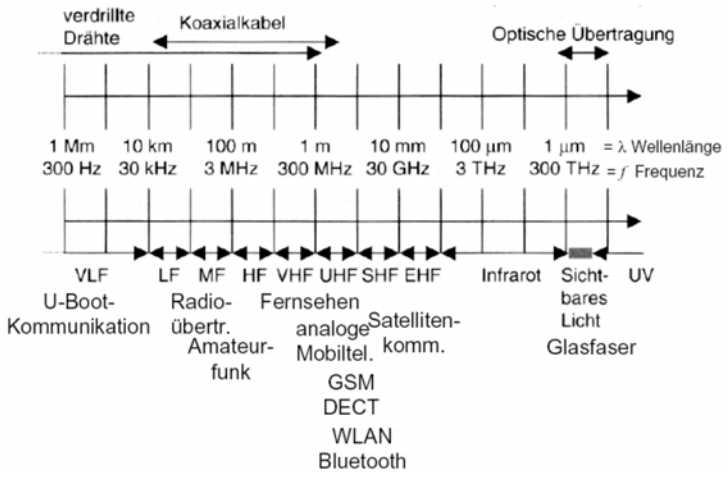

Abbildung1. Frequenzbänder (vgl. [Sch00])

oder über Lichtwellen. Meist wird jedoch die Funkübertragung bevorzugt. Für diesen Fall wurde nahezu weltweit ein Frequenzband bei 2,4 GHz reserviert, das ohne einen Lizenzerwerb genutzt werden kann. Neben WLANs nutzen dieses Frequenzband auch Mikrowellenherde oder schnurlose Telefone.
Die Entwicklung von WLANs hat viele Standards hervorgebracht, zu denen unter anderem die *IEEE 802.11* Familie, die vom *European Telecommunications Standards Institute (ETSI)* entwickelten *HIPERLAN*-Varianten oder der japanische *HiSwan* zählen. Der erstgenannte Standard, IEEE 802.11, wird in Kapitel 2 genauer betrachtet.

1.2 Heutige Anwendungsgebiete

Produkte der IEEE 802.11 Familie werden immer beliebter und oftmals schon als Alternative für leitergebundene Netze verwendet, da sie mittlerweile vergleichbare Leistungsmerkmale sowie akzeptable Preise bieten. Auch der Installationsaufwand ist gering, da das Verlegen von Kabeln entfällt.
In den Bereichen *Quality of Service (QoS))* oder Sicherheit jedoch liegen momentan noch große Defizite, was aber mit einer Ratifizierung von 802.11e und 802.11i zumindest teilweise behoben würde.
Die Reichweite liegt zwischen 10 Metern in Gebäuden, 300 Metern (auf freier Ebene), und mit Richtfunkantennen bei direkter Sichtverbindung sind sogar mehrere Kilometer möglich.
Diese Begebenheiten lassen ein breites Feld von Anwendungen erschließen:
Wireless LANs werden heutzutage immer häufiger in *Firmennetzen* eingesetzt. Es gibt viele Unternehmen, die WLAN für sich entdeckt haben, da besonders

auch die Ad-Hoc-Kommunikation große Flexibilität ermöglicht.
Auch die Zahl der *PWLAN-Hotspots (Public-WLAN-Hotspots)*, sowie deren Nutzer nimmt ständig zu wie z.B. in vielen Aufenthaltsbereichen der Universitäten, oder im Rahmen eines Pilotprojekts im Biergarten am Chinesischen Turm und im Seehaus in München, wo man für zwei Euro eine Stunde lang das Internet per WLAN nutzen kann (vgl. [uMMe]). Ebenso mit dem Verkauf von Vouchern auf denen sich ein Freischaltcode befindet, der dann eine gewisse Internet-Nutzungsdauer ermöglicht, laufen derzeit auch Pilotprojekte in den USA in einigen McDonalds-Filialen (vgl. [Cora]) und Starbucks-Filialen (vgl. [Corb]). Die Benutzung dieser Hotspots macht mindestens eine Anmeldung erforderlich und meistens muss man auch eine Nutzungsgebühr entrichten. Bei Starbucks beispielsweise kostet eine Tages-Flatrate knapp 10$.
Aber auch große Mobilfunkbetreiber wie Vodafone haben auf diesem Markt bereits Fuß gefasst und bieten Hotspots für Geschäftskunden in Flughäfen oder Hotels an, die dann bequem über die Telefonrechnung bezahlen.
Aussteller auf Messen nutzen bekannterweise gerne WLANs, um spontan Netze für ihre Besucher bereitzustellen.
Aber auch im *SOHO (Small Office, Home Office)* und im privaten Bereich hält die neue Technologie Einzug. Die meisten Komplett-Rechner werden schon mit WLAN-Karten verkauft und auch große *Internet Service Provider (ISP)* wie AOL oder T-Online bieten preiswerte Kombinationen von Access Point, integriertem DSL-Modem und Router in einem an. Die Ratifizierung des 802.11g Standards, der mittlerweile Bruttoübertragungsraten von 54 MBit/s auf dem lizenzfreien ISM-Band (2,4GHz) ermöglicht und zu 802.11b abwärts kompatibel ist, wird die Verbreitung von WLAN weiter beschleunigen.
Richtfunk WLAN-Netze können auch in strukturschwachen Regionen einen Breitband-Internetzugang bereitstellen, wie ein interessantes Beispiel aus Dänemark zeigt ([Neu03]). Auch die Netzwerkverbindung von Firmengebäuden *(last mile)* ist bei bestehender Sichtverbindung mit Richtfunkantennen über mehrere Kilometer möglich.

1.3 Wi-Fi

Der Begriff *Wi-Fi* steht für Wireless Fidelity und ist ein Standard der *WECA Organisation (Wireless Ethernet Compatibility Alliance)*, ein Zusammenschluss von über 200 Herstellern für IEEE 802.11 Geräte. Wi-Fi-zertifizierten Produkten wird die Interoperabilität zum IEEE 802.11b-Standard garantiert. Dem Anwender wird damit gewährleistet, dass er beim Aufbau und der Erweiterung seines WLANs keine Kompatibilitätsprobleme zu erwarten hat. Besonders in den USA wird „Wi-Fi“ aber auch gleichbedeutend mit IEEE 802.11 oder WLAN verwendet.

2 IEEE 802.11 Standard

2.1 Geschichte

Das *Institute of Electrical and Electronics Engineers (IEEE)* wurde 1963 gegründet, um die „Theorie und Praxis der Elektrotechnik und Informatik“ [oEEa] weiterzuentwickeln. Es besteht derzeit aus 366.000 Mitgliedern, unter anderem aus den Branchen Informatik, Biomedizin, Telekommunikation, Stromversorgung und Raumfahrt (vgl. [oEEb]).
Eine der Hauptaufgabenbereiche von IEEE ist die Standardisierung und Normierung. Ein Beispiel hierfür ist die Familie der 802.x Standards für lokale Netze, wie Ethernet (802.3) und Token Ring (802.5). Durch Standards der 802.x Familie werden die Schichten 1-2 des ISO-OSI Schichtenmodells spezifiziert. Dabei handelt es sich um die Bitübertragungsschicht (Physical Layer, PHY) und die Sicherungsschicht (Data Link Layer, DL). Der obere Teil der Sicherungsschicht, die so genannte Verbindungsabschnittssteuerungsschicht (Logical Link Control, LLC), ist hierbei für alle Standards der 802.x Familie identisch und im 802.2 Standard festgelegt. Desweiteren wurden bis heute sieben verschiedene Bitübertragungsschichten und Mediumzugriffsschichten (Medium Access Control, MAC) (unterer Teil der Sicherungsschicht) standardisiert.
Mit dem Ziel ein einfaches und robustes drahtloses LAN, das zeitbeschränkte und asynchrone Datendienste anbieten kann, zu entwerfen, begann IEEE mit der Entwicklung des IEEE 802.11 Standards. Die Geschichte des WLAN Standards IEEE 802.11 reicht bis in das Jahr 1987 zurück. Damals war er noch als Draft (untergeordnete Forschungsgruppe) mit der Bezeichnung 802.4L des übergeordneten Token Bus Standards (802.4), der sich mit der Entwicklung einer Datenübertragungstechnologie via Funk beschäfigt, bekannt. Die Idee, mit Maschinen in Fabrikhallen per Funk zu kommunizieren und diese zu steuern, weckte das Interesse der Industrie und so kam es, dass auch große Automobilkonzerne, wie z.B. General Motors, aktiv an der Entwicklung dieses Drafts beteiligt waren. 1990 erhielt die 802.4L Gruppe einen Normierungsauftrag *PAR(Project Autorisation Request)* von der IEEE, wodurch sie ein unabhängiger 802.X Standard und unter der heutigen Bezeichnung IEEE 802.11 bekannt wurde. Durch die großen technologischen und regulatorischen Unterschiede weltweit, wäre die Norm beinahe gescheitert, da spätestens nach 3 Jahren ein Draft veröffentlicht werden muss, was erst nach einer Fristverlängerung geschah.
1997, also 7 Jahre nach dem Normierungsauftrag, konnte dann endlich der erste Standard 802.11 WLAN verabschiedet werden, was allerdings immer noch nicht zur Marktreife ausreichte, da die Übertragungsraten mit maximal 2 MBit/s viel zu gering waren. Erst 2000, als die *Higher Data Rate Extensions* 802.11b und 802.11a verabschiedet wurden, kamen die ersten Produkte auf den Markt, welche Übertragungsraten bis zu 11 MBit/s bzw. 54 MBit/s ermöglichten und dem Standard letztendlich zum Durchbruch verhalfen (siehe [Ins02]).
Die folgenden Kapitel zeigen einen Überblick über den IEEE 802.11 Standard.

2.2 WLAN Topologien

2.2.1 Infrastrukturmodus

WLANs, die auf einen derartigen Modus zurückgreifen, basieren auf der Existenz einer Infrastrukturkomponente. Diese ist im Normalfall ein so genannter *Access Point (AP)*, mit dem jede beteiligte Entität, die im Kontext von WLAN *Stations (STAs)* genannt werden, direkt kommuniziert. Eine Kommunikation zwischen verschiedenen STAs ist prinzipiell nicht vorgesehen. Der AP und alle STAs, die mit dem AP logisch verbunden sind, werden als *Basic Service Set (BSS)* bezeichnet (vgl. Abbildung 2).
Ein *Extended Service Set (ESS)* liegt vor, wenn mehrere BSS über ein Verteilungssystem, ein so genanntes *Distribution System (DS)* verbunden sind, welches beispielsweise das Ethernet-Netzwerk eines Unternehmens sein kann. Ein ESS ermöglicht Roaming innerhalb des DS, also den transparenten Wechsel innerhalb eines ESS von einem BSS in ein anderes.

Vorteile des Infrastruktur-Modus:

- MAC Management Funktionen können vom AP koordiniert werden
- AP fungiert als Brücke zu anderen Netzen
- Kein Hidden Terminal Problem

Nachteile:

- AP kostet Geld
- AP muss geeignet positioniert und konfiguriert werden
- AP ist in der Regel immer online und somit Ziel von Hackern

2.2.2 Ad-hoc-Modus

In einem Ad-Hoc Netz kommunizieren die Teilnehmer eines Netzes wie in einem Peer-to-Peer Netzwerk direkt miteinander. Man spricht von einem *Independent Basic Service Set (IBSS)* (siehe 2).

Vorteile:

- Spontane Vernetzung
- Flexibilität
- wenig Konfigurationsaufwand

Nachteile:

- Höherer Verwaltungsaufwand für die STAs
- Hidden Terminal Problem
- WLANs können ungewollt entstehen
- Mit WEP muss Schlüssel jedesmal neu ausgehandelt werden

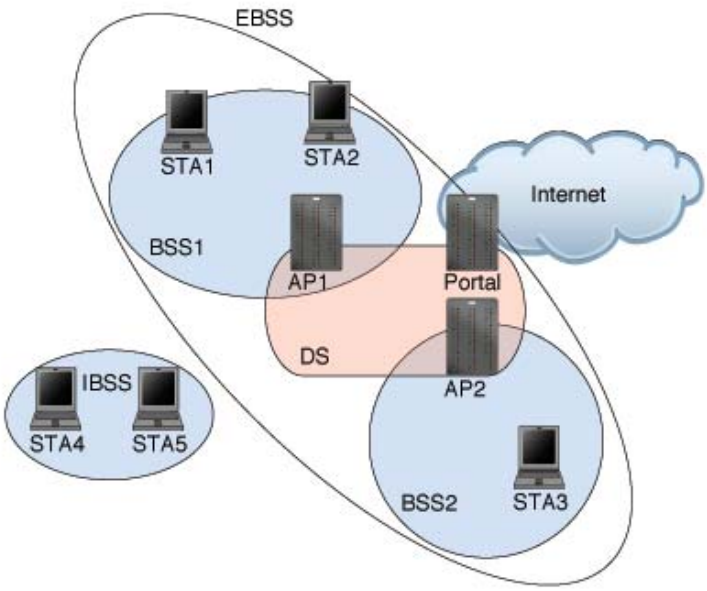

Abbildung2. Terminologie

2.3 Protokollschichten

Der IEEE 802.11 Standard spezifiziert die PHY-Schicht und die MAC-Schicht zur drahtlosen Kommunikation von stationären, portablen und mobilen Endgeräten [Insb]. Genauer betrachtet läßt sich die PHY-Schicht in die Teilschichten Physical-Medium-Dependant (PMD) und Physical-Layer-Convergence-Protocol (PLCP) unterteilen.
Im Folgenden soll nun eine detailliertere Beschreibung des Aufbaus und der Funktionsweise der MAC- und der PHY-Schicht nach dem IEEE 802.11 Standard erfolgen. Ein Überblick der Schichtenstruktur ist in Abbildung 3 gegeben.

2.3.1 MAC-Schicht

Die oberste Schicht, die durch den IEEE 802.11 Standard spezifiziert wird, ist die MAC-Schicht. Alle *Protocol Data Units (PDUs)*, die von der LLC-Schicht an die MAC-Schicht weitergereicht werden, müssen zuverlässig an die Peer-Entität übertragen werden. Dazu muss die MAC-Protokollschicht entsprechende Zugriffsmechanismen wählen. Um Management-Funktionen, wie Roaming, Power

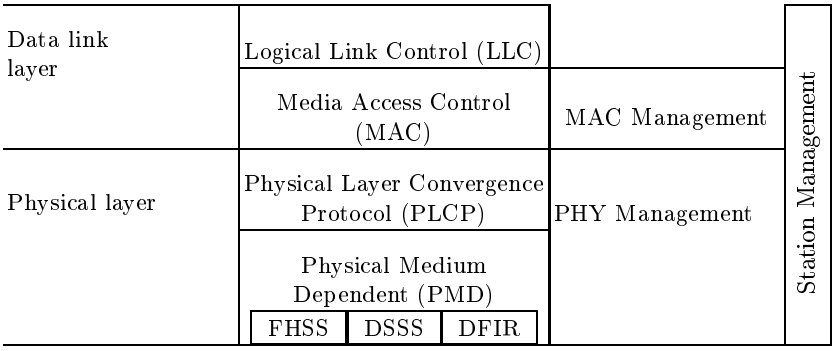

Abbildung3. Protokollebenen des IEEE 802.11 Standards

Management, etc. zu realisieren, existiert parallel zur MAC-Protokollschicht die MAC-Management-Schicht. Zunächst soll nun die MAC-Protokollschicht betrachtet werden.

2.3.1.1 MAC-Protokollschicht

Drahtlose Datenübertragung ist im Gegensatz zur drahtgebundenen Datenübertragung relativ unsicher, da die Signale durch Mehrwegausbreitung und Interferenzen durch andere WLANs, Mikrowellen, etc. gestört werden. Normalerweise wird die zuverlässige Übertragung von Nachrichten in der Transportschicht, z.B. durch TCP, sichergestellt. Da derartige Protokolle aber auf drahtgebundene Datenübertragungen ausgerichtet sind, eignen sie sich nur eingeschränkt für drahtlose Datenübertragungen. Deshalb ist es an dieser Stelle sinnvoller, die Fehlerbehandlung auf der Ebene der MAC-Schicht anzusiedeln [Sta02].
In diesem Sinne wird jede Nachricht der MAC-Schicht durch die MAC-Schicht der Peer-Entität bestätigt, d.h. der Empfänger schickt eine Quittung (Acknowledgment, ACK) an den Sender sofort nach Erhalt einer Nachricht. Erhält der Sender keine Bestätigung auf seine Nachricht innerhalb einer gewissen Zeitspanne, wiederholt er die Übertragung.
Um Daten versenden zu können, muss das Medium - in diesem Fall die Luft - frei, d.h. vorübergehend von keiner anderen Entität belegt sein. Im Gegensatz zu Medien wie Draht oder Glasfaser kann ein gleichzeitiger Zugriff mehrerer Entitäten auf das Medium (Kollisionen) bei Luftübertragung nicht allein durch Abhören erkannt werden. Das Zugriffsverfahren des IEEE 802.3 Standards (vgl. [Insa]), namens *Carrier Sense Multiple Access / Collision Detection (CSMA/CD)*, das bei Ethernet verwendet wird, ist bei einer Übertragung über die Luft nicht einsetzbar, da ein drahtloser Sender alle Signale anderer Sender in seinem nahen Umfeld überdeckt [Rot02].
Deshalb wird im IEEE 802.11 Standard ein anderes Verfahren für den Mediumzugriff verwendet. Dabei handelt es sich um *Carrier Sense Multiple Access* mit *Collision Avoidance (CSMA/CA)*. In CSMA/CA wird versucht, Kollisionen durch ein Wettbewerbsverfahren zu vermeiden. Sie können aber dennoch auftreten und werden dann durch das oben beschriebene Quittungsverfahren erkannt.

Desweiteren kann auf der Ebene der MAC-Protokollschicht optional ein Verfahren zur Lösung des Hidden Terminal Problems eingesetzt werden und ebenfalls optional ist ein zentral gesteuertes Verfahren für zeitbeschränkte Dienste. Wegen der zentralen Koordination wird dieses Verfahren auch *Point Coordination Function (PCF)* genannt. Das erste und zweite Verfahren haben im Gegensatz dazu den Namen *Distributed Coordination Function (DCF)*, da die Koordination auf jede beteiligte STA verteilt ist.
Alle drei Zugriffsverfahren zusammen sind auch als *Distributed Foundation Wireless Medium Access Control (DFWMAC)* bekannt, welches nun im Einzelnen erläutert wird.

Einfaches CSMA/CA
Das als erstes genannte Zugriffsverfahren ist einfaches CSMA/CA. Ziel dieses Verfahrens ist, den Zugriff auf das Medium, der von mehreren STAs parallel angestrebt wird, sequentiell darauf aufzuteilen. Will eine STA eine Nachricht senden, so hört sie das Medium bezüglich des *Clear-Channel-Assessment*-Signals der PHY-Schicht (vgl. [Insb]) ab. Ist das Medium für eine bestimmte Zeit, die so genannte *DCF Interframe Space (DIFS)* frei, so kann sie direkt senden. Das bedeutet, dass bei geringer Zahl sendewilliger STAs eine Datenübertragung ohne wesentliche Verzögerung stattfinden kann. Wird hingegen das Medium in dieser Zeitspanne von einer anderen STA belegt, so muss ein Wettbewerb um das Medium gestartet werden (vgl. Abbildung 4).

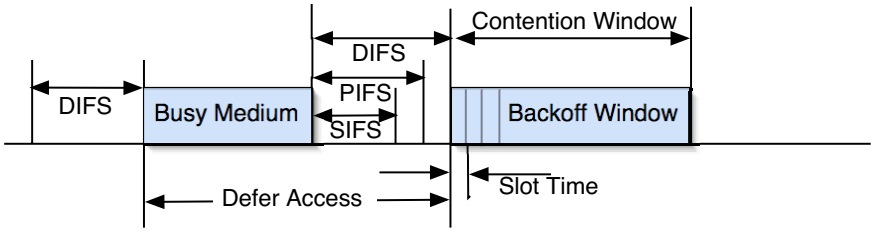

Abbildung4. Carrier Sense Multiple Access / Collision Avoidance (vgl. [Insb])

Dieser Wettbewerb besteht darin, dass jede sendewillige STA eine bestimmte Zeitspanne plus eine zufällige Wartezeit pausiert, bevor auf das Medium zugegriffen wird. Wer die kleinste zufällige Wartezeit besitzt, kann demnach als erstes auf das Medium zugreifen, alle anderen müssen warten und können erst nachdem das Medium wieder frei geworden ist, erneut den Wettbewerb starten. Um dem Problem der Starvation (unendliche Wartezeit) entgegenzuwirken, wird in der nächsten Runde des Wettbewerbs nicht erneut eine zufällige Wartezeit bestimmt, sondern mit der restlichen Wartezeit der vorigen Runde begonnen. So kann sichergestellt werden, dass jede STA nach einer gewissen Zeit auf das Medium zugreifen darf (vgl. Abbildung 5). Dieses Verfahren wird auch Backoff-

Algorithmus genannt.
Problematisch ist die maximale Größe der zufälligen Wartezeit, die Backoff-Zeit. Werden nur recht geringe Backoff-Zeiten benutzt, kann es zu vielen Kollisionen führen, da viele STAs die selbe Backoff-Zeit besitzen. Wählt man hingegen große Backoff-Zeiten, so sinkt zwar die Anzahl der Kollisionen, aber gleichzeitig auch der mittlere Durchsatz, da alle STAs lange auf den Medienzugriff warten müssen. Aufgrundessen ist im IEEE 802.11 Standard ein dynamischer Ansatz zur Berechnung der Backoff-Zeit gewählt worden. Die Backoff-Zeit wird in Vielfachen von Zeitschlitzen (Time Slots) angegeben. Die zufällige Anzahl n der Zeitschlitze darf Werte im Bereich $[0; CW]$ annehmen, wobei das Contention Window (CW) abhängig von der Häufigkeit der Fehlübertragungen generiert wird. CW wird nach folgender Formel berechnet: $CW = x^2 - 1$, mit $x \in \mathbb{N}$. Tritt ein Übertragungsfehler auf, so wird x um eins inkrementiert. Wird eine Nachricht erfolgreich übermittelt, so wird CW auf seinen kleinsten Wert zurückgesetzt. Abhängig von der PHY-Schicht gibt es untere und obere Schranken für das CW. Auch die Länge der Zeitschlitze ist abhängig von der PHY-Schicht.

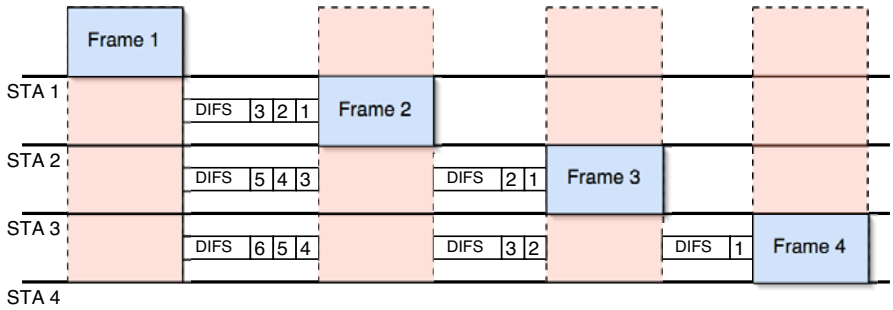

Abbildung5. Beispielkommunikation zwischen vier STA (vgl. [Rot02])

Ein Problem, das sich durch das Wettbewerbsverfahren ergibt, ist das oben angesprochene Senden von ACKs. Theoretisch müsste ein Empfänger einer Nachricht sich erst für den Zugriff auf das Medium bewerben, um eine Quittung zu senden. Möglicherweise kann dies jedoch so lange dauern, bis der ursprüngliche Sender der Nachricht denkt, dass seine Nachricht nicht korrekt übermittelt wurde. Deshalb sieht der IEEE 802.11 Standard neben DIFS eine weitere Wartezeit namens *Short Interframe Space (SIFS)* vor. SIFS ist wesentlich kürzer als DIFS (vgl. Abbildung 4). Will nun ein Empfänger einer Nachricht dem Sender eine Quittung zukommen lassen, so wartet er nur SIFS, bevor er den Sendevorgang einleitet. Folglich muss er nicht wie alle anderen sendewilligen STAs DIFS plus Backoff-Zeit warten und kann deshalb als erster auf das Medium zugreifen.
Außerdem wird SIFS bei der Versendung von fragmentierten Daten eingesetzt. Fragmentierung von Nachrichten tritt auf, wenn eine PDU der LLC-Schicht in der MAC-Schicht in mehrere kleinere PDUs, so genannte Fragmente, gesplittet

wird. Dies hat den Sinn, dass bei einer Fehlübertragung einer sehr langen Nachricht nicht die ganze Nachricht neu übertragen werden muss, sondern nur das Fragment, in dem der Fehler aufgetreten ist. Natürlich darf eine Nachricht auch nicht zu stark fragmentiert werden, da es sonst durch die Quittungen, die auf jedes Fragment folgen, zu einer ineffizienten Netzauslastung kommt.
Will eine STA nun eine lange Nachricht senden, wäre es notwendig sich für jedes Fragment um den Zugriff auf das Medium zu bewerben. Um dies zu verhindern, kann ein Sender, nachdem die Quittung auf ein Fragment eingetroffen ist, SIFS abwarten und dann direkt auf das Medium zugreifen, um das nächste Fragment zu senden. Der Empfänger muss dadurch bei hoher Netzauslastung nicht lange auf das Eintreffen der kompletten Nachricht warten. Der durch die Fragmentierung enstandene Daten-Burst kann ohne lange Unterbrechungen zügig übertragen werden (vgl. Abbildung 6).

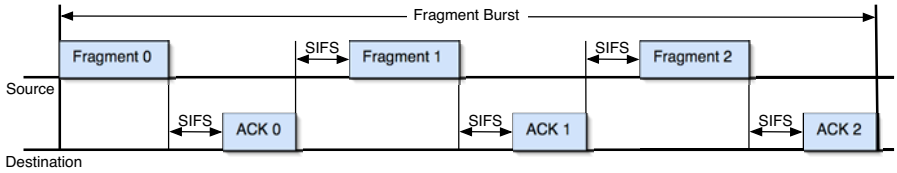

Abbildung6. Übertragung einer Nachricht in drei Fragmenten mittels CSMA/CA (vgl. [Insb])

Wie man bereits gut erkennen konnte, verbirgt sich in den unterschiedlich langen Wartezeiten die Möglichkeit, einzelnen Aktionen Prioritäten zuzuordnen. So hat das Senden von Quittungen eine höhere Priorität als das Senden einer neuen Nachricht, und das Senden von einzelnen Fragmenten einer Nachricht ebenfalls eine höhere Prioriät als das Senden einer weiteren Nachricht. Dieses Verfahren wird auch in den im Folgenden beschriebenen optionalen Erweiterungen des CSMA/CA Verfahrens angewendet.

CSMA/CA mit RTS/CTS

Ein Problem des einfachen CSMA/CA-Verfahrens ergibt die in Abbildung 7 dargestellte Konstellation. Angenommen STA 1 will eine Nachricht an STA 2 senden, gleichzeitg will allerdings auch STA 3 an STA 2 senden. Da STA 1 und STA 3 jedoch so weit voneinander entfernt sind, dass sie zwar beide in der Reichweite von STA 2 sind, sich untereinander aber nicht empfangen können, hört STA 1 nicht, wenn STA 3 sendet und STA 3 nicht, wenn STA 1 sendet. Es handelt sich dabei um das so genannte *Hidden Terminal Problem.*
Abhilfe schafft in diesem Fall ein weiteres Verfahren. Es basiert auf den zusätzlichen Nachrichten *Request-To-Send (RTS)* und *Clear-To-Send (CTS)* und ist eine optionale Erweiterung des einfachen CSMA/CA aus vorigem Kapitel.
Will eine STA eine Nachricht senden, so muss sie sich wie gewohnt darum be-

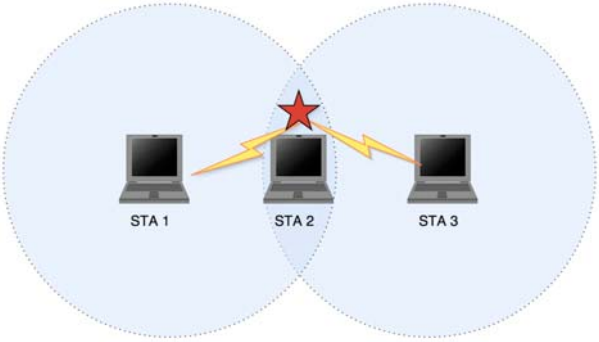

Abbildung7. Hidden Terminal Problem

werben. Bei diesem Verfahren wird aber im nächsten Schritt nicht die eigentliche Nachricht gesendet, sondern nur eine RTS-Nachricht, in der die Dauer für die Übertragung der folgenden Nachricht und ihrer Quittung vermerkt ist (vgl. Abbildung 8). Dadurch wissen alle umliegenden STAs, die in Reichweite sind und deshalb die Nachricht mithören können, dass nun eine Übertragung mit der angegebenen Dauer folgt. Sie speichern die Zeitdauer in ihrem *Net Allocation Vector (NAV)* ab. Doch die „Hidden Terminals", d.h. die STAs die nicht in Reichweite des Senders sind, jedoch in Reichweite zum Empfänger, haben noch keine Kenntnis über die bevorstehende Nachrichtenübertragung. Deshalb sendet

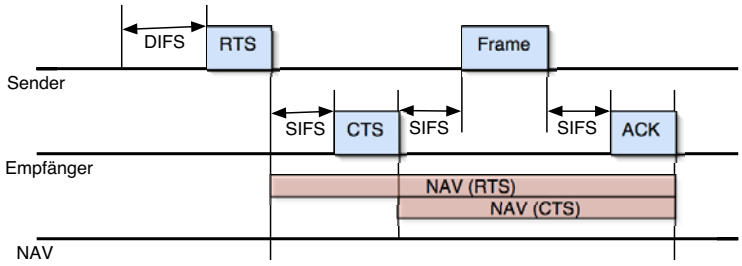

Abbildung8. Datenaustausch zweier STAs mittels CSMA/CA mit RTS/CTS

der Empfänger nach einer Wartezeit von SIFS eine CTS-Nachricht, in der ebenfalls die Dauer der noch bevorstehenden Nachrichtenübertragung enthalten ist. Natürlich ist diese im Gegensatz zur Dauer der RTS-Nachricht um die vergangene Zeit verkürzt. Nun haben alle STAs in Reichweite von Sender und Empfänger Kenntnis über die bevorstehende Nachrichtenübertragung und pausieren daraufhin die angegebene Zeitdauer. Nach einer weiteren Wartezeit von SIFS kann der Sender nun seine Nachricht senden und bei erfolgreicher Übermittlung die Quit-

tung dafür erhalten. Im Gegensatz zur physischen Reservierung, die durch den physischen Zugriff auf das Medium entsteht, nennt man die Reservierung durch Setzen des NAV-Wertes auch *virtuelle Reservierung*.

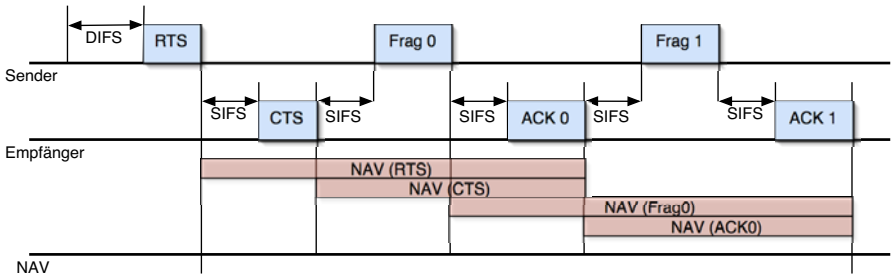

Abbildung9. Übertragung einer Nachricht in zwei Fragmenten mittels CSMA/CA mit RTS/CTS

Die Lösung des Hidden Terminal Problems bringt den Nachteil mit sich, dass ein höherer Verwaltungsaufwand nötig ist und zusätzliche Kontrollnachrichten verschickt werden müssen und so der Durchsatz an Nutzdaten sinkt. Deshalb ist es sinnvoll dieses Verfahren nur bei langen Nachrichten anzuwenden, die ähnlich zu oben beschriebener Fragmentierungstechnik aufgeteilt werden können. Dabei sendet eine STA eine RTS-Nachricht, die die Zeitdauer zum Versenden des ersten Fragments plus die Zeitdauer für die Quittung enthält (vgl. Abbildung 9). Im nächsten Schritt bestätigt der Empfänger dies mit einer entsprechende CTS-Nachricht und der Sender beginnt nach einer Wartezeit von SIFS mit der Übertragung des ersten Fragments. Damit der Sender nicht nach Erhalt der Quittung erneut eine RTS-Nachricht mit der Dauer des zweiten Fragments senden muss, besteht hier die Möglichkeit die RTS-Nachricht mit dem ersten Fragment zu kombinieren. Genauer gesagt enthält das erste Fragment ($Frag_0$) direkt die Zeitdauer für das Erreichen von ACK_0 und die Übertragung des zweiten Fragments ($Frag_1$), sowie der entsprechenden Quittung ACK_1. Um nun auch den Hidden Terminals die Zeitdauer mitzuteilen, enthält auch ACK_0 die noch verbleibende Zeitdauer, d.h. die Zeitdauer zur Übertragung von $Frag_1$ und ACK_1. ACK_0 entspricht also zusätzlich der CTS-Nachricht des Empfängers (vgl. [Sch00]).

Point Coordination Function (PCF)

Die beiden oben beschriebenen Verfahren der DCF können keine Dienstgüteparameter garantieren. Darunter versteht man zum Beispiel untere bzw. obere Schranken für die Übertragungsrate und Zugriffsverzögerung. Dies ist aber notwendig, um zeitbeschränkte Dienste, wie zum Beispiel *Voice over IP (VoIP)* oder Videokonferenzen, anbieten zu können. Aufgrunddessen besitzt der IEEE 802.11 Standard eine optionale Erweiterung des einfachen CSMA/CA, die so genannte *Point Coordination Function (PCF)*, die jedoch nur im Infrastrukturmodus ein-

gesetzt werden kann.
In der PCF wird eine STA - im Normalfall der AP - als zentrale Koordinationskomponente (*Point Coordinator*) benutzt, um ein so genanntes *Polling* durchzuführen. Polling ist ein in vielen Bereichen eingesetztes Verfahren für den verteilten Zugriff auf eine Ressource. Im Fall der PCF wird durch den Point Coordinator nach Round Robin Strategie jeder beteiligten STA das Medium der Reihe nach zugeteilt. Dadurch entsteht eine Art *Time Division Multiple Access (TDMA) mit Time Division Duplex (TDD)* (vgl. [Sch00]). Um in diesem Verfahren neben dem gleichmäßigen Zuteilen von Mediumzugriffen (symmetrischer Verkehr) auch asymmetrischen Verkehr wie bei DCF zuzulassen, wird in einer PCF-Zeitspanne (*Superframe*), eine wettbewerbsfreie Periode und eine Periode mit Wettbewerb eingesetzt (vgl. Abbildung 10).

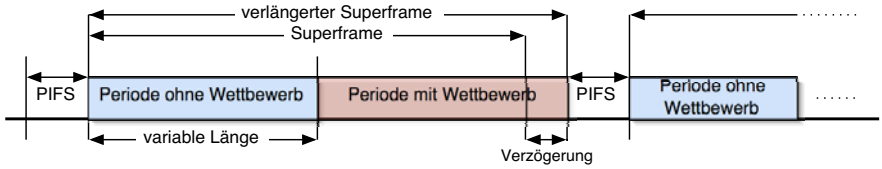

Abbildung10. Aufbau eines Superframes bei PCF

Will ein Point Coordinator zu Beginn eines Superframes eine wettbewerbsfreie Periode einleiten, muss er sich um das Medium bewerben. Jedoch gilt für ihn nicht die Wartezeit DIFS wie für alle anderen STAs, sondern nur der *PCF Interframe Space (PIFS)*. Da PIFS kleiner als DIFS ist, hat PCF eine höhere Prioriät als DCF, und der Point Coordinator kann, sobald eine Quittung auf die letzte Nachricht übertragen und PIFS gewartet wurde, die wettbewerbsfreie Periode einleiten. Das bedeutet aber auch, dass eine Periode mit Wettbewerb die wettbewerbsfreie Periode (in ihrer Position zu Beginn eines Superframes) verzögern kann, da der Point Coordinator wie gewohnt warten muss bis das Medium frei geworden ist (vgl. Abbildung 10). Andererseits ist es für den Point Coordinator aber auch möglich, gar keine Periode mit Wettbewerb zuzulassen, wenn er nach Ende einer wettbewerbsfreien Periode sofort nach einer Wartezeit von PIFS ($<$ DIFS) die nächste wettbewerbsfreie Periode einleitet. Eine Periode mit Wettbewerb wird dadurch ausgeschlossen.
Innerhalb einer wettbewerbsfreien Periode wird nun durch den Point Coordinator der ersten beteiligten STA eine Nachricht gesendet, die eine Zuteilung des Mediums enthält. Ggf. kann diese Nachricht auch Daten und/oder eine Quittung für die vorige Nachricht enthalten. Daraufhin kann diese STA nach einer Wartezeit von SIFS eine Nachricht an den Point Coordinator oder eine andere STA senden. Danach ist die Zuteilung des Mediums für diese STA beendet - auch wenn beispielsweise ein Fehler in der Übertragung aufgetreten ist - und der Point Coordinator kann nach einer weiteren Wartezeit von SIFS das Medium der nächsten STA zuteilen. Erreicht den Point Coordinator innerhalb von PIFS

(> SIFS) keine Antwort einer STA, so wird direkt die nächste STA ausgewählt (vgl. Abbildung 11).

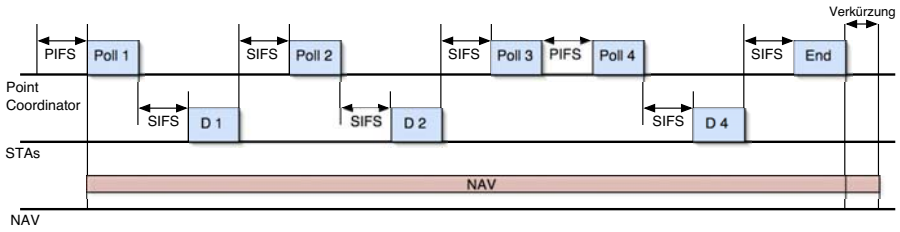

Abbildung11. Beispielkommunikation mittels PCF

Dadurch verkürzt sich natürlich die wettbewerbsfreie Periode. Deshalb wird am Ende einer wettbewerbsfreien Periode vom Point Coordinator eine zusätzliche Nachricht gesendet, die anzeigt, dass nun die wettbewerbsfreie Periode beendet ist und eine Periode mit Wettbewerb beginnen kann. Zusätzlich zu den Nachrichten, die explizit Beginn und Ende der wettbewerbsfreien Periode anzeigen, wird der koordinierte Zugriff auf das Medium durch das periodische Senden einer Nachricht, aus der das Setzen des NAV jeder beteiligten STA resultiert, unterstützt. Dadurch werden auch STAs, die die Nachrichten zu Beginn und Ende der wettbewerbsfreien Periode nicht erreicht haben, davon in Kenntnis gesetzt (vgl. [Insb]).
Zu Beginn des nächsten Superframes beginnt das Verfahren erneut.

MAC-Rahmen
Nachdem alle möglichen Zugriffsverfahren des IEEE 802.11 Standards vorgestellt wurden, soll nun der Aufbau einer PDU der MAC-Schicht, d.h. einer Nachricht, die zwischen zwei STAs auf der Ebene der MAC-Schicht ausgetauscht wird, dargestellt werden. Abbildung 12 zeigt die grundlegende Struktur eines derartigen Rahmens.
Demzufolge beinhaltet ein korrekter MAC-Rahmen ein Feld für die *Rahmensteuerung*, in dem allgemeine Informationen über den Rahmen und dessen Deutung enthalten sind. Ein weiteres Feld (*Duration ID*) mit einer Größe von zwei Byte gibt die Mikrosekunden an, für die das Medium zur Übertragung der Nachricht belegt sein wird. Die STAs setzen ihren NAV nach diesem Wert. Die folgenden Felder adressieren den Sender und Empfänger, bzw. spezifizieren sonstige Werte für das Routing. Zur Deutung dieser Adressfelder spielt jedoch der Typ des Rahmens, festgelegt durch die Rahmensteuerung, eine wesentliche Rolle. Tabelle 1 zeigt die verschiedenen Varianten. Zwischen der Adresse 3 und 4 befindet sich das *Sequence Control* Feld, das eine eindeutige Nummerierung der Fragmente einer PDU und der aufeinanderfolgenden PDUs vornimmt. Schließlich folgt der *Frame Body* mit variabler Länge (0-2312 Byte), welcher die Nutzdaten, den *Integrity Check Value* und den *Initialization Vector* (vgl. Kapitel 2.3.1.2)

	Frame Control	Durati-onID	Address 1	Address 2	Address 3	Sequ. Control	Address 4	Frame Body	FCS
Byte	2	2	6	6	6	2	6	0-2312	4
	Header							Body	

Rahmensteuerung (Frame Control): vgl. Abbildung 13
Belegungsdauer (Duration ID): NAV-Wert
Adressen 1-4: MAC-Adressen - Bedeutung abhängig von Rahmensteuerung (vgl. Abbildung 13, Tabelle 1)
Folgenummer (Sequence Control): eindeutige Identfizierung des Rahmens/Fragments
Frame Body: MAC Service Data Unit
Frame Check Sequence (FCS): 32-Bit Cyclic Redundancy Check

Abbildung12. MAC-Rahmen nach IEEE 802.11

enthält. Das letzte Feld (*Frame Check Sequence*) ist ein 32-Bit Cyclic Redundany Check (CRC), der zur Fehlererkennung für MAC Header und MAC Body dient. Als Generatorpolynom wird das Standard-Generatorpolynom für 32 Bit $G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ verwendet (vgl. [LPK03,Insb]). Eine Fehlerkorrektur ist nicht möglich. Deshalb muss bei Auftritt eines Fehlers der komplette Rahmen erneut übertragen werden.

	Prot. Vers.	Type	Sub-type	To DS	From DS	MF	RT	PM	MD	WEP	Order
Bit	2	2	4	1	1	1	1	1	1	1	1

Protocol Version: z. Z. Version 0
Type: Kontroll-, Management- oder Datenrahmen
Subtype: weiter Klassifizierung (z.B. Authentifizierungsrahmen, Datenrahmen+Quittung)
To/From DS: Adressierungsart (vgl. Tabelle 1)
More Fragments (MF): 1 wenn weitere Rahmen folgen
Retry (RT): 1 bei Übertragungswiederholung
Power Management (PM): 1 wenn übertragende STA im Sleep-Modus
More Data (MD): 1 wenn STA weitere Nachrichten (nicht Fragmente) senden möchte
Wired Equivalent Privacy (WEP): 1 wenn WEP-Protokoll benutzt wird
Order (Strictly Ordered Data): 1 wenn Reihenfolge beachtet werden muss

Abbildung13. Rahmensteuerungsfeld eines MAC-Rahmens

Die ersten zwei Byte eines MAC-Rahmens, die so genannte Rahmensteuerung, geben allgemeine Informationen über den Rahmen. Dabei handelt es sich um Informationen, wie *Protokollversion Typ* (Kontroll-, Management-, Datenrahmen), *Subtyp* (z.B. Authentifizierungsrahmen, Datenrahmen+Quittung,...) und Adressierungsart (*To/From DS*). Die Adressierungsart spezifiziert, wie die Adressen 1-4 des MAC-Frames zu deuten sind (vgl. Tabelle 1). Desweiteren wird im Feld *More Fragments* angegeben, ob weitere Fragmente folgen, und im darauf folgenden Feld (*Retry*), ob es sich um eine Übertragungswiederholung, z.B. auf-

grund eines fehlerhaft übertragenen Rahmens, handelt. Informationen den Status der STA betreffend (Doze/Awake), können in einem Bit für das *Power Management* (vgl. Kapitel 2.3.1.2) abgelegt werden. Mit dem nächsten Bit (*More Data*) wird angezeigt, ob der Sender eine weitere Nachricht senden möchte (z.B. bei PCF). Bezüglich des Sicherheitsmechanismuses (vgl. Kapitel 2.3.1.2) kann durch das Feld *Wired Equivalent Privacy (WEP)* die Art der Authentifizierung und Sicherung der Datenintegrität festgelegt werden. Wird dieses Bit auf den Wert 1 gesetzt, so wird ein Verfahren zur WEP angewendet. Das letzte Bit der Rahmensteuerung gibt an, ob die Nachrichten eine strikte Ordnung (*Strictly Ordered Data*) einhalten müssen.

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	physischer Empfänger	physischer Sender	BSSID	-
0	1	physischer Empfänger	BSSID	logischer Sender	-
1	0	BSSID	physischer Sender	logischer Empfänger	-
1	1	physischer Empfänger	physischer Sender	logischer Empfänger	logicher Sender

Tabelle1. Bedeutung der MAC-Adressen eines MAC-Frames

Eine wichtige Aufgabe der Rahmensteuerung ist die Festlegung der Adressierungsart. In diesem Zusammenhang sind Bit 9 (To DS) und 10 (From DS) der Rahmensteuerung von Bedeutung. Diese legen fest, wie die Adressen 1-4 des MAC-Rahmens interpretiert werden müssen. Es gibt die folgenden vier Varianten:

1. Sind beide Bits auf 0 gesetzt, so befindet man sich im Ad-hoc-Modus und die Adresse 1 repräsentiert den Empfänger der Nachricht und Adresse 2 den Sender. Die 3. Adresse zeigt an, in welchem BSS man sich befindet. Im Normalfall ist dies ein zufällig gewählter Identifikator dieses BSS.
2. Im zweiten Fall ist das „From BS“-Bit auf 1 gesetzt. Es handelt sich dabei um ein WLAN im Infrastrukturmodus, in dem eine Nachricht vom AP an eine STA gesendet wird. Die MAC-Adresse der STA befindet sich in der Adresse 1. In Adresse 2 wird der Identifikator des BSS (die MAC-Adresse des AP) festgehalten und in Adresse 3 befindet sich der logische Sender der Nachricht, d.h. die STA, die die Nachricht verfasst hat. Im Allgemeinen ist dies eine STA eines anderen BSS, die die Nachricht an das DS zur Weiterleitung geschickt hat.
3. Dafür muss innerhalb dieses anderen BSS die STA die Nachricht an den AP des BSSs senden. In diesem Fall wird lediglich das „To DS“-Bit gesetzt. Im Feld Adresse 1 befindet sich nun der Identifikator des BSS, in Adresse 2 die

MAC-Adresse der sendenden STA und in Adresse 3 der logische Empfänger der Nachricht, d.h. an den die Nachricht eigentlich gerichtet ist.

4. In der letzten Kombination wird das „From DS“- und das „To DS“-Bit auf 1 gesetzt. Eine derartige Nachricht wird zwischen zwei AP innerhalb eines DS versendet. Die MAC-Adresse des sendende AP steht dabei im Feld Adresse 2 und die MAC-Adresse des empfangenden AP im Feld Adresse 1. Dies sind die physischen Adressen des Senders bzw. Empfängers. Die logischen Adressen, d.h. der ursprüngliche Sender bzw. eigentliche Empfänger, werden durch das Feld Adresse 4 bzw. Adresse 3 identifiziert.

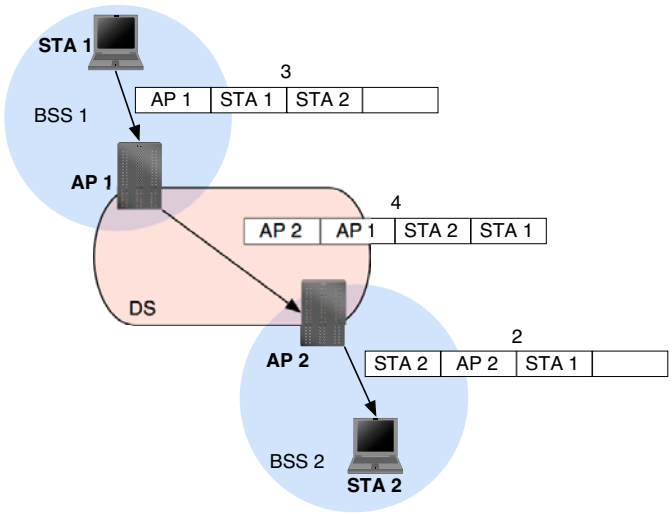

Abbildung14. Kommunikation zwischen zwei STAs in verschiedenen BSS

Sendet nun eine STA 1 eine Nachricht an eine STA 2 außerhalb ihres BSS, so sendet sie die Nachricht an den AP 1. Dieser leitet die Nachricht weiter - durch das DS - an den AP 2. Der AP 2 kann daraufhin die Nachricht an STA 2 zustellen (vgl. Abbildung 14). Durch die insgesamt vier Adressfelder muss zur Weiterleitung durch das DS kein Tunneling durchgeführt werden. Ein einfaches Kopieren der Adressen ist ausreichend.

2.3.1.2 MAC Management Sublayer

Im MAC Management Sublayer werden mehrere Funktionen implementiert, die für den Betrieb eines WLAN nötig sind, wie beispielsweise ein Mechanismus zur Synchronisation, für Power Management oder dem Roaming einer STA zwischen zwei BSSs.
Im Infrastrukturmodus übernimmt in der Regel der zuständige AP die Verwaltung dieser Funktionen. Im Ad-Hoc-Modus ist jede STA selbst für die Ausführung dieser Funktionen verantwortlich.

Synchronisation
Die *TSF (Timing Synchronization Function)*, die der Uhrensynchronisation dient, ist unter den MAC Management Funktionen besonders wichtig, da andere Funktionen wie beispielsweise der Frequenzwechsel beim FHSS, die PCF oder das Power Management auf genau synchronisierte Uhren angewiesen sind. In (quasi) periodischen Zeitabständen (etwa 100 ms) werden *Beacon Frames* (Leuchtfeuer) gesendet, die neben wichtigen Verwaltungsinformationen auch einen Zeitstempel enthalten, womit die STAs ihre internen Uhren stellen. Quasiperiodisch deshalb, da ein Beacon-Frame unter Umständen verspätet gesendet werden muss, falls das Medium zum geplanten Sendezeitpunkt *(Target Beacon Transmission Time)* besetzt ist (vgl. Abbildung 15), wobei der Zeitstempel immer den Sendezeitpunkt und nicht die geplante Sendezeit enthält. Die Intervalle, in denen die Beacon Frames gesendet werden sollen, verändern sich nicht, da die Dauer zwischen zwei aufeinanderfolgenden Target Beacon Transmission Times immer gleich ist.
Im Infrastrukturmodus übernimmt der AP die Versendung der Beacons, was den einfachen Fall darstellt.
Ad-Hoc-Netze haben keine zentrale Instanz, die den Beacon sendet, wodurch die Sache etwas komplexer gerät, da jede STA selbst für die Synchronisation zuständig ist und zur Target Beacon Transmission Time versucht, ihr Beacon zu versenden. Wenn also mehrere STAs eines Ad-Hoc-Netzes gleichzeitig versuchen, ein Leuchtfeuer zu senden, so kommt der Back-off-Mechanismus zum Einsatz. Dadurch sendet letztendlich nur eine STA den Beacon Frame und alle anderen STAs unterlassen ihre weiteren Versuche, zur aktuellen Target Beacon Transmission Time zu senden, und synchronisieren sich nach dem gerade empfangenen Beacon Frame. Im Falle einer Kollision ist das Beacon zerstört, womit alles STAs auf das nächstfolgende Leuchtfeuer warten.

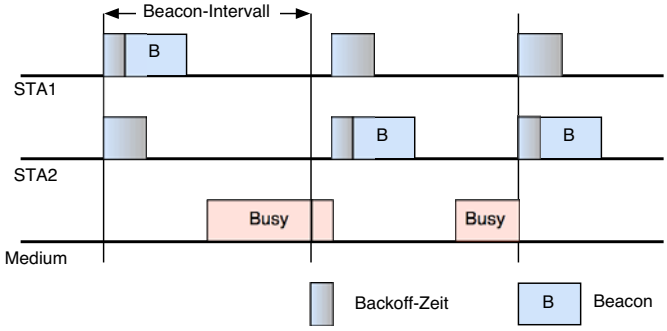

Abbildung15. Synchronisation zweier STAs im Ad-hoc-Modus

Registrierung

Bevor eine STA über einem AP kommunizieren kann, muss sie sich erst bei ihm registrieren. Dazu wertet sie die Beacon-Frames des APs aus, in denen sich unter anderem Informationen zur BSSID, zum Power Management und zum Roaming befinden, wodurch sie auch Informationen über den AP und das Netz erhält. Daraufhin sendet die STA einen *Association Request Frame* an den AP, der mit einem *Association Response Frame* antwortet. Ab jetzt ist die STA beim AP registriert und kann mit ihm kommunizieren.

Roaming
Die Bezeichnung Roaming verwendet man, wenn eine STA von einem AP zum nächsten wechselt. Dies ist nötig, wenn man sich beispielsweise in einem ESS aufhält und von einem BSS in ein anderes, mit dem ursrünglichen BSS überlappenden, BSS bewegt. Ein Roaming wird immer von einer STA initiiert und findet zwischen zwei APs statt, die jeweils ein BSS repräsentieren. Dabei geschieht Folgendes:

- STA stellt fest, dass die Empfangsstärke von AP1 zu gering ist und beginnt mit dem scanning, um weitere APs seines ESS aufzuspüren
- STA sucht sich aus allen APs denjenigen aus, dessen Signal am stärksten ist (beispielsweise AP2)
- STA schickt ein *Reassociation Request* an AP2, woraufhin dieser ihm antwortet und ihn dann bei AP1 per *IAPP (Inter-Access Point Protocol)* über das DS abmeldet

Roaming zwischen unterschiedlichen ESS muss auf höheren Schichten übernommen werden. Mobile IP ist ein solches Konzept.

Power Management
Die meisten STAs sind mobile Endgeräte, wie beispielsweise ein Notebook mit WLAN-PCMCIA-Karte, oder ein *Personal Digital Assistent (PDA)*, der ein WLAN-Modul benutzt. Da diese Geräte meist batteriebetrieben sind, muss darauf geachtet werden, wenig Energie zu verbrauchen, um eine möglichst lange Benutzung zu ermöglichen. Folglich müssen auch von WLAN-Produkten Energiesparmechanismen zur Verfügung gestellt werden. In WLANs übertragene Daten werden in Bursts gesendet und empfangen, was eine gute Voraussetzung für Power Management darstellt, weil eine STA deshalb oft ungenutzt bleibt *(idle)*. Dazu werden zwei Betriebsmodi bereitgestellt.
Im *Doze-Modus (schlafender Modus)* wird die komplette Sende- und Empfangselektronik, sofern keine Übertragungen anstehen, einfach abgeschaltet wobei die STA in periodischen Abständen wieder aufwacht um in der *Traffic Indication Map (TIM)* nachzusehen, ob eine Übertragung für sie ansteht. Die TIM ist Teil des Beacon-Frames und enthält eine Liste aller STAs, für die Pakete zwischengespeichert wurden. Begibt sich also eine STA in den Doze-Modus, so müssen alle Pakete an diese STA zwischengespeichert werden, was im Infrastrukturmodus

der AP oder im Ad-Hoc-Modus die sendenden STAs übernehmen (vgl. Abbildung 16). Der AP verwaltet die TIM zentral. Gibt es keinen AP, so verwaltet jede STA ihre eigene *Ad-Hoc TIM (ATIM)*.

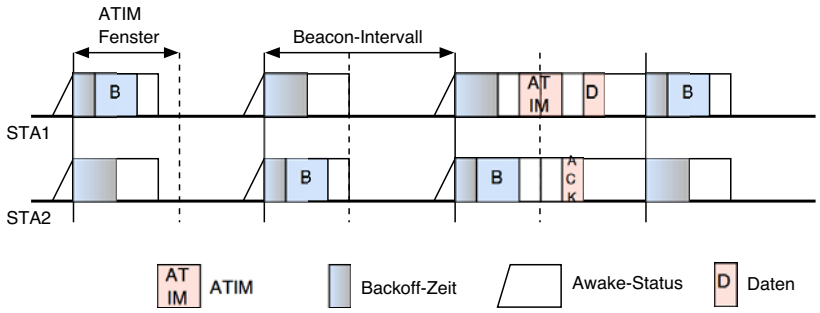

Abbildung16. Power Management im Ad-hoc-Modus

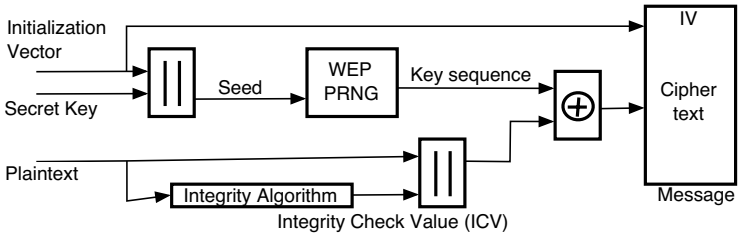

Abbildung17. Datenverschlüsselungsalgorithmus

Security

Das Thema Security ist eine der Schwächen von WLAN, weil die meisten Netz-Betreiber ihr WLAN nicht einmal verschlüsseln. Auch der am häufigsten verwendete *Wired Equivalent Privacy (WEP)*-Mechanismus, der eine 64 sowie mittlerweile auch eine 128 Bit Verschlüsselung bietet, ist mit relativ geringem Aufwand zu entschlüsseln. Zur Authentifizierung werden zwei Mechanismen angeboten: Bei der *Open System Authentication* werden nur zwei Frames, die die Identiät der STAs festlegt, gesendet. Die *Shared Key Authentication* ist ein typisches Challenge-Response-Verfahren, bei dem ein gemeinsam bekannter 40-Bit Schlüssel verwendet wird. Datenschutz wird über die WEP-Spezifikation ermöglicht. Die Ver- sowie die Entschlüsselung sind in den Abbildungen 17 und 18 dargestellt.

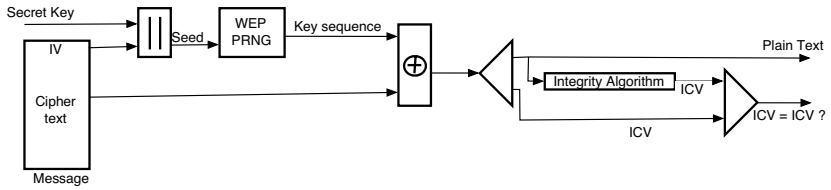

Abbildung18. Datenentschlüsselungsalgorithmus

2.3.2 PHY Layer

Entsprechend des Schichtenmodells wird der durch die MAC-Schicht entstandene MAC-Rahmen an die PHY-Schicht weitergereicht. Wie bereits erwähnt, ist die PHY-Schicht teilbar in die Physical-Layer-Convergence-Protocol- (PLCP) und die Physical-Medium-Dependant-Schicht (PMD).
Aufgabe der PLCP-Schicht ist die Bereitstellung eines einheitlichen Zugangspunktes der Bitübertragungsschicht (PHY-SAP) für die MAC-Schicht unabhängig der zugrundeliegenden PMD-Schicht. Wird durch jede PMD-Schicht bereits genügend Funktionalität bereitgestellt, ist keine PLCP-Schicht nötig.
Auf der Ebene der PMD-Schicht wird abhängig vom Bitübertragungsverfahren der PLCP-Rahmen in physische Signale gewandelt. Durch den IEEE 802.11 Standard werden drei verschiedene Bitübertragungsverfahren festgelegt. Dabei handelt es sich um *Frequency Hopping Spread Spectrum (FHSS)*, *Direct Sequence Spread Spectrum (DSSS)* und *Diffused Infrared (DFIR)*.

2.3.2.1 Frequency Hopping Spread Sprectrum

Das Bitübertragungsverfahren FHSS basiert auf der Funkübertragung im 2,4 GHz ISM-Band. Abhängig von nationalen Vorgaben über das ISM-Band sind unterschiedlich stärke Sendeleistungen zulässig. Beispielsweise lassen die USA eine Sendeleistung von 1 W EIRP (Equivalent Isotrophically Radiated Power) zu, wohingegen in Deutschland nur eine Sendeleistung bis zu 100 mW EIRP zulässig sind (vgl. [Insb]).
Um eine Überlagerung mehrerer WLANs zu realisieren, sieht IEEE 802.11 im FHSS-Verfahren eine Aufteilung des Frequenzbandes in mehrere nicht überlappende schmale Frequenzbänder vor. Die Anzahl der schmalen Frequenzbänder, welche jeweils einen Kanal repräsentieren, ist abhängig von der Breite des 2,4 GHz ISM-Bandes. In Deutschland gibt es 79 verschiedene Kanäle zwischen 2,402 GHz und 2,480 GHz mit einer Breite von 1 MHz (vgl. Abbildung 19). Mittels eines dem Sender und Empfänger bekannten, zufällig gewählten Pseudozufallszahlenverfahrens wird mindestens 2,5 mal in der Sekunde zu einer anderen Frequenz mit einem Mindestabstand von 6 MHz gewechselt. Dadurch erhält man einerseits eine gewisse Sicherheit gegen Abhören und andererseits kann die Störanfälligkeit verringert werden, da Störungen meist auf eine Menge angrenzender Frequenzbänder beschränkt sind.
Bevor es zur Modulation der Daten kommt, wird ein so genanntes *Scrambling* der *Service Data Unit (SDU)* vorgenommen, um Gleichstromanteile zu entfer-

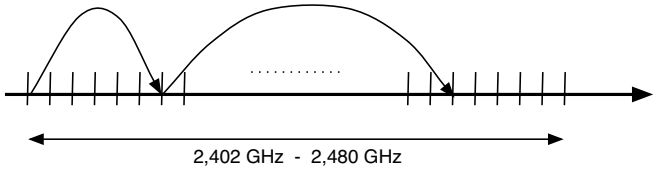

Abbildung19. Kanäle in FHSS

nen (DC blocking) und das Spektrum zu glätten (Verrauschen). Dies geschieht mittels eines linearen rückgekoppelten Schieberegisters (Linear Feedback Shift Register, LFSR) [LPK03], das mit dem Generatorpolynom $S(x) = x^7 + x^4 + 1$ und einem 127 Bit langen Wort die Daten verwürfelt. Schließlich wird eine so genannte 32/33-Kodierung durchgeführt. Dabei wird die SDU in Blöcke zu 32 Symbolen unterteilt und nach jedem Block ein *Stuff Symbol* eingefügt. Dies dient zur einfacheren Synchronisation zwischen Sender und Empfänger während der Übertragung der SDU. Die daraus resultierenden Daten werden auch als *Whitened Data* bezeichnet.
Bezüglich des FHSS-Verfahrens existieren im IEEE 802.11 Standard zwei verschiedene Modulationstechniken, die sich durch die Anzahl der übertragbaren Bits pro Symbol unterscheiden. Dabei handelt es sich um 2-Level Gauß'sche Frequenzmodulation (Gaussian Frequency Shift Keying, GFSK) und 4-Level Gauß'sche Frequenzmodulation. Die Anzahl der Level bestimmt dabei die Anzahl der verschiedenen Werte pro Symbol. Da es sich um eine Frequenzmodulation handelt werden diese Werte durch unterschiedliche Frequenzen repräsentiert (vgl. Abbildung 19). Bei 2-Level GFSK existieren demnach zwei verschiedene Frequenzen pro Symbol. Es kann also mit einem Symbol ein Bit übertragen werden. Bei 4-Level GFSK gibt es vier verschiedene Werte, und es können dadurch zwei Bit gleichzeitig pro Symbol übertragen werden. Die Übertragungsrate der Symbole liegt bei FHSS bei 1 Msps (sps = symbols per second). Folglich ist eine Datenrate von 1 MBit/s ($= 1$ Msps $\cdot 1 \frac{Bit}{Symbol}$) bei 2-Level-GFSK und 2 MBit/s ($=$ 1 Msps $\cdot 2 \frac{Bit}{Symbol}$) bei 4-Level-GFSK realisierbar. Jedoch wird auch bei 4-Level-GFSK die PLCP-Präambel (Preamble) und der PLCP-Header mit 1 MBit/s übertragen, da diese zur Synchronisation zwischen Sender und Empfänger dienen und eine optimale Synchronisation besser bei niedrigeren Datenraten erzielbar ist.
Ein PLCP-Rahmen bei FHSS besteht, wie in Abbildung 20 dargestellt, aus einer Präambel, einem Header und einer SDU. Die Präambel dient zur *Synchronisation* zwischen Sender und Empfänger und besteht aus einer alternierenden Folge von 0 und 1 der Länge 80. Darauf folgt der so genannte *Start of Frame Delimiter*, der den Anfang des Headers anzeigt. Er besteht aus der Folge 0000110010111101. Der folgende Teil des Rahmens wird als Header bezeichnet und beginnt mit der Länge der SDU in Bytes (*Packet Length Width*). Als nächstes folgt das *Packet Signaling Field*, in dem die Datenrate zur Übertragung der SDU angegeben wird. Da nur Datenraten ab 1 MBit/s und in Vielfachen von 0,5 MBit/s unterstützt

	SYNC	SFD	PLW	PSF	CRC	Whitened SDU
Bit	80	16	12	4	16	≤4095 Byte
	Preamble		Header			Daten
	Übertragungsrate: 1 MBit/s					1 - 2 MBit/s

Synchronisation (SYNC): alternierend 0,1
Start of Frame Delimiter (SFD): 0000110010111101
Packet Length Width (PLW) Länge der SDU
Packet Signaling Field (PSF): Datenrate in 0,5 MBit/s Schritten beginnend mit 1 MBit/s
Cyclic Redundancy Check (CRC): Fehlererkennung

Abbildung20. PLPC Rahmen bei FHSS

werden, ist der Wert des Feldes nur der Multiplikator bei einem festen Multiplikant von 0,5 MBit/s. Der Wert 0000 entspricht demnach einer Übertragungsrate von 1 MBit/s, der Wert 0001 der Übertragungsrate 1,5 MBit/s, usw. Das dritte und letzte Feld des Headers ist ein *Cyclic Redundancy Check*, wie er auch schon in der MAC-Schicht anzutreffen war. Der CRC-Algorithmus wird mit dem Generatorpolynom $G(x) = x^{16} + x^{12} + x^5 + 1$ durchgeführt.
Letztendlich wird die durch das Scrambling-Verfahren entstandene Whitened SDU an den PLCP Header angehängt. Die Länge dieser SDU darf 4.096 Byte nicht überschreiten. Damit ergibt sich ein Overhead durch die PLCP-Präambel (96 Bit) und den PLCP-Header (32 Bit) von 16 Byte, d.h. $\leq 3\%$ der Gesamtlänge.

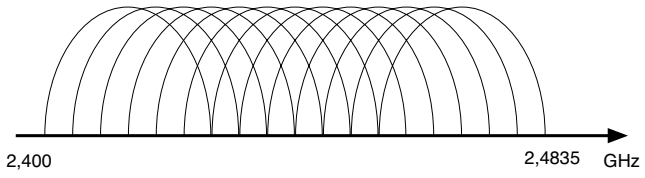

Abbildung21. Kanäle in DSSS

2.3.2.2 Direct Sequence Spread Spectrum
Ein weiteres Verfahren zur Bitübertragung ist DSSS. Anders als bei FHSS wird bei DSSS eine Datenübertragung nur auf einer Frequenz durchgeführt. Verschiedene Datenübertragungen können jedoch auch unterschiedliche Frequenzen nutzen. In Deutschland wurde dafür der Frequenzbereich 2,4-2,4835 GHz des ISM-Bandes in 13 überlappende Kanäle mit einer Bandbreite von je 22 MHz aufgeteilt (vgl. Abbildung 21). Um Interferenzen zu verhindern, gibt der IEEE 802.11 Standard einen Mindestabstand von 30 MHz zwischen den einzelnen Kanälen

überlappender oder adjazenter BSS vor, damit können drei überlappende BSSs existieren (vgl. Abbildung 22). Die Sendeleistungen bei DSSS entsprechen den Werten bei FHSS (Deutschland: 100 mW, USA: 1 W).

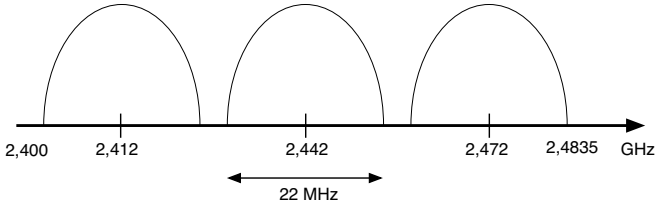

Abbildung22. Nichtüberlappende Kanäle in DSSS

Das DSSS-Verfahren basiert auf der Technik der Bandspreizung (vgl. [LPK02]). Dadurch wird eine bessere Ausnutzung des Frequenzbandes erreicht und die Störanfälligkeit für schmalbandige Störeinflüsse sinkt. Seinen Namen erhielt das Verfahren durch die direkte Abbildung des Spreizcodes auf jedes einzelne Bit. D.h. ein geschickt gewählter Spreizcode mit einer wesentlich höheren Frequenz wird mit einer XOR-Operation mit jedem einzelnen Bit addiert. Bei IEEE 802.11 wird ein 11 Chip langer Barker-Code zur Spreizung eingesetzt, da er eine gute Kreuzkorrelation aufweist. Der Barker-Code hat folgende Gestalt: $+1 - 1 + 1 + 1 - 1 + 1 + 1 + 1 - 1 - 1 - 1$. Ein Beispiel zeigt Abbildung 23.

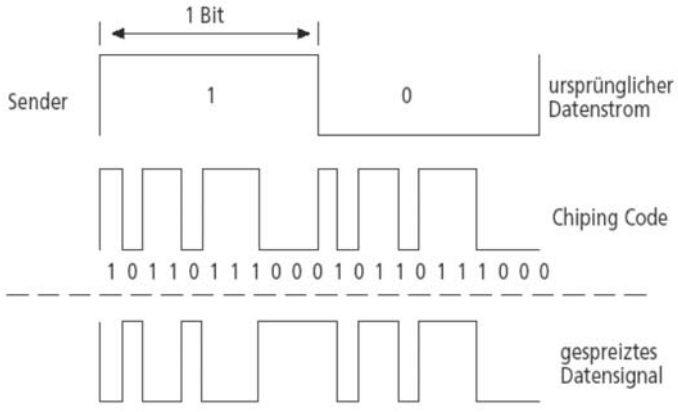

Abbildung23. Bandspreizung mit 11 Chip Barker-Code

Als Modulationsverfahren wird bei DSSS die Phasenmodulation (Phase Shift Keying, PSK) verwendet, da sie ebenfalls gut gegen äußere Störeinflüsse geeignet

ist. Bei der Übertragung machen sich Störeinflüsse meist durch eine Veränderung der Amplitude bemerkbar, im Normalfall aber nicht durch die Phase. Im IEEE 802.11 Standard sind zwei verschiedene Varianten der Phasenmodulation aufgeführt. Eine davon ist *Differential Binary PSK (DBPSK)*, das eine Datenrate von 1 MBit/s erzielt. Die zweite Variante ist *Differential Quadrature PSK (DQPSK)* und erreicht eine maximale Datenrate von 2 MBit/s.
DBPSK ist eine besondere Form des einfachen BPSK und benutzt gegenüber dem einfachen BPSK keine Referenzphase, sondern orientiert sich an der derzeitigen Phase. „Binary“ bedeutet in diesem Fall, dass nur zwei diskrete Werte unterschieden werden, bzw. ein Symbol nur ein Bit kodiert - ähnlich zu 2-Level GFSK bei FHSS. Die Kodierung zeigt Tabelle 2. Da die Symbolübertragungsrate (analog zu FHSS) bei DSSS 1 Msps beträgt, folgt daraus bei DBPSK eine Bitübertragungsrate von 1 MBit/s.

Symbol (1 Bit)	Änderung der Phasenlage
0	0
1	π

Tabelle2. Differential Binary Phase Shift Keying

Im Gegensatz zu DBSPK benutzt DQPSK zwei Bit zur Darstellung eines Symbols und erreicht dadurch eine Bitübertragungsrate von 2 MBit/s. Die Kodierung ist in Tabelle 3 ersichtlich.

Symbol (2 Bit)	Änderung der Phasenlage
00	0
01	$\frac{\pi}{2}$
10	$-\frac{\pi}{2}$
11	π

Tabelle3. Differential Quadrature Phase Shift Keying

Der PLCP-Rahmenaufbau bei DSSS besteht wie bei FHSS aus einer Synchronisationsphase zu Beginn des Rahmens mit einer Länge von 128 Bit (vgl. Abbildung 24). Dies ist wesentlich länger als bei FHSS (80 Bit), aber notwendig, da die *Synchronisation* bei DSSS schwieriger ist als bei FHSS. Darauf folgt analog zu FHSS das Feld *Start Frame Delimiter*, das den Beginn des PLCP-Headers anzeigt. Das Feld enthält die Bitfolge 1111001110100000. Das nächste Feld sind die ersten 8 Bit des PLCP-Headers, das so genannte *Signal*-Feld. Darin wird die Datenrate der MPDU als Vielfache von 100 kbps definiert. Einer Datenrate von 1 MBit/s entspricht also einem Wert von 00001010 ($10 \cdot 100$ kbps). Das *Service*-Feld des PLCP-Headers ist bis dato unbelegt. Die Zeitdauer zur Übertragung

der MPDU in Mikrosekunden wird im Feld *Length* festgelegt. Die maximale Zeitdauer zur Übertragung der MPDU entspricht also $2^{16}-1$ Mikrosekunden $\approx 0{,}07$ Sekunden. Das letzte Feld des PLCP-Headers ist ein 16-Bit *Cyclic Redundancy Check* mit dem Generatorpolynom $x^{16}+x^{12}+x^5+1$ (analog zu FHSS). Die zu übertragende MPDU befindet sich in den letzten 4095 Byte des PLCP-Rahmens.

	SYNC	SFD	Signal	Service	Length	FCS	SDU
Bit	128	16	8	8	16	16	$\leq$4095 Byte
	Preamble		Header				Daten
	Übertragungsrate: 1 MBit/s						1 - 2 MBit/s

Synchronisation (SYNC): alternierend 0,1
Start of Frame Delimiter (SFD): 1111001110100000
Signal: Datenrate in 100 kbps Schritten
Service: Reserviert für spätere Zwecke
Length: Länge der MPDU in Mikrosekunden
Frame Correction Sequence (FCS)

Abbildung24. PLPC Rahmen bei DSSS

Allgemein hat sich das DSSS-Verfahren gegenüber dem FHSS-Verfahren durchgesetzt, weil es viel robuster gegen Störeinflüsse ist und vor allem auch höhere Datenraten zuläßt (vgl. Kapitel 3.2). Ein weitere Variante der PHY-Schicht ist die Übertragung mit diffusem Licht, die im nächsten Kapitel vorgestellt wird. Diese wird aber in der Praxis überhaupt nicht eingesetzt.

2.3.2.3 Diffused Infrared

Das Bitübertragungsverfahren DFIR basiert auf der Übertragung mit Licht nahe der sichtbaren Grenze. Dazu pulsiert eine LED, die infrarotes Licht mit einer Wellenlänge zwischen 850 nm und 900 nm aussendet, mit einer Leistung von 2 Watt. Ein Impuls hat eine Länge von 250 ns und kann ein Bit übertragen. Infrarotes Licht kann wie sichtbares Licht nicht durch undurchsichtige Gegenstände, wie Wände, Möbel, etc. dringen. Deshalb ist ein BSS bei einer gebäudeinternen Nutzung an einen Raum gebunden. Daher ist einerseits keine Interferenz mit anderen BSSs möglich, andererseits ist dadurch aber für jeden einzelnen Raum eines Gebäudes ein eigenes BSS nötig. Eine Nutzung außerhalb von Gebäuden ist nur bedingt einsetzbar, da das sichtbare Licht Störeinflüsse auf infrarotes Licht bewirkt. Nur mit teuren Sende- und Empfängseinheiten wird eine verlässliche Kommunikation möglich. Innerhalb von Gebäuden ist jedoch die notwendige Hardware relativ preiswert. Ein weiterer Vorteil ist, dass das Frequenzspektrum des infraroten Lichts im Gegensatz zum ISM-Band nicht an staatliche Regulierungen gebunden ist und dadurch ohne Lizenzkosten genutzt werden kann.
Als Modulationsverfahren wird bei DFIR 16-Puls-Phasen-Modulation (PPM)

und 4-PPM eingesetzt. Als Standard gilt 16-PPM, bei dem 4-Bit lange Blöcke in 16-Bit lange Codesequenzen transformiert werden (vgl. Tabelle 4). Da man also eine 16 Bit Codesequenz benötigt um einen echten 4-Bit Block darzustellen, vergehen zur Versendung eines Blocks 250 ns $\cdot$ 16 = 4000 ns. Dies entspricht demnach einer Datenrate von $\frac{4Bit}{4000ns} = 1MBit/s$

0000	$\rightarrow$	0000000000000001
0001	$\rightarrow$	0000000000000010
0011	$\rightarrow$	0000000000000100
0010	$\rightarrow$	0000000000001000
$\vdots$	$\rightarrow$	$\vdots$
1000	$\rightarrow$	1000000000000000

Tabelle4. 16-PPM

Alternativ zu 16-PPM kann 4-PPM eingesetzt werden. Bei 4-PPM wird ein 2-Bit Block zu einer 4-Bit Codesequenz transformiert (vgl. Tabelle 5). Um demnach zwei Bits darzustellen wird eine Zeitdauer von 250 ns $\cdot$ 4 = 1000 ns benötigt. Daraus resultiert eine Datenrate von $\frac{2Bit}{1000ns} = 2MBit/s$.

00	$\rightarrow$	0001
01	$\rightarrow$	0010
10	$\rightarrow$	0100
11	$\rightarrow$	1000

Tabelle5. 4-PPM

Der Aufbau eines PLCP-Rahmens bei DFIR ist in Abbildung 25 dargestellt. Wie bei FHSS und DSSS beginnt jeder Rahmen mit einem Feld zur *Synchronisation*. Bei DFIR sind hierfür jedoch weniger alternierende Bits nötig als bei DSSS und FHSS. Die nächsten vier Bit sind reserviert für den *Start Frame Delimiter*, der bei DFIR der Bitsequenz 1001 entspricht. Als erstes Feld des Headers folgt darauf ein drei Bit langes Feld für die Datenrate (*Data Rate*). Diese kann die Werte 000 für 1 MBit/s (bei 16-PPM) und 001 für 2 MBit/s (bei 4-PPM) annehmen. Anders als bei DSSS und FHSS geben die nächsten 32 Bit bei DFIR dem Empfänger die Möglichkeit, ein so genanntes *DC Level Adjustment* durchzuführen. Dadurch kann der Empfänger Schwellwerte für die Unterscheidung von einer gesendeten 0 oder 1 setzen. Abhängig vom verwendeten Modulationsverfahrens wird die Bitfolge 0000 0000 1000 0000 0000 0000 1000 0000 bei 16-PPM oder 0010 0010 0010 0010 0010 0010 0010 0010 bei 4-PPM zur Adjustierung eingesetzt. Das nächste Feld gibt die Anzahl der Bits der zu übertragenden SDU an. Schließlich folgt wie bei FHSS und DSSS ein 16-Bit CRC mit dem Generatorpolynom $x^{16} + x^{12} + x^5 + 1$ und die zu übertragende SDU, die bei DFIR eine maximale Länge von 2500 Byte besitzen darf.

	SYNC	SFD	DataRate	DCLA	Length	FCS	SDU
Bit	57-73	4	3	32	16	16	$\leq$2.500 Byte
	Preamble		Header				Daten
	250 ns						

Synchronisation (SYNC): alternierend 0,1
Start of Frame Delimiter (SFD): 1001
Data Rate: 000 für 1 MBit/s und 001 für 2 MBit/s
DC Level Adjustments sequences (DCLA) Adjustierung der Amplitudenschwellwerte
Length: Länge der PDU
Cyclic Redundancy Check (CRC) : Fehlererkennung

Abbildung25. PLCP Rahmen bei DFIR

Aufgrund der geringen Reichweite (bis max. 20 m) und der weiteren Nachteilen wird das Modulationsverfahren DFIR in der Praxis nicht eingesetzt.

3 Übersicht zu IEEE 802.11 Standards

Da der IEEE Standard 802.11 Gegenstand aktueller Forschung ist, gibt es viele so genannter Working Groups, die beispielsweise einen Funkstandard beschreiben, sich mit der internationalen Angleichung von Funkfrequenzen, oder einer besseren *Quality of Service (QoS)* Implementierung auseinandersetzen. Dadurch entsteht ein komplexes Gefüge von Substandards, wofür die nachfolgende Aufzählung einen Überblick über den momentanen Stand der Dinge geben soll:

3.1 IEEE 802.11 - 1997

- Erster allgemeiner Standard für lokale drahtlose Netze
- Status: 1997 abgeschlossen
- Definition eines gemeinsamen MAC-Protokolls
- Definition gemeinsamer physischer Übertragungsverfahren: DSSS, FHSS, DFIR
- Frequenz: 2,4 -2,48 GHz ISM
- Übertragungsraten: 1 & 2 MBit/s

3.2 IEEE 802.11a - High data rate extension in the 5 GHz band

- hohe Übertragungsraten im 5-GHz-Frequenzband
- Status: 1999 abgeschlossen
- Frequenz: 5 GHz
- Übertragungsraten: bis zu 54 MBit/s
- Modulationsverfahren: OFDM

3.3 IEEE 802.11b - Higher data rate extension in the 2.45 GHz band

- Weiterentwicklung von 802.11-1997
- Status: 1999 abgeschlossen
- Frequenz: 2,4 GHz
- Übertragungsraten: bis zu 11 MBit/s
- Modulationsverfahren: DSSS (1 und 2 MBit/s), CKK(5,5 und 11 MBit/s)

3.4 IEEE 802.11c - Supplement to Bridge Standard

- Verbindung von Subnetzen protokollmäßig auf OSI-Schicht 2
- Status: 1998 abgeschlossen

3.5 IEEE 802.11d - Update of regulatory domains

- Untersuchung von Regulierungsvorgaben in Nordamerika und Europa
- Status: 2001 abgeschlossen

3.6 IEEE 802.11e - MAC Enhancements for Quality of Service

- Einführung verbesserter QoS-Mechanismen
- Status: aktiv
- *Hybrid Coordination Function (HC)*
- *Enhanced Distributed Coordination Funktion (EDCF)*

3.7 IEEE 802.11f - IAPP Inter Access Point Protocol

- Definition eines *Inter Access Point Protocol (IAPP)*
- Status: 2003 abgeschlossen
- ermöglicht Interoperabilität zwischen APs unterschiedlicher Hersteller
- wichtig für Roaming

3.8 IEEE 802.11g - Higher Rate Extension to 802.11b

- Erhöhung der Datenraten auf 54 MBit/s im 2,4-GHz-Band
- Status: 2003 abgeschlossen
- Frequenz: 2,4 GHz
- Übertragunsraten: bis zu 54 MBit/s
- Modulationsverfahren: DSSS (1 und 2 MBit/s), CCK (5,5 und 11 MBit/s), OFDM (6, 12, 18, 24, 36, 48, 54 MBit/s)
- Abwärtskompatibel zu 802.11b

3.9 IEEE 802.11h - SMa - Spectrum Managed 802.11a

- Ergänzungsstandard zur Regulierung der Signalstärke und für dynamische Frequenzwahl
- Status: 2003 abgeschlossen
- Frequenz: 5 GHz
- *Transmission Power Control (TPC)* reduziert die Sendestärke auf ein Minimum
- *Dynamic Frequency Selection (DFS)* wechselt automatisch die Frequenz, sobald es zu Überschneidungen mit anderen Funksignalen (z.B. Radar) kommt

3.10 IEEE 802.11i - MAC Enhancements for Security

- Verbesserung des Datenschutzes und der Zugangskontrolle
- Status: aktiv
- Verlängerung des Initialisierungsvektors von 24 Bit auf 128 Bit

3.11 IEEE 802.11j - 4.9 GHz - 5 GHz Operation in Japan

- Einführung des 5-GHz-Standards in Japan
- Status: aktiv
- Regulierungsbehörden in Japan sollen 5-GHz-Frequenzen für 802.11 freigeben

3.12 IEEE 802.11k - Radio Resource Measurement of Wireless LANs

- Radio Resource Management für höhere Protokollschichten
- Status: aktiv
- Auslastung von WLANs messen und geeignete Reaktionen ermöglichen

3.13 IEEE 802.11m - Maintenance PAR

- Verwaltung von Korrekturen im 802.11-1997 Standard
- Status: aktiv
- Spezifikationen von 802.11 sollen auf den neuesten Stand gebracht werden
- aus 802.11-1997 wird 802.11-2004?

3.14 IEEE 802.11n - High Throughput

- Übertragungsraten sollen erhöht werden
- Status: noch kein Normierungsauftrag vorhanden
- Entwurf sieht Übertragungsraten bis zu 320 MBit/s vor

4 Die Zukunft von IEEE 802.11

4.1 Schwächen von WLAN

In naher Zukunft müssen auf jeden Fall die Schwächen der Technologie eliminiert werden, auch um den Vorsprung vor den Konkurrenten HIPERLAN und HiSwan auszubauen. Bemühungen dazu finden sich in den Working Groups 802.11e, bei denen die QoS von einer *Hybrid Coordination Function (HCF)* und der *Enhanced Distributed Coordination Fuction (EDCF)* realisiert werden soll, und in 802.11i, bei dem an einem *Extensible Authentication Protocol (EAP)* und einer alternativen Verschlüsselung zu WEP gearbeitet wird. Ebenfalls werden mit Standards wie 802.11n die Übertragungsraten weiter ansteigen, was jedoch noch noch einige Jahre auf sich warten lassen dürfte.

4.2 WLAN und UMTS 3G

Mittelfristig wird sich zeigen, wie WLAN zu UMTS (3G) stehen wird. Eine Vision von Uwe Scheffel (vgl. [Sch]) beschreibt ein Szenario, in dem WLAN als direkte Konkurrenz den UMTS-Breitband-Datendiensten mit kommerziellen Hotspots den Rang abläuft. Durch den Kauf der UMTS-Lizenzen und die weitaus höheren Investitionen in der Infrastruktur wird UMTS nicht in der Lage sein, auf diesem Markt konkurrenzfähige Preise zu anzubieten.

Literatur

[Cora] McDonalds Corporation. http://www.mcdwireless.com.

[Corb] Starbucks Corporation. http://www.starbucks.com.

[Insa] Institute of Electrical and Electronics Engineers. *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.* Standard 802.3.

[Insb] Institute of Electrical and Electronics Engineers. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* Standard 802.11.

[Ins02] Institute of Electrical and Electronics Engineers. *73. Tagung der IEEE Projektgruppe 802, LMSC, Wireless PANs, LANs und MANs*, Vancouver, Juli 2002.

[LPK02] C. Linnhoff-Popien and A. Küpper. Mobilkommunikation I, 2002.

[LPK03] C. Linnhoff-Popien and A. Küpper. Mobilkommunikation II, 2003.

[Neu03] Jürgen Neumann, September 2003. http://freifunk.net/artikel/magazin/01_Djursland_jpn.

[oEEa] Institute of Electrical and Electronics Engineers. http://www.lkn.ei.tum.de/ieee/.

[oEEb] Institute of Electrical and Electronics Engineers. http://ieee.org.

[Rot02] Jörg Roth. *Mobile Computing - Grundlagen, Technik, Konzepte.* dpunkt.verlag, 1 edition, 2002.

[Sch] Uwe Scheffel. http://www.de.tomshardware.com/business/20030502/idf_berlin-04.html.

[Sch00] Jochen H. Schiller. *Mobilkommunikation.* Addison-Wesley, 2000.

[Sta02] William Stallings. *Wireless Communications and Networks.* Prentice Hall, 2002.

[uMMe] FIWM Förderkreis IT und Medienwirtschaft München e.V. http://www.e-garten.net.