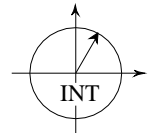


UNIVERSITÄT KARLSRUHE  
INSTITUT FÜR NACHRICHTENTECHNIK  
Prof. Dr.rer.nat. Friedrich Jondral



# **Erweiterung des IEEE 802.11 Standards für den Einsatz in Spectrum Pooling Systemen**

Diplomarbeit von

**Albert Krohn**

Hauptreferent : Prof. Dr.rer.nat. Friedrich Jondral  
Betreuer : Dipl.-Ing. Timo Weiss

Beginn : 13.03.2002  
Abgabe : 13.09.2002



# Inhaltsverzeichnis

1	Einleitung	1
2	Spectrum Pooling	3
2.1	Spectrum Pooling als anonyme Koexistenz . . . . .	4
2.2	Technische Eigenschaften von Pools . . . . .	4
3	Der Standard IEEE802.11	7
3.1	Begriffe und Architektur . . . . .	7
3.2	MAC - Dienste . . . . .	9
3.2.1	Rahmen und Adressierung . . . . .	10
3.2.2	Authentifizierung und Verschlüsselung . . . . .	12
3.2.3	Zugriffsverfahren . . . . .	12
3.3	MAC-Management . . . . .	17
3.3.1	Synchronisation . . . . .	17
3.3.2	Energiemanagement . . . . .	18
3.3.3	Assoziation, Dissoziation und Roaming . . . . .	19
3.4	Physikalische Schichten . . . . .	19
3.5	802.11a - OFDM-PHY-Schicht . . . . .	20
3.5.1	Datenraten, Parameter . . . . .	21
3.5.2	Rahmen . . . . .	21
3.5.3	Präambeln . . . . .	22
3.5.4	Kommunikationsablauf . . . . .	23
3.6	Die 802.11 Familie . . . . .	24
4	Modifikation von 802.11a für Spectrum Pooling	25
4.1	Detektion und Information . . . . .	27
4.1.1	Boosting . . . . .	31
4.1.2	Broadcast mit dem Zeit-Frequenzverfahren . . . . .	34
4.2	Synchronisation . . . . .	38
4.2.1	Grobe Frequenzsynchronisation . . . . .	40
4.2.2	Rahmen- und genaue Frequenzsynchronisation . . . . .	41
4.2.3	Kreuz- und Autokorrelation in der Anwendung für Präambeln . . . . .	46
4.2.4	Master-Synchronisation . . . . .	53
4.2.5	Vergleich des Rechenaufwandes von Auto- und Kreuzkorrelation . . . . .	53

## *Inhaltsverzeichnis*

4.3	Ergebnisse des Präambeldesigns für Spectrum Pooling . . . . .	54
4.4	FDMA - OFDM - Nebeneffekte . . . . .	56
4.4.1	Nebeneffekte zum Nachteil der Mietnutzer . . . . .	56
4.4.2	Nebeneffekte zum Nachteil der Stammnutzer . . . . .	61
4.5	Weitere Modifikationen auf der physikalischen Schicht . . . . .	62
4.6	Ergebnisse und Zusammenfassung für das Systemdesign . . . . .	64
4.6.1	PHY-Schicht . . . . .	65
4.6.2	MAC-Schicht . . . . .	65
4.6.3	Ungünstige Sonderfälle . . . . .	67
5	Abschliessende Bemerkungen und Zukunft von Spectrum Pooling	69
5.1	Zukünftige Einsatzgebiete für Spectrum Pooling . . . . .	70



## *Inhaltsverzeichnis*

# 1 Einleitung

Betrachtet man das elektromagnetische Spektrum als ein Allgemeingut, so stellt sich die Frage, ob es volkswirtschaftlich sinnvoll und gerecht ist, dass die Bundesregierung ihre Haushaltslöcher kurzfristig mit dem Verkauf von Frequenznutzungslizenzen saniert. Der Staat bereichert sich am Verkauf, anstatt dieses Gut frei zur Verfügung zu stellen. Im August 2000 wurden nach über 150 Auktionsrunden 145 MHz Bandbreite an 6 Wettbewerber für ca. 99 Mrd. DM verkauft. Die Unternehmen, die diese immensen Summen aufbrachten, sind natürlich auch große Steuerzahler. Durch die Abschreibung der Lizenzinvestitionen kommen große Steuerausfälle auf zukünftige Regierungen zu. Die Käufer der Lizenzen, die für 20 Jahre gültig sind, tragen auch noch weitere Kosten: Neben Investitionen für die Technologie und Infrastruktur wurde ihnen noch eine Versorgungspflicht mitgereicht, die aussagt, dass bis Ende 2005 50% aller Bürger mit UMTS-Netz versorgt sein sollen. Dass Lizenzen für Bandbreite nicht teuer sein müssen, zeigen die vergleichbaren Versteigerungen in Österreich (1,7 Mrd DM insgesamt) oder der Schweiz (<1Mrd. DM), Portugal (<1Mrd. DM), den Niederlanden, Schweden (gar keine Versteigerung, sondern Vergabe). Mobilfunkanbieter aus diesen Ländern können aufgrund ihrer „geringen“ Investition im eigenen Land auch noch international bei Auktionen mitbieten. Der Besitz der Lizenz bringt noch weitere Unsicherheiten mit sich. Die wissenschaftlichen Erkenntnisse bezüglich der Strahlenbelastung durch Mobilkommunikation stecken noch in den Kinderschuhen. Die Risiken und Gesundheitsschäden sind bisher weder statistisch erfasst (besonders mangels Landzeitstudien), noch verstanden. Daher ist es durchaus denkbar, dass zukünftige Gesetze die erlaubte Strahlenbelastung deutlich gegenüber dem heutigen Wert einschränken. Das würde die Investoren im Mobilfunkbereich schmerzhaft treffen.

Nach der Präsentation von UMTS-Handys auf der CeBit 2002 werden nun die ersten Geräte kommerziell zum Einsatz kommen. Ob sich die erwähnten Investitionen amortisieren oder nicht, wird jedes Unternehmen für sich selbst erfahren. Sicher ist jedoch, dass die Geldmittel, die für die Versteigerung der Lizenzen erzielt wurden, volkswirtschaftlich auch sinnvoller hätten eingesetzt werden können. So wäre z.B. die feindliche Übernahme von Mannesmann durch den britischen Konzern Vodafone zu verhindern gewesen.

Für die Mitbewerber und Zuschauer dieser einzigartigen Auktion hat sich vor allem eines heraus kristallisiert: Wer im Wettbewerb und Konkurrenzkampf der mobilen Telekommunikation bestehen will, muss über gewaltiges Investitionspotential verfügen. Kleinen Anbietern wird von vornherein der Zugang versperrt. Es stellt sich auch hier die Frage, ob diese Monopolisierung -besonders für den Kunden- wünschenswert ist. Schon im Jahre 1995 hat sich Noam [NOA95] für den *Open Spectrum Access (OSA)* ausgesprochen. Seine Vorstellung war, dass jeder Bandbreite durch Mietung bekommen kann, der sie gerade benötigt. Selbstverständlich haben auch

## 1 Einleitung

hier wichtige Institutionen für das Allgemeinwohl wie Rettungsdienste, Polizei und Militär, Vorrang. Durch die flexible Vermietung würde sich vor allem der Markt auch für diejenigen Anbieter öffnen, die nicht über ein Startkapital von mehreren Mrd. DM verfügen, wie es für UMTS nötig war. Ausserdem wird das sowieso beschränkte Spektrum auch effizienter genutzt. Brach liegende Bänder würden nicht durch die starre Vergabe von Lizenzen blockiert. Um diesem Idealfall der Nutzung entgegenzustreben, kommt *Spectrum Pooling* zum Einsatz. Die Idee ist, dass Besitzer von Spektrum dieses kurzfristig vermieten, falls sie es selber gerade nicht brauchen. So würde man der Open Spectrum Access-Idee näher kommen und könnte von den Vorteilen der diversifizierten Nutzung profitieren.

## 2 Spectrum Pooling

Der Begriff *Spectrum Pooling* wurde von Joseph Mitola [MIT99] geprägt und in Zusammenhang mit *Cognitive Radio* gesehen. Nach seiner Vorstellung bedeutet Spectrum Pooling das Zusammenfassen von Frequenzbereichen zu *Pools*, um diese dann neben ihrer normalen Nutzung zusätzlich an neuartige Nutzer zu vermieten. Ausgehend von der Feststellung, dass das Spektrum sehr ineffizient genutzt ist, sucht man nach Möglichkeiten, wie man die Nutzung ausweiten kann. Mitola schlägt vor, dass die Besitzer von Spektralbereichen (*Stammnutzer*) diese an *Mietnutzer* vermieten, wenn sie sie selbst nicht nutzen. Es ergeben sich daraus für beide Parteien vielfältige Vorteile:

- Es existiert insgesamt wesentlich mehr genutzte Bandbreite als vorher
- Das Spektrum wird effizienter genutzt
- Die Stammnutzer haben eine zusätzliche Einnahmequelle
- Es kann flexibel auf Spitzenlasten (Mittagszeit, Bahnhöfe etc.) reagiert werden
- Es ist keine neue Vergabe der Frequenzen (wie im OSA-Konzept) nötig
- Es sind keine gewaltigen Investitionen nötig, um auf Bandbreite zuzugreifen

Um Spectrum Pooling zu nutzen werden neuartige Mobilgeräte mit zusätzlicher Funktionalität benötigt. Ein Pool kann nur dann effizient genutzt werden, wenn die Mietnutzer in der Lage sind, über einen weiten Frequenzbereich zu operieren. Der RF-Teil der Geräte muss also sehr breitbandig sein. Eine ausführliche Diskussion über Sender- und Empfängerstruktur ist in [TAS01, S.15ff] zu finden.

Weiterhin muss ein Mobilgerät für Spectrum Pooling sehr schnell auf frei werdende Ressourcen reagieren. Die Vergabe von freier Bandbreite und die Aushandlung des Preises muss also von einem Computer übernommen werden. Der Nutzer kann nur noch Direktiven (z.B. maximaler Preis, der gezahlt werden soll) bei der Auswahl von Kanälen vorgeben. Mitola bezieht auch kognitive Aspekte für die Auswahl von freien Kanälen mit ein. So würde ein Mobilgerät z.B. aus selbst erzeugten Kontexten zu einem gewissen Grad in der Lage sein, die Eigenschaften der benötigten Übertragung zu beurteilen. Das wäre eine erhebliche Erleichterung für den Nutzer und würde die Dienstqualitäten durch differenziertere Auswahl verbessern.

Um Spectrum Pooling zu realisieren, ist vor allem ein neuartiges Protokoll nötig, das den Zugriff auf die Ressourcen steuert. Mitola bezeichnet dieses als *Radio Etiquette Protocol* [MIT99, S.3]. Dieses Protokoll muss vor allem eines garantieren: Dem Stammnutzer muss uneingeschränkte Priorität gelassen werden. Der Stammnutzer würde mit einer Inband-Signalisierung darüber informieren, dass gerade Bandbreite verfügbar ist, und die Mietnutzer könnten nach automatischer Aushandlung des Mietvertrags dieses Spektrum nutzen. Mitola schlägt die Inband-Signalisierung

## 2 Spectrum Pooling

vor, um damit auch gleich die Bandbereiche und Übertragung (implizit) mitzuteilen. Der Nachteil ist allerdings, dass potentielle Mietnutzer zuvor über alle denkbaren Kanäle und Übertragungverfahren informiert sein müssen und sämtliche Kanäle abhören müssten. Sollte der Stammnutzer seine Ressource benötigen, bevor die Vergabe an den Mietnutzer planmäßig abgelaufen ist, muß er trotzdem diesen Vorzug erhalten. Um Spectrum Pooling für den Einsatz interessanter zu machen, soll nun der ursprüngliche Gedanke von Mitola weitergeführt werden:

### 2.1 Spectrum Pooling als anonyme Koexistenz

In dieser Arbeit soll Spectrum Pooling als eine Koexistenz von zwei verschiedenen Zugriffsverfahren (von Stamm- und Mietnutzer) verstanden werden, wobei der Stammnutzer *keine* Kommunikation mit dem Mietnutzer durchführt. Das heißt, dass der Mietnutzer selbständig entscheidet, welche Bereiche (Zeit, Frequenz) des Pools frei sind und sie bei Bedarf eigenständig belegt und wieder frei gibt. Hier ist die Priorisierung der Stammnutzer von noch größerer Bedeutung, denn sie sind über eine fremde Nutzung ihrer Ressource weder informiert noch von Protokollseite her darauf eingestellt. Ein solches System hat den Vorteil, dass es sofort einsatzfähig ist und keinerlei Investitionen auf Seiten der Stammnutzer nötig sind. Das erhöht die Akzeptanz der momentanen Eigentümer der interessanten Spektralbereiche. So kann Spectrum Pooling aus dieser Sicht einen nahtlosen Übergang zum Open Spectrum Access liefern und moderne Anforderungen an Bandbreite und Flexibilität befriedigen.

Die Pools unterscheiden sich vor allem in Lage im Frequenzband und dem Multiplexverfahren der Stammnutzer. Zunächst sollen die technischen Unterschiede und Voraussetzungen für Spectrum Pooling herausgestellt werden, um Pools nach ihren Eigenschaften bewerten zu können.

### 2.2 Technische Eigenschaften von Pools

Verschiedene Multiplexverfahren seitens der Stammnutzer und ihre Eignung für Spectrum Pooling:

**TDM** Stammnutzer, die ihre Ressource mit einem Zeitmultiplexverfahren vergeben, sind nur eingeschränkt für Spectrum Pooling geeignet. Es ist hier danach auszuwählen, wie schmal die Zeitschlitze sind und ob Carrier Sense-Mechanismen im Protokoll der Stammnutzer existieren. Sollten die Stammnutzer sehr schnelle Zugriffswchsel und kurze Zeitschlitze nutzen, so wird es dem Mietnutzersystem sehr schwer fallen, dies stets schnell zu registrieren und darauf zu reagieren.

**FDM** Ein Pool, in dem die Bandbreite in Frequenzkanäle aufgeteilt wird, ist ideal für Spectrum Pooling. Die nicht genutzten Kanäle können von den Mietnutzern belegt werden.

**CDM** Bandspreiztechniken jeder Art (DSSS, FH) sind für Spectrum Pooling kritisch. Sollte das Stammnutzersystem DSSS verwenden, so ist eine Erkennung der Stammnutzer sehr schwierig. Es müssten aus den bestehenden, überlagerten Sendungen die Chip-Kombinationen herausgefunden werden, die noch nicht verwendet sind. FH-Systeme sind nur

dann geeignet, wenn der Trägerwechsel sehr langsam (einige  $ms$ ) geschieht. Da so langsame hops kaum verwendet werden, müssen FH-Systeme wohl auch ausgeschlossen werden. **SDM** Örtlich getrennte Funkssysteme sind für den Einsatz von Spectrum Pooling geeignet. Denkt man z.B. an Richtfunkssysteme, so werden die Frequenzbänder räumlich hauptsächlich dort belegt, wo die Hauptkeulen der Antennen verlaufen. Ausserhalb dieses Bereiches wären die entsprechenden Frequenzbereiche des Stammmnutzersystems für die Mietnutzer verwendbar. Hier muss besonders auf Sende- und Empfangsleistung geachtet werden. Auch ist die klare lokale Beschränktheit der Nutzung dieser Frequenzen ein Faktor im Systementwurf.

Es lässt sich auf jeden Fall sagen, dass es prinzipiell *nicht* vermieden werden kann, dass es zu Kollisionen (wenn auch sehr kurzen) zwischen Stammmutzern und Mietnutzern kommt. Die einzige Lösung wäre, die Signalisierung der Ressourcensteuerung des Stammmnutzersystems zu interpretieren, was einen erheblichen Aufwand bedeutet und meist aus Mangel an Informationen über das Modulationsverfahren etc. sowieso nicht möglich ist. Die maximale erlaubte Kollisionszeit muss also aus dem Stammmnutzersystem heraus ermittelt werden und durch das Zugriffsverfahren der Mietnutzer garantiert werden. Prinzipiell kann man die Worst Case-Kollisionslänge mit Hilfe des Protokolls auch extrem klein machen. Eine zu kleine Wahl wird sich jedoch auf den Durchsatz auf Mietnutzerseite auswirken und deswegen einen Pool evtl. völlig uninteressant für die Mietnutzer machen.

Stammmnutzersysteme, die wie die Mietnutzer eine Listen-Before-Talk-Etikette in ihrem Protokoll verfolgen, sind für den Einsatz von Spectrum Pooling nicht geeignet. Sollte nämlich eine erhebliche oder sogar die ganze Bandbreite von Mietnutzern besetzt sein, und die Stammmnutzer diese Belegung feststellen und deshalb nicht zugreifen, so ist die oberste Direktive von Spectrum Pooling verletzt: die Stammmnutzer sollen uneingeschränkte Priorität haben! Die Stammmnutzer müssen also eine Ressourcenverteilung besitzen, an der die Mietnutzer in keiner Weise beteiligt sind. Carrier Sense-Mechanismen auf Seiten der Stammmnutzer dürfen nicht vorhanden sein.

Die Lage im Frequenzband hat einen wesentlichen Einfluss auf die Parameter des Übertragungsverfahrens, das für Spectrum Pooling zum Einsatz kommen soll. So sind z.B. Effekte wie Mehrwegeausbreitung bei hohen Frequenzen deutlicher.

Fasst man all diese Betrachtungen zusammen, so sieht man, dass der Einsatz von Spectrum Pooling sich aus technischer Sicht im Wesentlichen auf FDM-Systeme mit fester Kanalzuweisung reduziert. Glücklicherweise funktionieren fast alle alten Sprechfunkssysteme genau so. Die penible Abstimmung der Sendeleistung der Mietnutzer sowie eine intelligente Schwellendetektion im Empfänger zur Erkennung der Stammmnutzer ist eine zentrale Aufgabe.

In dieser Arbeit soll Spectrum Pooling als Modifikation des etablierten Standards IEEE 802.11 untersucht werden. Deshalb folgt im nächsten Kapitel zunächst eine Zusammenfassung des Standards.

## 2 *Spectrum Pooling*

## 3 Der Standard IEEE802.11

Der Standard IEEE802.11 gehört zur Familie der IEEE802 Standards. Sie alle haben gemeinsame Schichten im *Data Link Layer*, nämlich das *Bridging* (802.1) und die *Logical Link Control*-Schicht (802.2). Sie unterscheiden sich also im Wesentlichen nur in der MAC-Schicht und in der physikalischen Schicht. Ein weiteres Mitglied dieser Familie ist z.B. der 802.3 Standard, der unter der Bezeichnung *Ethernet* große Verbreitung gefunden hat. IEEE802.11 befasst sich mit der Vernetzung von mobilen Geräten, die über eine Luftschnittstelle verfügen, also ihre Daten über Funk austauschen.

### 3.1 Begriffe und Architektur

Hier sollen zunächst einige Bezeichnungen aufgeführt werden, die im IEEE802.11 Standard [IEEE8] definiert sind. Der elementare Baustein eines IEEE802.11-Netzes ist die Station (*STA*). Jede Station bietet eine Grundausstattung an Diensten, die *Station Services* (*SS*). Eine Zusammenfassung mehrerer Stationen wird als *Basic Service Set* (*BSS*) bezeichnet. Ist dieses BSS unabhängig von weiterer Infrastruktur, so heißt es *Independent Basic Service Set* (*IBSS*). Die lokale Begrenzung eines BSS ergibt sich durch die physikalische Erreichbarkeit der Stationen. Ein BSS wird stets von einer *Coordination Function* (*CF*) kontrolliert. Sie verteilt den Zugriff auf das Medium. IBSSs können auch als *ad hoc*-Netzwerke verstanden werden, da sie keinerlei weitere Konfiguration benötigen, und nur so lange bestehen, wie durch die Kolokation eine Funkverbindung möglich ist. Ein Infrastrukturnetzwerk in IEEE802.11 besitzt hingegen mehr als nur Stationen. Es gibt einen Zugriffspunkt (*Access Point*, *AP*), der neu hinzukommenden Stationen ermöglicht, sich zu dem bereits etablierten Netz zu assoziieren.

Ein AP ist normalerweise schlicht eine STA, die weitere Dienste (Address-Mapping, Synchronisation etc.) auf höheren Schichten anbietet. Das Verteilsystem (*Distribution System*, *DS*) ist die logische Einrichtung, über die z.B. Nachrichten verteilt werden. Eine Station, die im physikalischen Empfangsbereich mehrerer BSSs steht, kann funktional ein DS aufbauen. In Abbildung 3.1 ist STA2 ein AP und bietet somit neben den Stationsdiensten (*SS*) auch noch weitere Dienste (*Distribution System Services*, *DSS*) an. Sind über solche APs mehrere BSSs miteinander verbunden, so spricht man von einem *Extended Service Set* (*ESS*). Das hat den Vorteil, dass alle Stationen der verschiedenen BSS eines ESS von höheren Schichten als zu einem Netz zugehörig angesehen werden. Die Stationen können innerhalb eines ESS ihre Position verändern. Diese Bewegung wird als *BSS-Transition* bezeichnet. So ist es z.B. möglich, dass sich STA4 aus BSS2 nach BSS1 bewegt. STA4 würde dann vom neuen AP (STA2) reassoziert. Assoziation ist ein

### 3 Der Standard IEEE802.11

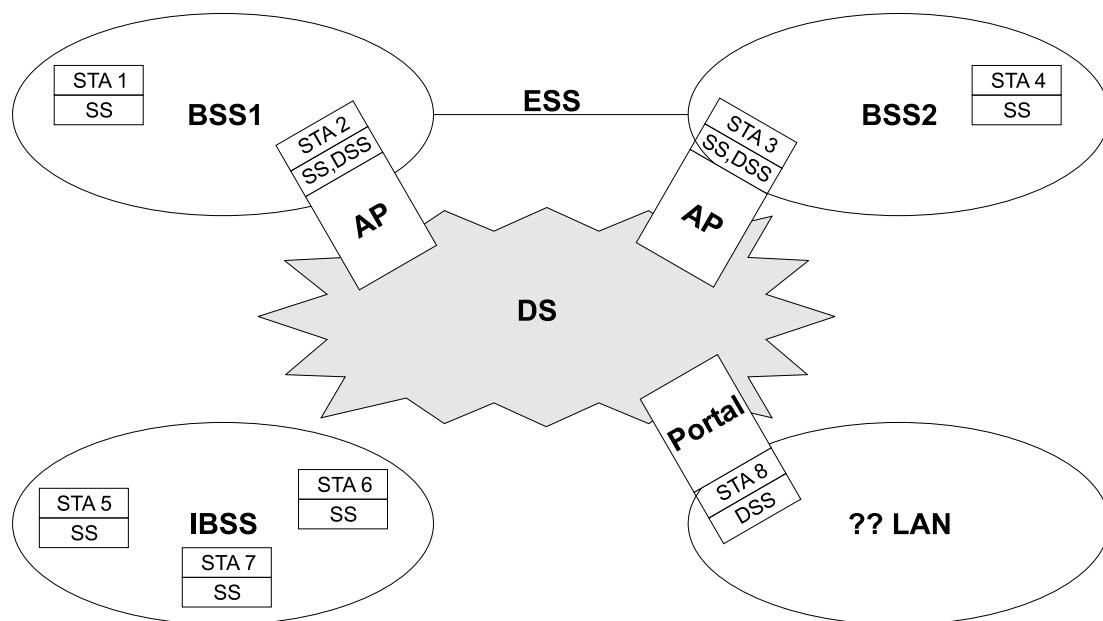


Abbildung 3.1: 802.11Komponenten

wichtiger Begriff in der Architektur des 802.11 Standards. Eine STA ist stets nur zu einem AP assoziiert. Die Assoziation ist ein DSS und ist deshalb nur zwischen APs und Stationen möglich. STAen, die in einem IBSS miteinander kommunizieren, sind nicht miteinander assoziiert! In Abbildung 3.1 hat STA8 die Funktion eines *Portals*. Sie bietet die Integration anderer Netze an. Wie genau eine solche Anbindung definiert sein soll, ist jedoch im IEEE802.11 Standard nicht spezifiziert.

In Abbildung 3.2 ist die Einbettung der 802.11 Spezifikation in das Standardmodell 802.x dargestellt. Der Standard definiert die MAC- und PHY-Schicht. Die Datendienste sind für die LLC-Schicht über den MAC-SAP zu erreichen. Die Managementfunktionen werden von den Unterschichten selbst benutzt und sind auch über das schichtenübergreifende Stationsmanagement (MLME-SAP, PLME-SAP) erreichbar. Die folgende Übersicht soll die Einteilung der Dienste klarstellen:

Stationsdienste(SS):

- Authentifizierung
- Deauthentifizierung
- Verschlüsselung
- Asynchroner Datendienst (*MSDU delivery*)

Dienste des Verteilsystems (DSS)

- Assoziation

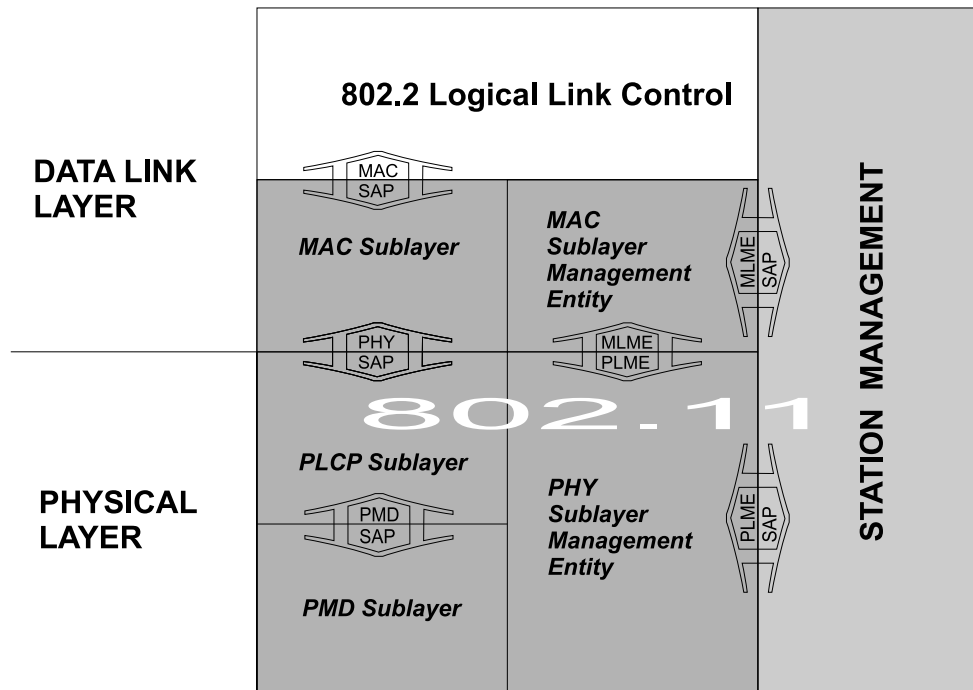


Abbildung 3.2: Schichtenmodell von 802.11

- Dissoziation
- Reassoziaton
- Distribution
- Integration

Somit ist es klar, dass es z.B. in einem IBSS, in dem es keinen AP gibt, auch keine Assoziation gibt. Genausowenig können dort MSDUs verteilt werden, da Distribution ebenfalls ein DSS ist und somit nur in Infrastrukturnetzwerken und nicht in einem IBSS verfügbar ist.

## 3.2 MAC - Dienste

Die MAC-Schicht hat außer der Hauptaufgabe des Datendienstes, also im Wesentlichen der Zugriffssteuerung, auch noch weitere Aufgaben wie Verschlüsselung, Roaming, Synchronisation. Für fast alle Dienste der MAC-Schicht sind Funktionen des Managements nötig. Diese werden von der MAC-Schicht eingesetzt, um z.B. die Umgebung nach möglichen Kommunikationspartnern zu scannen oder die aktuelle Systemzeit zu erfahren. Weitere Details zu den Funktionen des Managements sind in Abschnitt 3.3 zu finden.

Um an einem Infrastrukturnetzwerk teilzunehmen (um z.B. die Dienste des Verteilsystems zu nutzen), muß eine Station zu genau einem AP assoziiert werden. Der Ablauf ist wie folgt: Eine Station bewegt sich in die physikalische Erreichbarkeit eines AP. Sie hört auf spezielle, periodisch wiederholte Pakete (*Beacons*) des AP und kann so die nötigen Informationen finden, um

### 3 Der Standard IEEE802.11

sich anschließend mit dem AP zu authentifizieren und zu assoziieren. Kann die STA solche *Beacons* nicht aufspüren, so ist sie auch in der Lage, mittels eines *Probe*-Paketes selber eine Anfrage auf bestimmte Dienste zu stellen. Zur Assoziation gehört ein *Association Identifier (AID)*, der vom AP für jede assoziierte Station vergeben wird.

#### 3.2.1 Rahmen und Adressierung

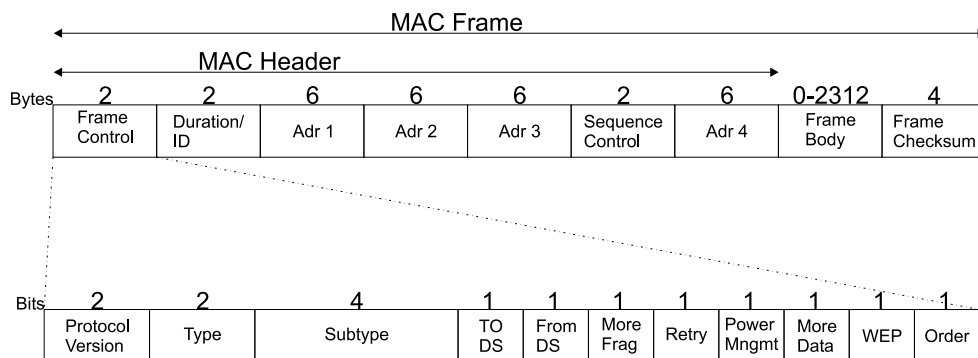


Abbildung 3.3: MAC-Datenrahmen und Inhalte

Die prinzipielle Struktur eines MAC-Rahmens ist in Abbildung 3.3 dargestellt. Die Felder im MAC-Rahmen haben folgende Bedeutung:

- **Frame Control:** Wie man in Abbildung 3.3 sieht, enthalten die ersten zwei Bytes des MAC-Header besonders Informationen über den Datenaustausch. Neben Protokollversion und Typ der Nachricht, sind die Felder *From/To DS* für die Adressierung wichtig. Sie geben an, wie die Felder *ADR1-ADR4* zu interpretieren sind. Ist das *More Frag*-Bit gesetzt, so ist die Nachricht ein Teil einer längeren Nachricht und es folgen noch weitere Rahmen.
- **Duration ID:** Hier sind Informationen über den virtuellen Belegungsmechanismus abgelegt. Weitere Erklärung zu dieser Funktion im 802.11 Netz in Abschnitt 3.2.3.
- **ADR1-ADR4:** Die Adressfelder (je 48 Bit, wie bei anderen 802.x Standards) haben je nach Ursprung und Ziel des Rahmens, was sich in den From/To DS Bits widerspiegelt, verschiedene Bedeutung. In Tabelle 3.1 ist eine Übersicht, angelehnt an [SCH00], zusammengefasst. Die Abkürzungen sind folgendermaßen zu verstehen:

**DA** (Destination Address) MAC-Adresse der Empfängerstation

**SA** (Source Address) MAC-Adresse der Sendestation

**RA** (Receiver Address) MAC-Adresse des Empfangs-AP

**TA** (Transmitter Address) MAC-Adresse des Sende-AP

**BSSID** (BSS Identifier):

- a) ist die STA assoziiert oder selber ein AP, so ist BSSID die MAC-Adresse des AP

To DS	From DS	ADR1	ADR2	ADR4	ADR4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	SA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA

Tabelle 3.1: Bedeutung der Adressfelder im MAC-Rahmen

b) ist die Station Mitglied eines IBSS, ist BSSID die Adresse des IBSS.

- **Sequence Control:** Ist eine Übertragung fehlerhaft, so kann es vorkommen, dass bei einer wiederholten Übertragung Pakete doppelt vorhanden sind. Mit Hilfe der Sequenznummer ist es möglich, diese dann herauszufiltern.
- **Frame Body:** Das Datenfeld, das eine maximale Länge von 2312 Bytes hat, enthält transparente Informationen. Falls das *WEP* Bit im Frame Control gesetzt ist, sind diese Informationen verschlüsselt.
- **Frame Checksum:** Die 32 Bit Prüfsumme hilft, Übertragungsfehler zu behandeln. Das Generatorpolynom ist in [IEEE8, S.40] festgelegt.

Es gibt außer dem Datenrahmen noch den Managementrahmen, der in Abbildung 3.4 zu sehen ist. Weiterhin gibt es noch besondere Rahmen wie *ACK*, *RTS*, *CTS*, *Probe*, *Beacon* usw.,

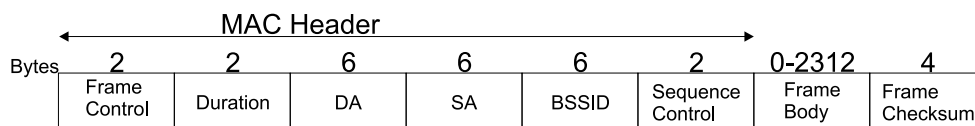


Abbildung 3.4: MAC-Managementrahmen

die jeweils eine eigene Struktur aufweisen. Eine Station, die einen Rahmen empfängt, benutzt stets die erste Adresse im Rahmen (z.B. Datenrahmen: ADR1), um festzustellen, ob die Nachricht an sie gerichtet ist. Ist der Rahmen nicht für sie bestimmt, so wird er ohne Reaktion verworfen. Die Adressen der MAC-Schicht gliedern sich in verschiedene Typen. Der elementarste Typ ist der der *individuellen Adresse*. Sie repräsentiert direkt die Adresse einer Station und ist in ad hoc-Netzen von besonderer Bedeutung. Außerdem existieren sogenannte *Multicast-Gruppenadressen*, mit denen ein logischer Verbund von Stationen auf einmal angesprochen wird. Die *Broadcast-Gruppenadresse* spricht alle Stationen in einem LAN an. Dafür werden in der MAC-Adresse alle Bits auf 1 gesetzt.

### 3 Der Standard IEEE802.11

#### 3.2.2 Authentifizierung und Verschlüsselung

Jede Station hält Zustandsvariablen zu jeder anderen Station, zu der direkte Kommunikation im Netz nötig und gewollt ist. Diese Variablen repräsentieren die Zustände *Authentifizierung* und *Assoziation*. Aus diesen Variablen heraus werden drei Verbindungszustände produziert:

- I Anfangszustand (weder authentifiziert noch assoziiert)
- II Authentifiziert, aber nicht assoziiert
- III Authentifiziert und assoziiert

Der Verbindungszustand gibt an, welche Pakete zwischen den Stationen ausgetauscht werden können und welche zurückgewiesen werden. Im Zustand *I* ist z.B. kein Datenverkehr zum Verteilungssystem möglich, da eine Anmeldung noch nicht erfolgt ist. Um den Verbindungszustand mit einer anderen Station zu ändern, sind einige Regeln festgelegt. So ist z.B. eine Multicast-Authentifizierung nicht möglich, da Authentifizierung stets nur zwischen zwei Stationen gilt. Eine Deauthentifizierung jedoch kann an eine Gruppenadresse gerichtet sein. Der trivialste Fall einer Authentifizierung ist die *Open System Authentication*, bei der der Verschlüsselungsalgorithmus *WEP (Wired Equivalent Privacy)* zur Authentifizierung schlicht übergangen wird. Die zweite Variante ist die *shared key* Authentifizierung. Hier wird der Verschlüsselungsalgorithmus verwendet, der einen gemeinsamen, geheimen Schlüssel voraussetzt. Dieser muss jedoch zuvor über einen externen Weg (also außerhalb des 802.11 Protokolls) verteilt werden und bleibt in der MAC-Schicht als *Write-Only* nach außen hin verborgen.

Authentifizierung wird zwischen den Stationen und deren APs verwendet. In einem IBSS wird Authentifizierung zwischen den Stationen ebenfalls empfohlen.

In einem Übertragungsmedium wie der Luft ist Datensicherheit und Verschlüsselung ein besonders wichtiger Aspekt, da man nie sicher sagen kann, ob nicht doch ein unerwünschter Teilnehmer mithört. Die Verschlüsselung mit dem bereits erwähnten WEP-Algorithmus ist im 802.11 Standard optional, also nicht in jeder Infrastruktur notwendigerweise implementiert oder vorausgesetzt. Seine Funktionsweise sei hier dennoch kurz erklärt:

Der gemeinsame, geheime Schlüssel wird zusammen mit einem Initialisierungsvektor dafür verwendet, eine Pseudozufallsfolge (möglichst langer Periode) zu erzeugen. Diese wird auf den zu übertragenen Bitstrom addiert. Die Daten wurden vorher noch um eine Prüfsumme erweitert, um unautorisierte Veränderungen am Inhalt der Daten nachvollziehen zu können und die Datenintegrität zu sichern. Anschließend wird der veränderte Bitstrom zusammen mit dem Initialisierungsvektor übertragen. Mit Hilfe des empfangenen Initialisierungsvektors kann zur Deschiffrierung die additive Pseudozufallsfolge wieder erzeugt und von den Daten subtrahiert werden. Da spezielle Pakete wie *CTS*, *RTS*, *ACK* besonders häufig übertragen werden und allein aus ihrer Position in der Übertragung identifiziert werden könnten, sollte der Initialisierungsvektor häufig gewechselt werden. So können sich Dritte einen Entschlüsselungsangriff mit Hilfe dieser speziellen Frames nicht erleichtern.

#### 3.2.3 Zugriffsverfahren

Das fundamentale Zugriffsverfahren im 802.11 Standard ist ähnlich dem Ethernet ein *CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance)* - Verfahren. Es stellt ein verteiltes Zu-

griffsverfahren dar und wird deshalb als *Distributed Coordination Function (DCF)* bezeichnet. Neben diesem konkurrierenden Zugriffsverfahren gibt es auch noch ein kontrolliertes Zugriffsverfahren (*Point Coordination Function, PCF*), das von einer ausgewählten Station organisiert wird. Es ist im wesentlichen ein *Polling*-Verfahren. Der *Point Coordinator (PC)* (normalerweise die STA, die den AP repräsentiert) sendet Anfragen an die zugeordneten Stationen und diese antworten daraufhin. Ein selbständiges Senden einer Station ist innerhalb dieser PCF nicht erlaubt. So lassen sich Dienstqualität, Übertragungsraten zwischen STAen etc. realisieren. Da die Priorisierung des PC innerhalb der PCF durch das verteilte Zugriffsverfahren realisiert wird, ist das zentrale Zugriffsverfahren (PCF) innerhalb von CSMA/CA erklärt. Das heisst, es baut auf die Techniken von CSMA/CA auf und ist somit kein wirklich zusätzliches Zugriffsverfahren. In 802.11 sollten sich Perioden der DCF, die als *Contention Period (CP)* bezeichnet werden, mit Perioden der PCF (*Contention Free Period, CFP*) abwechseln.

### DCF-CSMA/CA

Der CSMA/CA-Mechanismus in 802.11 baut besonders auf verschiedene Zeitabstände zwischen gesendeten Frames auf. Prioritätensteuerung wird über unterschiedliche Wartezeiten bestimmt. Die Station mit der kürzesten Wartezeit gewinnt einen konkurrierenden Zugriff, da sie bereits mit dem Senden beginnt, während die anderen Stationen noch wartend das Medium beobachten. Diese Warteintervalle, deren Längen und Auftreten, seien hier kurz zusammengefasst:

- **SLOT**  $9\mu s$ : Dies ist die kleinste Zeiteinheit für die Wahl der zufälligen Wartezeiten im Backoff-Algorithmus.
- **SIFS** (*Short Inter Frame Space*,  $16\mu s$ ): wird vor Frames eingesetzt, die höhere Priorität als alle anderen haben (z.B. ACK, CTS), da diese Wartezeit die kürzeste von allen ist.
- **PIFS** (*Point Coordination Inter Frame Space*,  $25\mu s$ ): Diese Wartezeit benutzt der PC, um eine neue CFP einzuleiten. Sie ist kürzer als DIFS, deshalb gewinnt er Priorität.
- **DIFS** (*Distributed Inter Frame Space*,  $34\mu s$ ): ist die Standardwartezeit innerhalb der DCF, bevor ein neuer konkurrierender Zugriff ausgehandelt wird.
- **EIFS** (*Extended Inter Frame Space*  $\approx 700\mu s$ ). Die Länge dieser Wartezeit ist erheblich länger als alle anderen, sie wird eingesetzt nach Empfang einer Nachricht mit falscher Prüfsumme.

(Die Zeitangaben sind abhängig vom PHY-Layer und entsprechen hier den Angaben aus der OFDM-Schicht 802.11a.)

Das CSMA/CA-Zugriffsverfahren, das die Kollisionswahrscheinlichkeit von Stationen herabsetzt, die gleichzeitig einen Sendewunsch haben, muss besonders während einer laufenden Sendung und nach dem Beenden einer Sendung in Kraft treten. Während eine andere Station sendet, muss das Medium also als besetzt erkannt werden und dementsprechend keine kollidierende Nachricht auf den Weg geschickt werden. Ist die fremde Sendung beendet, kommt der Zeitpunkt, in dem es besonders wahrscheinlich ist, dass Stationen, die während der vergangenen Sendung eine Sendeaufforderung erhalten haben, mit anderen in Konkurrenz treten. Dafür gibt es einen speziellen Algorithmus, der den Anfangszeitpunkt einer Sendung zufällig verzögert und so die Kollisionen herabsetzt. Es gibt für eine Station, die eine Sendung abschicken will, zunächst drei

### 3 Der Standard IEEE802.11

Szenarien:

1. Ist das Medium frei und wurde die letzte Sendung korrekt beendet (es wurde die korrekte Prüfsumme empfangen), so wird eine Zeitdauer DIFS gewartet, ob das Medium frei bleibt. Ist es während der gesamten Wartezeit frei geblieben, so beginnt die Station nach Ablauf der Verzögerung sofort mit der Sendung.
2. War die letzte Sendung unvollständig oder fehlerhaft, so wird die Wartezeit durch eine längere Zeit EIFS ersetzt - ansonsten bleibt das Verhalten gleich.
3. Ist das Medium besetzt, so wird gewartet, bis das Medium nach der letzten Aktivität irgendeiner Station mindestens eine Dauer der Länge DIFS frei geblieben ist. Daraufhin wird der *Backoff*-Algorithmus gestartet und eine zusätzliche Wartezeit ausgewürfelt. Da diese Wartezeit nun (idealerweise) bei allen Stationen unterschiedlich ist, wird die Station, die die kleinste Wartezeit gewürfelt hat, ihre Sendung verschicken können. Die anderen Stationen merken das, da sie während der Wartezeit stets die Aktivität des Mediums beobachten. Sollte eine andere Station früher mit der Sendung beginnen, so wird die eigene noch weiter verzögert. Die Stationen warten dann wieder, bis die sendende Station fertig ist. Dann beginnt wieder der Backoff-Algorithmus, aber diesmal mit etwas veränderten Parametern. Alle Stationen, die schon einmal (vergeblich) versucht haben, eine Sendung zu verschicken, warten jetzt nur noch die Wartezeit, die vom letzten Mal übrig geblieben ist. So wird erreicht, dass die Stationen, denen schon besonders oft andere zuvor gekommen sind, eine kürzere Wartezeit für den nächsten, konkurrierenden Zugriff haben, und somit ihre Chance wächst, dass sie die Konkurrenzphase gewinnen.

Um das Zusammenspiel mehrerer Stationen zu verdeutlichen, soll das Beispiel in Abbildung 3.5 erklärt werden: Zum Zeitpunkt  $t_0$  bekommt STA4 von höherer Protokollschicht das Signal, ein Paket zu verschicken. STA4 befindet sich damit in dem oben erwähnten Szenario 1 und wartet also ein DIFS ab, ob das Medium frei bleibt. Nach dieser Wartezeit schickt STA4 das Paket los. Während nun STA4 das Paket verschickt (die Empfangsbestätigung der Zielstation durch ein ACK-Frame ist hier zur Vereinfachung nicht dargestellt), bekommen STA2 und STA3 von höheren Schichten auch eine Sendeaufforderung. Sie befinden sich also in Szenario 3. Sie warten, bis das Medium mindestens eine Zeit DIFS frei ist, und dann beginnt die Konkurrenzphase (*Backoff Window*). Sie würfeln beide eine Zufallszahl aus dem Intervall  $[0, CW]$ , zählen diese in gleicher Geschwindigkeit herunter und versenden beim Erreichen der Null ihre Nachricht. STA3 hatte eine 4 gewürfelt, also wird der Zählvorgang schneller beendet sein als bei STA2. STA3 beginnt mit der Sendung, da im Zeitpunkt  $t_4$  das Medium immer noch frei ist. STA2 bekommt dies mit (die Stationen beobachten das Medium während den Wartezeiten) und bricht den Zählvorgang ab. Sie muss jetzt wieder warten, bis das Medium für ein DIFS frei ist, und kann ihren Zähler dann weiter herunter zählen. Sie würfelt keine neue Zahl! Sollten zwei Stationen die gleiche Zufallszahl gewählt haben, so kommt es dennoch zur Kollision. Diese wird jedoch erkannt, da die Empfängerstationen aufgrund der fehlerhaften Prüfsumme keine Bestätigung verschicken. Ist also eine solche Kollision aufgetreten, so werden die sendenden Stationen ihre Zufallszahl aus einem größeren Bereich auswählen, um die Kollisionswahrscheinlichkeit noch weiter her-

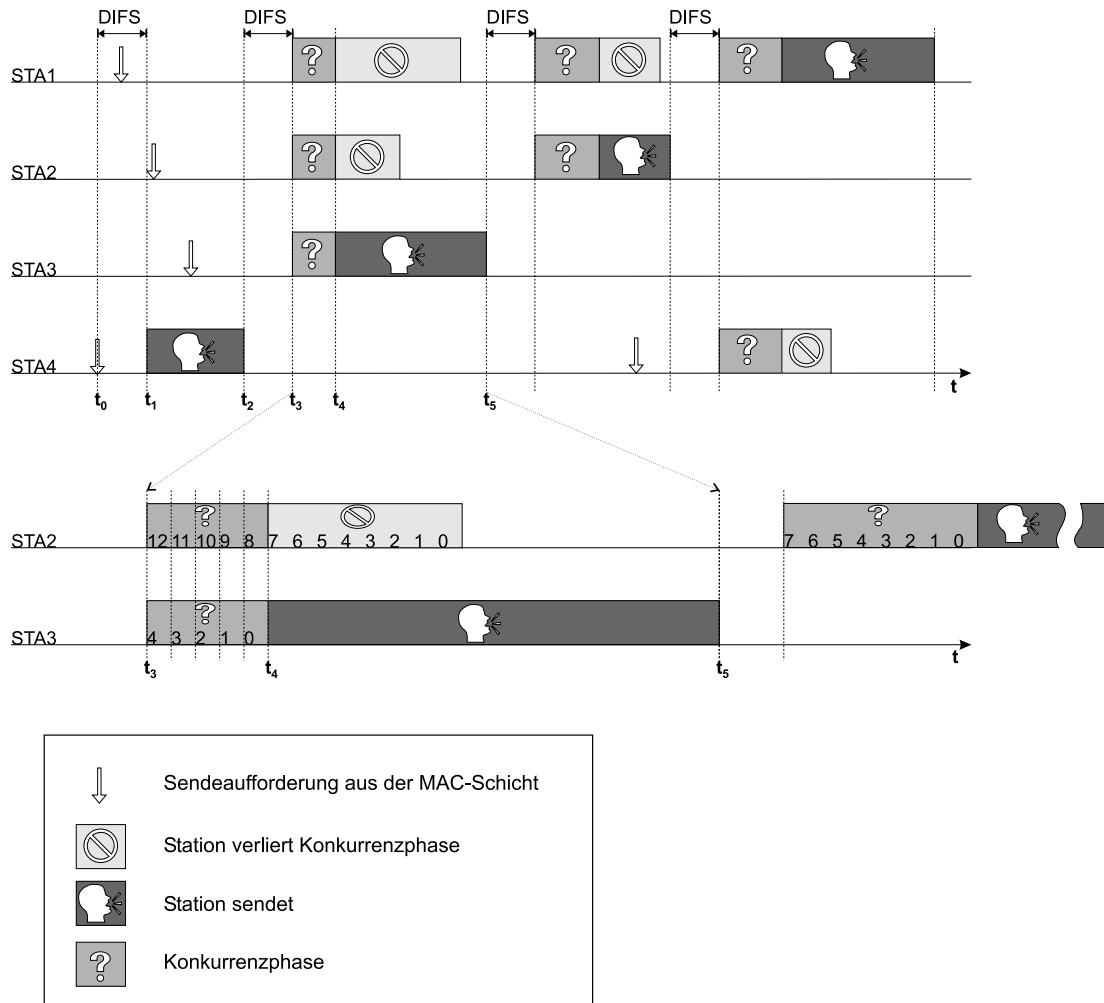


Abbildung 3.5: CSMA/CA in 802.11

### 3 Der Standard IEEE802.11

abzusetzen. Der Standard sieht hier eine exponentielle Vergrößerung des Intervalls  $[0, CW]$  bis zu einer maximalen Größe  $[0, CW_{max}]$  vor. Die Zufallszahl wird gleichwahrscheinlich aus dem Intervall  $[0, CW]$  gewählt. In [BIA96] und [CAL00] ist gezeigt, wie man die Intervalllänge im Laufe des Zugriffsverfahrens am günstigsten wählen kann, um den maximalen Durchsatz zu erreichen.

#### Hidden Terminals und der RTS/CTS Mechanismus

Ein besonders kritisches Problem in FunkLANs ist das der *Hidden Terminals*. In Funknetzen

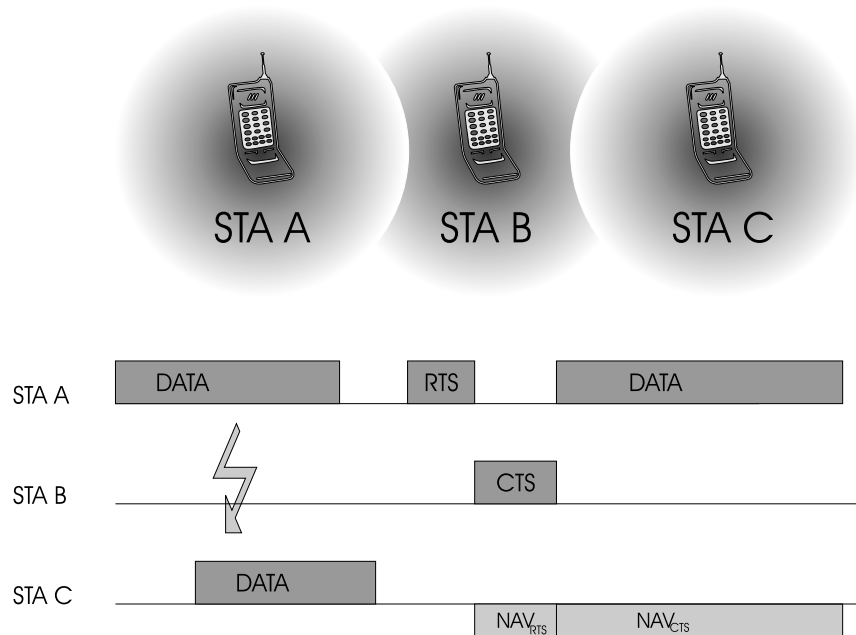


Abbildung 3.6: Hidden Terminal und RTS/CTS-Mechanismus

kann es aufgrund der Sendeleistung passieren, dass Stationen zwar mit den nächsten Nachbarn kommunizieren können, aber nicht alle anderen Stationen, die für Kollisionen in der Übertragung verantwortlich sind, wahrnehmen. In Abbildung 3.6 ist z.B. Station C nicht im physikalischen Sende/Empfangsbereich von Station A. Will STA A an STA B senden, und STA C, die davon überhaupt nichts mitbekommt, ebenfalls, so kommt es in STA B zur Überlagerung der beiden Pakete, was sie unbrauchbar macht und eine Wiederholung erfordert.

Um diese Kollisionen zu vermeiden, wird ein zusätzlicher Handshake eingesetzt. STA A sendet erst ein RTS-Paket los, das erheblich kürzer ist als das Datenpaket (die Längen in Abbildung 3.6 sind nicht maßstäblich!), und STA B antwortet mit einem ebenfalls sehr kurzen CTS. Dieses CTS kann STA C empfangen und die *virtuelle Belegung* auslösen. In den RTS oder CTS Rahmen werden Informationen über die Länge des kommenden Datenpaketes mitgeteilt. So weiß STA C, wie lange STA A und STA B Daten austauschen und wird seinen (*Network Allocation Vector, NAV*) entsprechend setzen. Dieser gibt an, bis wann das Medium virtuell von anderen Stationen

belegt ist. Auf diese Weise wird die Kollision von Paketen in STA B verhindert, was sich natürlich positiv auf den Durchsatz im Netzwerk auswirkt. Ist das Datenpaket jedoch so kurz, dass sich der zusätzliche Aufwand nicht lohnt, so wird von dem RTS/CTS-Handshake abgesehen.

#### PCF

Anders als die DCF bietet die *Point Coordination Function* einen kollisionsfreien Zugriff. Zur Kontrolle dieses Zugriffsverfahren wird ein *Point Coordinator* eingesetzt, der die Stationen im BSS anspricht. Da die Regeln der PCF auf den Regeln der DCF beruhen, braucht keine zusätzliche Funktionalität implementiert zu werden. Die CFP (*Contention Free Period*), in der die PCF gilt, wird vom PC eingeleitet, indem er seine Wartezeit (PIFS) nach dem letzten Paket auf dem Medium kleiner als alle anderen wählt und so den Zugriff bekommt. Jede CFP soll mit dem Senden eines *Beacon*-Rahmens beginnen, der die Stationen im Netz veranlasst, ihren NAV zu setzen, und somit bis zum Ende der CFP nicht zu senden. Während der CFP werden die STA, die der PC in der *Polling List* hält, vom PC angesprochen, um Daten zu oder von ihnen zu übertragen. STAen können sich der CFP entziehen, indem sie bei der Assoziation kein *CF-Pollable* angeben. Soll dieser Zustand geändert werden, so muß eine Reassoziatioen ausgelöst werden.

#### Weitere Dienste

Ist eine Nachricht zu lang, um in einen Standard MAC-Frame-Body platziert zu werden, so ist Fragmentierung nötig. Dazu wird die Nachricht zerlegt und im Sequence Control-Feld im MAC-Header werden Nummerierungen eingetragen.

## 3.3 MAC-Management

Das Management wird, wie in Abbildung 3.2 gezeigt, als eigenständiger Teil der Protokollschichten verstanden, der die Dienste in der MAC- und PHY-Schicht mit Funktionalität unterstützt. Außerdem sind die Managementeinheiten in den Protokollschichten über die MLME- bzw. PLME-SAP zu erreichen.

### 3.3.1 Synchronisation

Alle Stationen in einem BSS besitzen eine gemeinsame Zeitbasis, die mit Hilfe der *Timing Synchronization Function (TSF)* realisiert wird. Als Zeitzähler besitzt jede STA einen *64Bit-Zähler*, der im Mikrosekundentakt erhöht wird. Die Synchronisation zwischen den Stationen soll  $4\mu s$  plus die maximale Laufzeit im Medium nicht überschreiten. Zum periodischen Verteilen der aktuellen Systemzeit werden Beacon-Frames eingesetzt. Sie werden zu periodischen Zeitpunkten gesendet und beinhalten die aktuelle Systemzeit. Jeder Empfänger eines solchen Beacons stellt seine Uhr dann auf die aktuelle Zeit. Wie in Abbildung 3.7 zu sehen ist, kann es passieren, dass das Medium zu dem Zeitpunkt besetzt ist, an dem eigentlich ein Beacon hätte übertragen werden sollen. In einem solchen Fall wird die Übertragung des Beacons verschoben. Es wird jedoch als Zeitstempel stets die Zeit verwendet, zu der die Übertragung *tatsächlich* stattfindet, und somit

### 3 Der Standard IEEE802.11

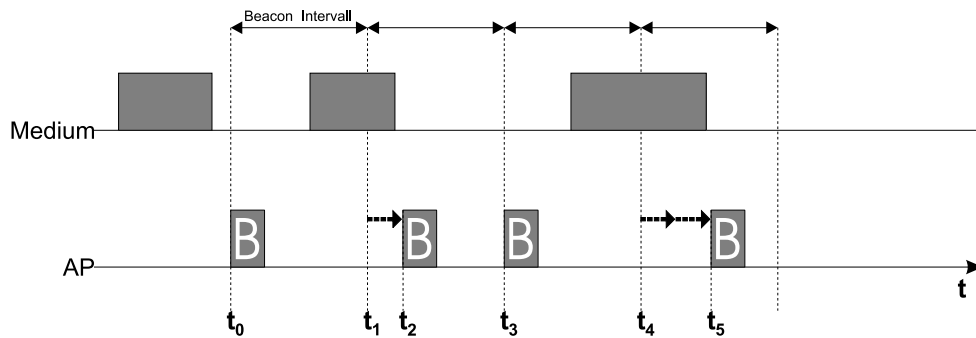


Abbildung 3.7: Zeitsynchronisation mit Beacon-Frames

bleibt die Systemzeit richtig. Lediglich der Zeitpunkt der Übermittlung ist flexibel.

Beacon-Frames werden in Infrastrukturnetzen vom AP generiert. In IBSS (ohne AP) sendet jede STA Beacons. Dafür nehmen alle STA im IBSS die gleiche Beacon-Rate an und konkurrieren zum Beacon-Sendezeitpunkt mit Hilfe der DCF darum, welche STA ein Beacon verschickt.

Um sich zu einem bestehenden Netz zu synchronisieren, hört eine Station eine gewisse Zeit auf verfügbare Beacons. Entspricht die *SSID (Service Set Identifier)* derjenigen, nach der die STA gerade sucht, so werden Parameter wie Beacon-Periode, BSSID etc. angenommen und im Falle eines Infrastrukturnetzes evtl. eine Assoziation zum AP durchgeführt. Neben diesem passiven Mechanismus ist eine STA auch in der Lage einen *Probe-Rahmen* zu senden, in welchem er die gewünschte SSID verbreitet. Hört ein passender Kommunikationspartner diesen Probe-Rahmen, so wird er bestätigt und der Verbindungsaufbau kann beginnen.

Es ist einer STA auch erlaubt, unabhängig vom weiteren Umfeld selber ein neues BSS zu eröffnen. Dafür muß sie einfach die Beacon-Periode und ID des BSS festlegen und Beacons versenden.

#### 3.3.2 Energiemanagement

FunkLANs werden besonders dort eingesetzt, wo eine feste Verdrahtung der Geräte nicht erwünscht ist. Die teilnehmenden Geräte sind also mehr oder weniger mobil und besitzen häufig Batterien als Energieversorgung. Um die Betriebszeit der mobilen Geräte nicht unnötig herabzusetzen, befasst sich das 802.11 Protokoll auch mit Energiemanagement.

Jede STA kann entweder voll eingeschaltet sein oder nur vereinzelt auf spezielle Beacons hören und die restliche Zwischenzeit ausgeschaltet sein. Der AP spielt im Zusammenhang mit Energiemanagement eine besondere Rolle. Er ist stets voll verfügbar und speichert die Nachrichten vorübergehend, die an Stationen gerichtet sind, die gerade im Energiesparmodus sind. Zu diesem Zweck wird eine *Traffic Indication Map (TIM)* eingerichtet, die angibt, für welche Stationen Datenverkehr ansteht. Diese TIM wird mit jedem Beacon vom AP übertragen. Da auch die STA im Energiesparmodus von Zeit zu Zeit auf Beacons hören, werden sie so informiert, ob sie sich für Datenverkehr voll einschalten müssen.

In IBSSs werden *ATIMs (Ad Hoc Traffic Indication Messages)* verwendet, die Informationen

über ein zu sendendes Datenpaket beinhalten. Eine STA, die an andere STA, welche im Energiesparmodus sind, Daten verschicken will, sendet direkt nach dem Beacon solche ATIMs aus, um den Kommunikationswillen zu äußern. Alle Stationen müssen in diesem Zeitfenster „wach“ sein. Da diese ATIM-Rahmen im Vergleich zum eigentlichen Datenverkehr sehr kurz sind, kann eine Station, auf die keine Übertragung wartet, bis zum nächsten Beacon-Zeitpunkt abschalten und Energie sparen.

#### 3.3.3 Assoziation, Dissoziation und Roaming

Hier soll noch einmal ein Ablauf zusammengefasst werden, wie eine Station Verbindung zu einem Netz aufbaut:

1. Die Station besitzt keine Verbindung oder will ihre Verbindung aufgrund der schlechten Übertragungsrate oder aus anderen Gründen ändern.
2. Die Station benutzt das MAC-Management-Dienstprimitiv *MLME-scan.request*, um Informationen über die Umgebung zu erhalten.
3. Dieser Dienst analysiert die möglichen Kommunikationspartner
  - passiv:** indem er Informationen in allen Beacons, die er empfangen kann, interpretiert.
  - aktiv:** indem er Probe-Frames mit dem gewünschten Verbindungen und Diensten aussendet und auf Probe-Response-Frames wartet.
4. Das MAC-Management-Dienstprimitiv *MLME-scan.confirm* liefert Informationen über gefundene BSSs zurück.
5. Ist ein möglicher Kommunikationspartner gefunden, so wird unterschieden zwischen IBSS und Infrastruktur-Netzwerk:
  - IBSS:** Die STA übernimmt Parameter wie Beacon-Periode, FH-Set, Datenrate etc. und nimmt am Versenden von Beacons teil.
  - Infrastruktur-Netzwerk:** Die STA authentifiziert und assoziiert sich mit dem AP. Sie tauscht mit ihm Parameter wie Power-Managementstatus, CF-Pollablestatus etc. aus und beginnt ihre Uhr nach Beacons vom AP zu stellen.

## 3.4 Physikalische Schichten

Prinzipiell wird in 802.11 (wie in Abbildung 3.2 zu sehen) die physikalische Schicht in eine *Physical Medium Dependent (PMD)* und eine darüberliegende *Physical Layer Convergence Procedure (PLCP)* aufgeteilt. Wie jedoch die Dienste und Funktionalitäten der physikalischen Schicht in diesen Unterschichten aufgeteilt werden, ist nicht zwingend. Für das 802.11 Protokoll sind bisher 4 verschiedene physikalische Schichten vorgeschlagen:

1. FHSS (*Frequency Hopping Spread Spectrum*) im 2.4Ghz-Band mit maximal 2Mbit/s
2. DSSS (*Direct Sequence Spread Spectrum*) im 2.4Ghz-Band mit maximal 2Mbit/s
3. IR (*Infrared*) im 850 – 950nm Bereich mit maximal 2Mbit/s
4. OFDM (*Orthogonal Frequency Division Multiplex*) im 5Ghz-Band mit maximal 53Mbit/s

Im Rahmen dieser Arbeit soll nur auf die aktuellste und zukunftsreichste Variante (802.11a), die OFDM-PHY-Schicht eingegangen werden.

### 3.5 802.11a - OFDM-PHY-Schicht

Obwohl OFDM schon in den 60er Jahren erdacht wurde, hat sich dieses Übertragungsverfahren (es ist zugleich auch ein Zugriffsverfahren) erst sehr spät aus dem militärischen in den zivilen Bereich durchgesetzt. In den 90ern wurden dann Systeme wie ADSL, HDSL, DAB, HDTV mit OFDM zum Einsatz gebracht. Bei OFDM wird die verwendete Bandbreite nicht wie bei klas-

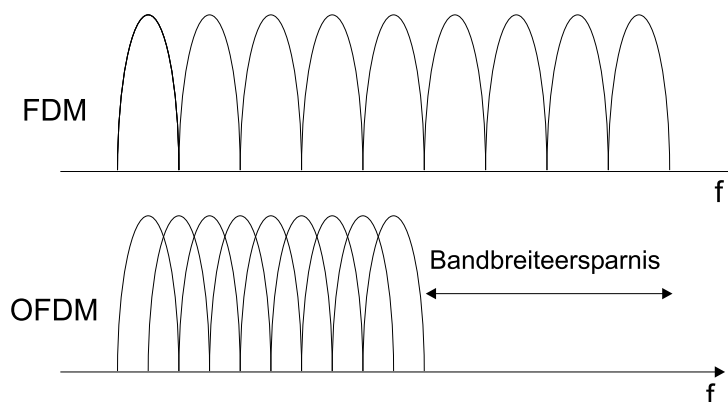


Abbildung 3.8: Bandbreitenvorteil bei OFDM

sischen FDM in getrennte Frequenzbänder geteilt. Stattdessen überlappen sich die Unterbänder teilweise, und somit wird Bandbreite gespart. Abbildung 3.8 zeigt, wie die Teilbänder bei OFDM zusammengeschoben werden. Damit die überlappten Bänder noch voneinander zu trennen sind, müssen die einzelnen Träger zueinander orthogonal sein. Der Empfänger betrachtet stets ein OFDM-Symbol der Dauer  $T$ . Wenn die Schwingungsdauer der Unterträger dann ganzzahlig in das Intervall  $T$  passen, ist eine fehlerlose Rückgewinnung der Sendung möglich. Die Symboldauer  $T$  ist bei OFDM ein wichtiger Parameter. Der Abstand der Unterträger ist nämlich durch die Orthogonalitätsbedingung dann  $\Delta_F = 1/T$ .

Die einfache Basisbandsignalerzeugung ist ein bedeutender Vorteil von OFDM. Für ein klassisches FDM-Verfahren wären die jeweiligen Trägerfrequenzen zu erzeugen und die gewünschte Modulation müsste aufmultipliziert werden. Bei OFDM ist das Zeitsignal der überlagerten, orthogonalen Unterträger eines Symbols gerade die inverse Fouriertransformierte der  $QAM$  Symbole auf den Unterträgern. Nun lässt sich also das Zeitsignal z.B. durch IFFT, wie in [RIC00, S.34f] gezeigt, aus den Parametern der Modulation ( $QAM$ - oder  $PSK$ -Varianten) erzeugen, ohne dass die vielen Trägerfrequenzen zur Verfügung stehen müssen. Das ist eine erhebliche Einsparung von Komplexität in den Sendern und Empfängern.

Ein weiterer Vorzug von OFDM ist die effektive Art, wie Mehrwegeausbreitung behandelt wird. Hierfür wird vor der Sendung eines Symbols dieses in einem *Guard Intervall* zyklisch fortgesetzt. Somit können verzögert ankommende Unterträger nicht mehr die Orthogonalität verletzen (es entsteht nur eine Phasenverschiebung), denn die FFT-Berechnung im Empfänger beginnt erst nach dem Ablauf des Guard Intervalls. Es muß lediglich sicher gestellt werden, dass das Guard Intervall länger als jede mögliche Verzögerung durch Mehrwegeausbreitung ist.

### 3.5.1 Datenraten, Parameter

MBit/s	Modulation	Coderate	Bits/Unterträger	CodeBits/Symbol	Datubits/Symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Tabelle 3.2: Datenraten und Parameter

Tabelle 3.2 (entsprechend [IEEE9, S.9]) zeigt die möglichen Datenraten, wobei nur  $6\text{ MBit/s}$  obligatorisch für alle 802.11a Geräte ist. Es werden 48 Daten-Unterträger verwendet und 4 für Pilottöne. Die Pilottöne liegen auf den Trägern im Abstand 7 und 21 von der Mitte. Der Träger auf der HF-Mittelfrequenz wird nicht benutzt. Der Frequenzabstand der Unterträger beträgt  $\Delta_F = 312,5\text{ kHz}$ , daraus ergibt sich eine FFT-Periode von  $1/\Delta_F = 3,2\mu\text{s}$ . Die benötigte Bandbreite ist für einen OFDM-Kanal  $(48 + 4 + 1) \cdot 0,3125\text{ MHz} = 16,563\text{ MHz}$ . Die Kanäle werden mit Sicherheitsabstand im 20MHz-Raster angelegt. Das Guard-Intervall beträgt  $800\text{ ns}$ , was einer Laufdifferenz von 240m entspräche. Die Dauer eines OFDM-Symbols ergibt sich zu  $4,0\mu\text{s}$ .

### 3.5.2 Rahmen

Der MAC-Rahmen wird in den PHY-Rahmen eingebettet. Die Übertragung des Headers des PHY-Frames ist obligatorisch mit der niedrigsten Datenrate vorzunehmen. So können Stationen, die wegen der hohen Rate den Datenteil nicht empfangen können, zumindest ausrechnen, bis wann der Kanal belegt ist. Dies ist für das Zugriffsverfahren und den *virtual carrier sense* Mechanismus (siehe Kapitel 3.2.3) wichtig. Die Felder im PHY-Rahmen haben folgende Bedeutung:

### 3 Der Standard IEEE802.11

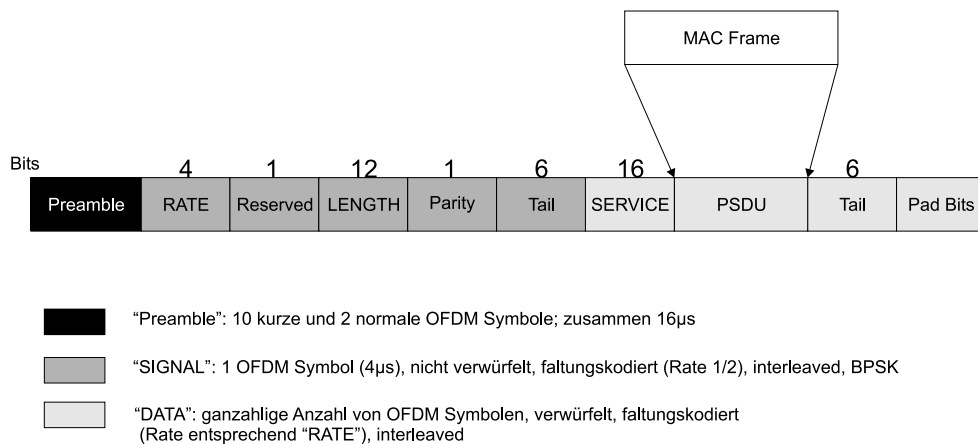


Abbildung 3.9: Aufbau des PHY-Rahmen

- **Preamble:** Die Präambel besteht aus zehn kurzen und zwei langen Trainingssequenzen mit einer Gesamtdauer von 16µs. Sie ist zur Synchronisation, Verstärkereinstellung und für das Zugriffsverfahren nötig.
- **RATE:** Hier wird über die Übertragungsrate im Datenteil informiert.
- **LENGTH:** Gibt die Anzahl der Bytes an, die die PSDU enthält.
- **Parity:** Ein gerades Paritätsbit zur Fehlererkennung für die vorangegangenen 16 Bit.
- **Tail:** Alle sechs Bits werden zu Null gesetzt.
- **SERVICE:** Alle Bits werden zu Null gesetzt, wobei die ersten sieben Bits den Verwürfler im Empfänger initialisieren; d.h. sie sollen helfen, den Anfangszustand des Verwürflers im Sender zu schätzen.
- **PSDU:** Enthält den vorbereiteten MAC-Frame.
- **Tail:** Alle Bits werden zu Null gesetzt, um den Faltungscodierer zurückzusetzen. Hier ist zu beachten, dass die Tail-Bits zwar ein Teil von DATA sind, somit also auch verwürfelt werden, aber sie anschließend dennoch erneut auf „0“ zurückgesetzt werden!
- **Pad Bits:** Es wird die nötige Anzahl an Bits (Wert=Null) angehängt, damit die Gesamtlänge der Nachricht ein ganzzahlig Vielfaches der Länge eines OFDM-Signals wird.

#### 3.5.3 Präambeln

Jeder Rahmen, der die physikalische Schicht verläßt, wird mit einer Präambel versehen. Diese hat verschiedene Aufgaben der Korrektur und Synchronisation zu erfüllen. In Abbildung 3.10 ist eine Präambel der OFDM-Schicht zu sehen. Sie besteht aus 10 kurzen (*sts*: Short Training Symbols) und 2 langen (*LTS*: Long Training Symbols) Trainingssymbolen. Die ersten 7 der kurzen Trainingssymbole werden für die Signalerkennung, die automatische Empfangsverstärkerregelung und den Carrier Sense-Mechanismus verwendet. Die nächsten 3 kurzen Trainingssymbole sind für die grobe Frequenzversatzschätzung und Zeitsynchronisation. Die kürzere Dauer der ersten Trainingssymbole hat vor allem für die Schätzung des Frequenzversatzes Bedeutung: Durch

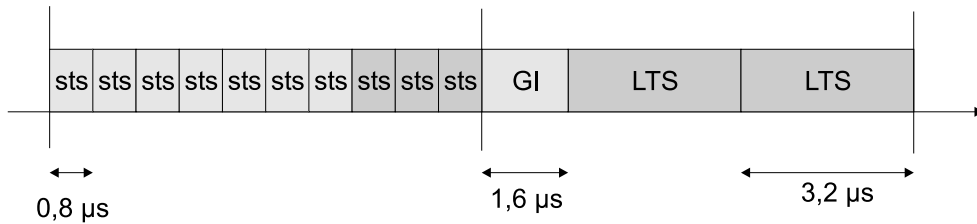


Abbildung 3.10: Aufbau der Präambel in 802.11a

die kürzere Dauer kann eine kürzere Korrelationslänge realisiert werden, was eine Schätzung des Frequenzversatzes ermöglicht, auch wenn dieser mehr als ein Unterträgerabstand ist. Eine detailliertere Ausführung findet man in [OFD00]. Diese verkürzten Symbole werden erzeugt, in dem die Träger von der Sequenz

$$S_{-26,26} = \sqrt{\frac{13}{6}} x \{0, 0, 1 + j, 0, 0, 0, -1 - j, 0, 0, 0, 1 + j, 0, 0, 0, -1 - j, 0, 0, 0, -1 - j, 0, 0, 0, 1 + j, 0, 0, 0, 0, 0, 0, -1 - j, 0, 0, 0, -1 - j, 0, 0, 0, 1 + j, 0, 0, 0, 1 + j, 0, 0, 0, 1 + j, 0, 0, 0, 1 + j, 0, 0\}$$

moduliert werden. Es wird nur jeder vierte Träger eingesetzt, was zu einer Periodizität im Zeitbereich führt, die nur noch ein Viertel (also  $3,2\mu s / 4 = 0,8\mu s$ ) der ursprünglichen ist. In Abbil-

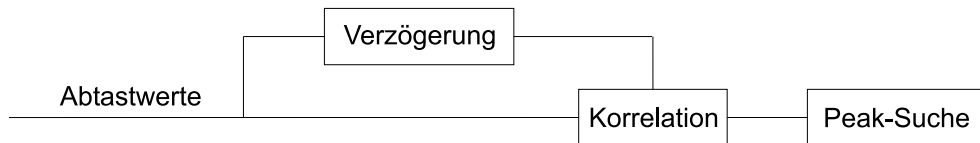


Abbildung 3.11: Empfängerstruktur für Präambeln

dung 3.11 sieht man eine vereinfachte Darstellung eines typischen Empfängers für Präambeln. Die einlaufenden Daten werden je nach Wiederholungslänge der Symbole in der Präambel (z.B. für die kurzen Trainingssymbole:  $0,8\mu s$ ) zeitverzögert und mit sich selbst korreliert. Wenn dann zwei gleiche Symbole in den Abtastwerten auftreten, die die Länge besitzen, die der eingestellten Verzögerung entspricht, so ist der Korrelationswert hoch. Anschließend muß noch diese Korrelationspitze gefunden werden.

### 3.5.4 Kommunikationsablauf

#### Senden

Nachdem die MAC-Schicht festgestellt hat, dass der Kanal frei ist und mit Hilfe des Managements die nötigen Parameter wie Datenrate etc. eingestellt hat, ruft sie das entsprechende Dienstprimitiv auf, um die Sendung zu starten. Die PLCP-Schicht stellt daraufhin die Parameter in der PMD-Schicht ein und verursacht den Beginn der Sendung der Präambel und des „SIGNALS“.

### 3 Der Standard IEEE802.11

Anschließend werden die Daten von der MAC-Schicht byteweise an die PLCP-Schicht übertragen und zur Sendung verarbeitet. Die folgende Datenverarbeitung wird *nur* mit den Feldern SERVICE, PSDU, Tail, Pad Bits gemacht. Hier wird zunächst ein Verwürfler mit 127 bit langer Periode eingesetzt. Beim Anfang der Sendung wird der Verwürfler auf einen zufälligen Status gesetzt, welcher im Empfänger später (mit Hilfe der Null Bits im SERVICE-Feld) geschätzt wird. Die verwürfelten Bits werden mit einem Faltungscodierer der Gedächtnislänge 7 codiert und danach kommt noch ein Interleaver zum Einsatz. Der Interleaver hat die Aufgabe, nahe beieinanderliegende Datenbits auf weit auseinanderliegende OFDM-Träger zu verteilen. Er arbeitet stets mit der Länge eines OFDM-Symbols. Es werden also keine OFDM-Symbole miteinander verschachtelt. Diese Daten werden dann an die PMD-Schicht weitergereicht. Die MAC-Schicht ist jederzeit in der Lage, die Übertragung abzubrechen.

#### Empfangen

Nach dem Empfang der Präambel wird, falls diese eine Sendeleistungsgrenze überschreitet, das Eintreffen einer Nachricht an die MAC-Schicht mitgeteilt. Die PHY-Schicht beginnt nun, den SIGNAL-Teil des PHY-Rahmens zu finden um die entsprechende Datenrate einzustellen. Mit Hilfe der RATE und LENGTH Felder wird dann das Medium bis zum Ende der Nachricht als besetzt signalisiert. Die PSDU wird decodiert und entwürfelt. Dazu wird vorzugsweise der Viterbi-Algorithmus verwendet. Sollte die Nachricht vor dem erwarteten Ende abbrechen oder das Paritätsbit nicht stimmen, so wird der Fehler an die MAC-Schicht mitgeteilt. Alle Symbole, die nach dem erwarteten Ende der Nachricht folgen, werden kommentarlos ignoriert.

## 3.6 Die 802.11 Familie

Zur Vollständigkeit sollen alle Unterstandards von 802.11 genannt werden. Das sind

**802.11a** Physikalische Schicht auf OFDM-Basis

**802.11b** Neuauflage der Physikalischen Schicht von 802.11 mit DSSS und Übertragungsraten bis zu  $11\text{Mbit/s}$

**802.11c** Abläufe in der MAC-Schicht wurden für ISO-Bridging angepasst

**802.11d** Anpassung der PHY-Schichten für die lokalen Beschränkungen einiger Länder

**802.11e** QoS wurde in der MAC-Schicht realisiert

**802.11f** Spezifikation von Hand Over zwischen Geräten verschiedener Hersteller

**802.11g** Erweiterung des 802.11b für bis zu  $22\text{Mbit/s}$  Übertragungsraten mit Erhalt der Abwärtskompatibilität

**802.11h** Erweiterung der MAC-Schicht für den europäischen Markt mit Sendeleistungsregelung und dynamischer Frequenzwahl

**802.11i** Erweiterung der Verschlüsselung mit WEP in der MAC-Schicht, Alternative Verschlüsselungsvorschläge und sicherere Authentifizierung

## 4 Modifikation von 802.11a für Spectrum Pooling

Zunächst sollen nochmals die technischen Voraussetzungen der Pools und Nutzersysteme zusammengefasst werden, die die Arbeitsgrundlage der theoretischen Betrachtungen und Simulationen in dieser Arbeit sind. Die Voraussetzungen für das Stammnutzersystem:

- Die Stammnutzer verwenden ein FDMA-Verfahren.
- Die Stammnutzer verwenden keinen Carrier Sense-Mechanismus.
- Die mittleren Sendeleistungen der Stammnutzer sind bekannt.
- Die Breite eines Stammnutzers im Frequenzbereich ist größer oder gleich dem Unterträgerabstand des OFDM-Systems der Mietnutzer.
- Die Stammnutzer können eine Worst Case-Kollisionslänge von  $t_{coll,max}$  vertragen.
- Die Stammnutzer besitzen keine Kommunikation mit den Mietnutzern. Speziell ist der Ablauf der Ressourcenvergabe der Stammnutzer nicht bekannt.

Auch an das Mietnutzersystem werden einige Anforderungen gestellt:

- Die Mietnutzer verwenden eine modifizierte Variante des Zugriffsverfahren aus IEEE802.11.
- Die Mietnutzer verwenden OFDM als Modulationsverfahren, die Parameter müssen dem Frequenzbereich und der Mobilität angepasst werden.
- Die Mietnutzer besitzen neben dem Pool *keinen* weiteren Übertragungskanal, der für Signalisierungen, Assoziation oder Hand Over genutzt werden kann.
- Die Mietnutzer sind in der Lage, die Stammnutzer zu erkennen und die angeforderten Ressourcen für die Stammnutzer freizugeben.
- Die Mietnutzer kennen a priori die grundlegenden Parameter vom Mietnutzersystem in denjenigen Pools, in denen sie kommunizieren werden. Das sind:
  - Die Bandbreite der Pools
  - Die Lage der Pools im Frequenzband
  - Die OFDM-Parameter des Mietnutzersystems der Pools wie Anzahl der Träger, Samplingrate, FFT-Länge etc.

Der betrachtete Frequenzbereich (*Pool*) wird in kleinere Abschnitte aufgeteilt. Diese Aufteilung entspricht dem Unterträgerabstand des OFDM-Systems der Mietnutzer. Die Stammnutzer sollen, wie schon oben genannt, stets mindestens die Breite eines Trägerabstandes haben. Somit kann bei der Detektion der Stammnutzer jeweils für jeden Frequenzwert der FFT des Mietnutzersystems entschieden werden, ob ein Stammnutzer vorhanden ist oder nicht.

#### 4 Modifikation von 802.11a für Spectrum Pooling

Es stellt sich nun die Frage, wie eine Koexistenz zwischen den Stammnutzern, die uneingeschränkte Priorität im Pool haben, und den Mietnutzern, die die freien Frequenzbereiche *eigenmächtig* nutzen, realisiert werden soll. In Abbildung 4.1 sieht man auf der linken Seite den typi-

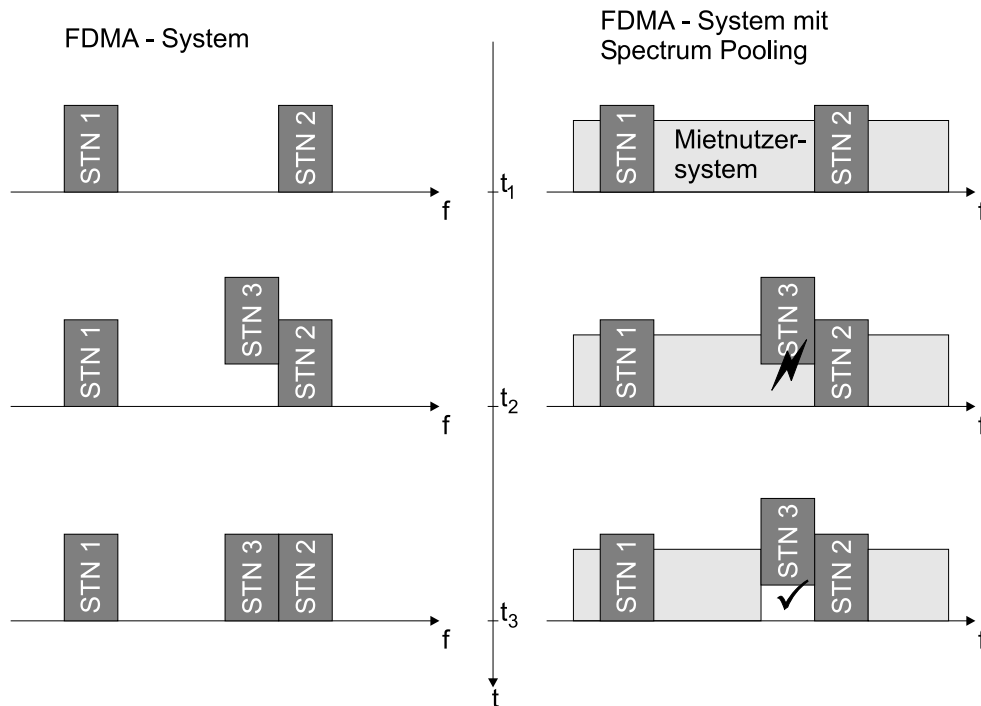


Abbildung 4.1: Koexistenz von Stamm- und Mietnutzern

schen Verlauf von Frequenzbelegungen in einem Stammnutzersystem, das ein FDMA-Verfahren (z.B. ein kanalorientiertes Sprechfunksystem) verwendet. Zum Zeitpunkt  $t_1$  sind zwei Stammnutzer im System. Zum Zeitpunkt  $t_2$  kommt ein weiterer Stammnutzer (STN 3) dazu. Auf der rechten Seite sieht man die vergleichbare Situation mit Spectrum Pooling. Zum Zeitpunkt  $t_1$  füllt das Mietnutzersystem die freien Ressourcen des Stammnutzersystems voll aus. Die frei gelassenen Bandbereiche müssen also erkannt werden. Zum Zeitpunkt  $t_2$  kann jedoch der neu eintretende Stammnutzer seinen Frequenzbereich nicht nutzen, da das Mietnutzersystem diesen Bereich belegt. Es kommt zu einer Kollision. Jetzt muss das Mietnutzersystem sich schnellst möglich aus dem Bereich zurückziehen, auf den der Stammnutzer Anspruch erhebt. Zum Zeitpunkt  $t_3$  ist dies geschehen. Das Mietnutzersystem hat den Bandbereich von STN3 verlassen und dieser kann - wie gewohnt - mit der Übertragung beginnen.

An dem kleinen Beispiel von oben zeigt sich, welche primären Probleme bei dem Einsatz von Spectrum Pooling behandelt werden müssen. Als erstes steht der Aufgabenkomplex der

#### DETEKTION und INFORMATION

Hier dreht sich alles um den Schutz der Stammnutzer. Zunächst wird ein zuverlässiger Mechanismus benötigt, um die Stammnutzer zu erkennen. Sollte diese Detektion von Stammnutzern nicht

zentralisiert organisiert sein, so müssen nach der Detektion die Informationen über die STN gesammelt werden. Der Sammelpunkt (den hier logischerweise der AP übernimmt) muss diese Detektionsinformationen *auswerten*. Die nun generierte Information über den Belegungszustand des Pools muss wiederum *zuverlässig* an alle Teilnehmer des Mietnutzersystems verteilt werden. Sind die freien Bandbereiche geklärt, so ist der nächste Themenbereich die

### SYNCHRONISATION

Synchronisation im Mietnutzersystem wird benötigt, um überhaupt Datenübertragung jeglicher Art zu realisieren. Die Synchronisation muss auch die Produktionsstreuungen und Temperaturschwankungen der Schwingkreise der Sender und Empfänger ausgleichen. Synchronisiert werden müssen verschiedene Dinge. Will man eine Übertragung (wie in dieser Arbeit) mit OFDM bewerkstelligen, so müssen die Rahmenstruktur, die Abtastung, die Phase und Trägerfrequenz äußerst gut synchronisiert sein. OFDM ist z.B. bezüglich des Frequenzversatzes besonders empfindlich. Das liegt an der mathematisch orthogonalen Anordnung der OFDM-Unterträger. Sind die Trägerfrequenzen im Empfänger gegenüber dem Sender auch nur leicht verschoben (z.B. einige Prozent des Trägerabstandes), so ist die Orthogonalität der OFDM-Träger nicht mehr gewährleistet und das SNR degradiert. Zur Durchführung der Synchronisation sind vor allem Phasenregelkreise, Verwürfler und regelbare Oszillatoren im Einsatz. Ausserdem werden spezielle *Präambeln* verwendet, um Synchronisationsaufgaben zu übernehmen.

Zum Schluss zeigt sich noch ein etwas außergewöhnlicher Themenkreis als Quelle einiger Probleme in hier diskutierten Systemen:

### FFT-NEBENEFFEKTE

Das Zusammenleben von Stamm- und Mietnutzersystem soll (wie in Abbildung 4.1) über die Trennung im Frequenzbereich geschehen. Das heisst, dass beide Teilnehmer dafür Sorge tragen müssen, dass sie nicht in die Bandbereiche des anderen Systems hineinstrahlen. Das Mietnutzersystem verwendet OFDM. Bei OFDM wird das Zeitsignal für die Übertragung durch eine IFFT und Zeitfensterung hergestellt. Somit haben die Fouriertransformierten der OFDM-Unterträger jeweils eine  $\frac{\sin(x)}{x}$ -Struktur. Das heisst, dass jeder dieser Träger Leistung über die gesamte Poolbreite verstreut. Daraus entsteht natürlich ein unerwünschtes Störsignal für die Stammnutzer. Im Empfänger des MTN-Systems passiert etwas Ähnliches. Die streng bandbegrenzten Zugriffe einzelner Stammnutzer werden durch die Zeitfensterung und FFT im Empfänger nicht vollständig richtig dargestellt. Der Erwartungswert des Periodogramms eines Stammnutzers wird hier von Bedeutung sein.

## 4.1 Detektion und Information

Wie schon in Kapitel 2.1 angesprochen, ist die Erkennung der Stammnutzer von herausragender Wichtigkeit. Wenn es keine informelle Kommunikation zwischen MTN und STN geben soll, so muss das MTN-System alleine in der Lage sein, die STN stets zuverlässig und schnell zu erkennen und diese Informationen innerhalb des MTN-System ebenfalls schnell und zuverlässig

#### 4 Modifikation von 802.11a für Spectrum Pooling

zu verteilen. Die Detektion von Stammnutzern wird über eine Leistungsmessung realisiert. Es müssen im Mietnutzersystem periodische Sendepausen eingehalten werden, in denen auf allen Frequenzbändern im Pool Leistungsmessungen durchgeführt werden. Sollte auf einem Frequenzband eine Leistung gemessen werden, die oberhalb einer festgelegten Schwelle liegt, so wird dies als Anwesenheit eines Stammnutzers interpretiert. Die An- oder Abwesenheit von Stammnutzern auf verschiedenen Frequenzen wird als *Belegung* bezeichnet. Der erste Schritt zur *Detektion und Information* ist also die Messung der Stammnutzer. Hierzu wird die FFT im Empfänger eingesetzt: Einige OFDM-Symbole lang werden Abtastwerte des Signals an der Antenne gewonnen. Die FFT im Empfänger macht aus der Anzahl von zeitlichen Abtastwerten für ein OFDM-Symbol dann Signalpunkte im Frequenzbereich. Betrachtet man nun die FFT-Werte auf einer Frequenz über mehrere OFDM-Symbole, so bekommt man zeitlich hintereinander Abtastwerte auf einzelnen Frequenzen. Diese sind nun Abtastwerte der potentiell vorhandenen Stammnutzer auf den jeweiligen Frequenzen. Um mit diesen Abtastwerten nun auf jeder einzelnen Frequenz eine Entscheidung fällen zu können, ob ein Stammnutzer da ist oder nicht, wird eine Schwellendetektion eingesetzt.

Die komplexen Abtastwerte nimmt man in ihren Komponenten als normalverteilt an, und somit ist die Amplitude nach [JON99, S.33] rayleigh-verteilt. Eine detaillierte Betrachtung zur mathematischen Modellierung ist in [HIL02] zu finden. Das Einstellen der Schwelle ist besonders durch das Abwägen zwischen Fehlalarmen und Entdeckungswahrscheinlichkeit charakterisiert. Wird die Schwelle sehr niedrig gesetzt, also bei kleinen Leistungen schon auf einen Stammnutzer geschlossen, so ist zwar die Entdeckung der Stammnutzer sehr sicher, aber die Quote der Fehlalarme steigt auch. Das bedeutet für den Stammnutzer eine zuverlässige Erkennung, was sehr wünschenswert ist. Das Mietnutzersystem muss allerdings dann mit den häufigen Fehlalarmen kämpfen, die eine unnötige Blockade von eigentlich freien Frequenzen bedeutet. Um die Detektion von Stammnutzern so sicher wie möglich zu machen, wird ein räumlicher Diversity-Ansatz gewählt. Dies ist wie folgt zu verstehen:

Wenn nur eine Station die Erkennung der Stammnutzer übernimmt, so ist es durchaus möglich, dass ungünstige räumliche Konstellationen der beteiligten Sender und Empfänger dazu führen, dass Stammnutzer nicht erkannt werden. Die zwei häufigsten Fälle (Fading, große Entfernung) sind auf Abbildung 4.2 zu sehen. Wenn hier nur der AP die Detektion übernimmt, so kann er z.B. die Stammnutzer-Station STN1 nicht erkennen, weil diese zu weit entfernt ist. Da sie aber zur Mietnutzer-Station STA1 relativ nahe ist, muß sie erkannt werden und ihr Frequenzbereich im Mietnutzersystem ausgespart werden. STN2 hingegen ist zwar nahe genug am AP, was eine Detektion ermöglichen würde, aber durch Multipath-Fading kann der AP sie nicht erkennen.

Es liegt also nahe, die Detektion der Stammnutzer nicht nur von einer zentralen Station aus zu vollziehen, sondern einfach alle STAen des Mietnutzersystems mit einzubeziehen. Abbildung 4.2 zeigt dies. STA1 ist näher an STN1 als der AP, und hat somit auf dem Frequenzbereich von STN1 eine höhere Empfangsleistung. STA1 kann also diesen Stammnutzer detektieren und diese Detektion anschließend dem AP mitteilen. Genauso verhält es sich mit STN2. Der AP hat leider einen Fading-Einbruch auf dem Kanal von STN2. Da aber STA2 und STA3 den STN2 „gehört“ haben, ist die Detektion gesichert.

Da die Stammnutzer ihre Anwesenheit mit der Zeit ändern, ist eine periodische Messphase zur Detektion notwendig. Der AP leitet diese Detektion mit einem speziellen Management-Rahmen

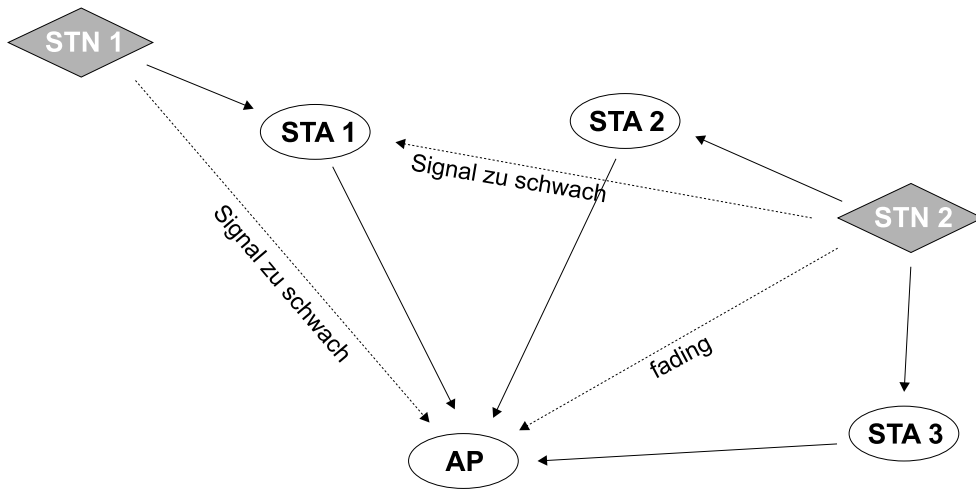


Abbildung 4.2: Typische Problemfälle bei der Detektion

ein. Dieser ist in Abbildung 4.3 zu sehen. Damit die Detektion nicht verzögert wird, kann der

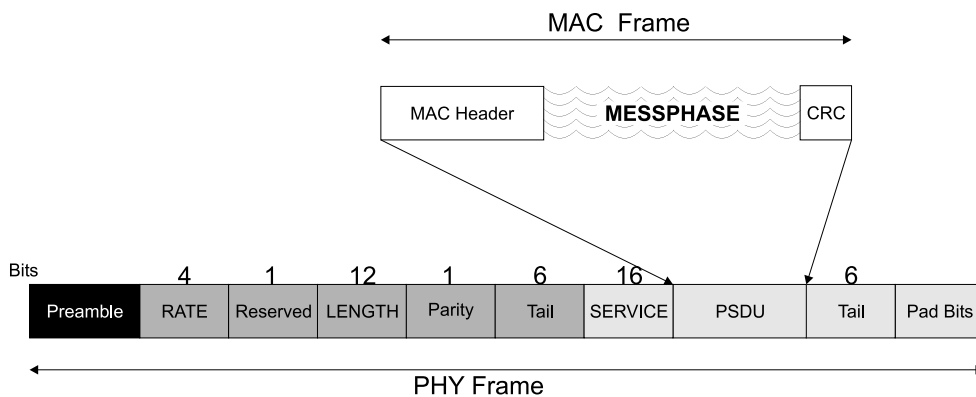


Abbildung 4.3: Detektionsrahmen

AP sich die Priorität dieses Rahmens im Zugriffsmechanismus von 802.11 mit Hilfe eines PIFS holen. Im Type- und Subtype-Feld wird dieser Rahmen als *Detektionsrahmen* spezifiziert. Dieser Rahmen enthält keine Daten (auch keine „0“!), aber die Länge, die für die Detektion nötig ist. Die Empfängerstationen empfangen also diesen MAC-Rahmen, und im Datenteil sendet der AP *keine* Daten, womit die Empfängerstationen automatisch das Umgebungsrauschen bzw. vorhandene Stammnutzer als Nutzdaten empfangen, diese werden dann der Schwellendetektion für Stammnutzer unterworfen. Jede STA ermittelt so während dieses Detektionrahmens die aktuelle Belegung und erstellt einen individuellen *Belegungsvektor* (BV). In diesem Belegungsvektor spiegelt sich der aktuelle Belegungszustand des Pools wider. In Abbildung 4.4 ist ein solcher Belegungsvektor zu sehen. Ist die Zugriffsbreite der STN größer als die eines Unterträgerabstandes (so wie auch in diesem Beispiel), so kann ein *komprimierter* Belegungsvektor verwendet



## 4.1.1 Boosting

Ziel ist es zunächst, die Messergebnisse der beteiligten Stationen zu sammeln. Damit auch bei schwacher Zellenbesetzung eine gute Abdeckung mit Messungen funktioniert, werden zusätzlich zu den STAen noch *Boosting-Stationen* eingesetzt, die nur für die Messung der Stammnutzer verwendet werden. Die Messphase wird stets durch den AP initiiert. Dieser sendet den Detektionsrahmen und daraufhin führen alle Stationen aus diesem System im Datenteil dieses Rahmens die Messung durch, indem sie im Datenteil des Rahmens einfach Abtastwerte nehmen, und diese dann blockweise einer FFT unterziehen. Nachdem mehrere solcher Blöcke transformiert wurden, hat man für jeden FFT-Frequenzwert Abtastwerte im Frequenzbereich, die man dann einer Schwellenentscheidung unterziehen kann. Es wird also im Mietnutzersystem stets für jeden einzelnen OFDM-Unterträger entschieden, ob er verwendet werden darf oder nicht.

Das Boosting wird zeitlich auch in den Detektionsrahmen nach der Messung eingebettet. Das ermöglicht eine leichte *Abwärtskompatibilität* zu alten Geräten. Sollen neue Spectrum Pooling-Geräte auf 802.11a Basis an einem herkömmlichen 802.11a-Netz teilnehmen, so sind überhaupt keine wesentlichen Modifikationen nötig, um auf die alte Struktur zurückzuschalten. Der Detektionsrahmen würde im Falle des alten 802.11-Netzes von der MAC-Schicht des AP einfach nicht verschickt, und deshalb wären dann auch alle weiteren Mechanismen für Spectrum Pooling nicht aktiv.

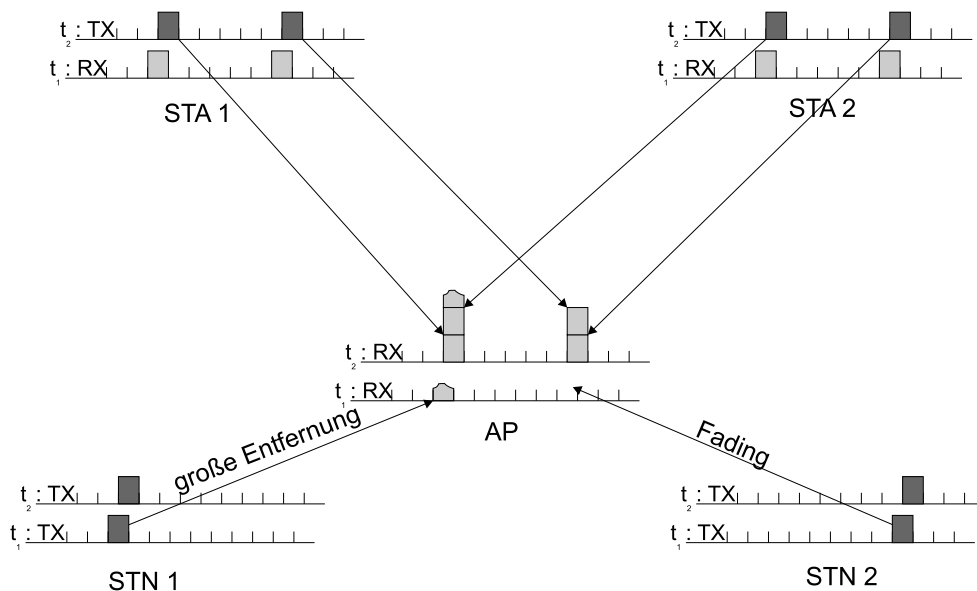


Abbildung 4.5: Boosting neuer Stammnutzer

## 4 Modifikation von 802.11a für Spectrum Pooling

### Die Boosting-Phase

Die Messung beginnt in Abbildung 4.5 zum Zeitpunkt  $t_1$ : Die beiden Stammnutzer STN1 und STN2 senden eifrig weiter, während alle Stationen im Mietnutzersystem (auch der AP) die Messung durchführen. Zur Zeit  $t_2$  ist die Messung beendet, die STAen im System sowie auch (falls vorhanden) die Boosting-STAen werten nun ihre Abtastwerte aus, und entscheiden, ob auf den einzelnen Kanälen Stammnutzer sind oder nicht. Diese Entscheidungen werden in einem neuen BV zusammengefasst. Der Vergleich mit dem *noch gültigen*, alten BV zeigt, wo seit der letzten Messung neue Stammnutzer im Band aufgetreten sind. Im Beispiel auf Abbildung 4.5 sind beide STN neu dazugekommen. Als Nächstes wird ausschließlich auf den Frequenzen, auf denen die einzelnen Stationen neue Stammnutzer detektiert haben, das Boosting-Signal gesendet. Es ist ein einfaches Jam-Signal ohne sinnvollen Inhalt. Es sorgt nur dafür, dass der AP in der zweiten Messphase die neuen Stammnutzer besser erkennt, weil ja nun auf den Bändern der neuen Stammnutzer zusätzliche Leistung von den Stationen im Mietnutzersystem empfangen wird. Wie man in Abbildung 4.5 sieht, konnte der AP den STN2 in der ersten Messphase aufgrund von Fading überhaupt nicht erkennen. STN1 hat er auch auf Grund der großen Entfernung nur schlecht detektieren können. In der zweiten Messphase sieht das schon ganz anders aus. Die STN senden weiter und die STA, die diese erkannt haben, senden ebenfalls. So akkumuliert sich die Leistung im Empfänger des AP. STN2, der vorher vom AP gar nicht gesehen wurde, wird in der zweiten Messphase von STA2 und STA1 geboostet. Der AP empfängt also ein verstärktes Signal, und durch die verteilte Sendung aus verschiedenen Richtungen wird das Problem des Multipath Fading umgangen.

Das Boosting mit Jam-Signalen hat im Hinblick auf den gewollten Effekt der Messverteilung einen entscheidenden Vorteil gegenüber allen Verfahren, die sich an *Datenübertragung* orientieren: Der AP, der eigentlich nichts weiter als eine oder-Verknüpfung der BVs der verschiedenen STAen durchführt, bekommt diese Verknüpfung durch die zeitgleiche Überlagerung der Jam-Signale schon im Empfangssignal präsentiert. Somit ist klar, dass hier viel Übertragungszeit gespart werden kann. Bei einer Übertragung der BVs der einzelnen Stationen an den AP müssten diese nämlich hintereinander gesendet werden. Da sie aber im Anschluss sowieso oder-verknüpft würden, kann das Boosting-Konzept hier ansetzen.

Durch dieses Boosting ergibt sich aber auch ein Nachteil. Da die STAen auf den STN-Frequenzen das Boosting-Signal senden, werden diese natürlich gestört, und das auch noch massiv, da ja viele STAen dieses Boosting zur gleichen Zeit durchführen. Nun muss man sich aber auch vor Augen führen, dass ein STN im schlimmsten Fall noch viel längeren Störungen ausgesetzt ist. Sollte er nämlich direkt nach der letzten Messphase in das System getreten sein, so wird er ja erst im nächsten Detektionsrahmen erkannt. Die Zeitdauer zwischen zwei Messungen ergibt also die Worst Case-Stördauer  $t_{coll,max}$ , die ein STN verkraften muss. Diese muss beim Systemdesign des Mietnutzersystems mit Hilfe der Detektionsrahmenperiode auf die Stammnutzer abgestimmt werden. Die zusätzliche Dauer der Boosting-Phase (einige OFDM-Symbole à  $4\mu s$ ) ist im Vergleich zur Zeitdauer zwischen zwei Messungen (typischerweise 1-2  $ms$ ) vernachlässigbar. Es entstehen den Stammnutzern durch das Boosting also in Zeitrichtung keine nennenswerten, zusätzlichen Störungen. Anders sieht es in Amplitudenrichtung aus. Da im Gegensatz zur Datenübertragung, wo stets nur eine Station sendet, hier *alle* Stationen senden, akkumuliert sich die

Leistung nicht nur im AP, wo dies ja gewollt ist, sondern natürlich auch bei den Stammnutzern. Es muss also genau abgestimmt werden, mit welcher Leistung das Boosting stattfinden soll. Dies wird abhängig von der Anzahl der STAen im Mietnutzersystem sein.

### Die Mapping-Phase

Nun sind aber nicht nur neu dazugekommene STN von Interesse, sondern auch die, die schon in der letzten Messphase erkannt worden waren. Würde man hier genauso verfahren und schlicht mit Hilfe des Boosting die Stammnutzer signalisieren, so würde dies zwar genauso gut wie bei den neu dazugekommenen STN funktionieren, hätte aber einen nicht akzeptablen Nachteil: Die STN würden nicht nur einmal - nämlich bis zur ihrer Detektion - gestört, sondern auch danach immer wieder periodisch in jeder Messphase. Dieses bewusste, periodische Stören muss umgangen werden. Dennoch soll aber auf die Vorteile vom Boosting nicht verzichtet werden. Also muss das Boosting für die „alten“ STN eben nur auf den Trägern des Mietnutzersystems stattfinden. Dafür muss jedem OFDM-Träger ein Boosting-Platz zugewiesen werden. Da im Normalfall weniger Träger für das Mietnutzersystem frei sind, als es insgesamt Träger im Pool gibt, muss für diese zweite Boosting-Phase eventuell mehr Zeit verwendet werden. Der logische Aufbau im

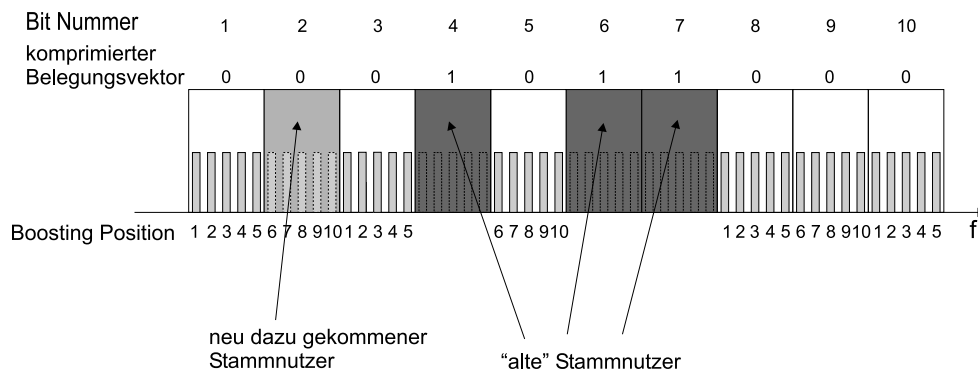


Abbildung 4.6: Mapping in der zweiten Boosting-Phase

Frequenzbereich ist in Abbildung 4.6 zu sehen. Die Bits des Belegungsvektors werden nummeriert, und anschließend werden innerhalb des Pools Positionen ausgewählt, auf denen das Boosting für die „alten“ Stammnutzer stattfindet. Dies wird als *Mapping* bezeichnet. Hierfür werden nur die aktuell gültigen Mietnutzerträger verwendet. Es ist also der letzte Belegungsvektor immer noch verbindlich! Eine Station, die zum Beispiel den Stammnutzer auf der Position 4 immer noch sieht, wird in dieser zweiten Boosting-Phase auf denjenigen Trägern das Jam-Signal senden, die mit der Boosting-Position 4 bezeichnet sind. Der AP wird während dieser zweiten Phase dann entscheiden können, ob ein Frequenzband wieder frei gegeben werden kann oder nicht. Nun gibt es für diese Boosting-Phase allerdings wieder einige Komplikationen. Wenn, wie in Abbildung 4.6, ein neuer Stammnutzer einige Boosting-Positionen durch seine Anwesenheit überdeckt, so kann der AP hier nicht die richtige Entscheidung treffen, ob ein Jam-Signal da ist oder nicht. Er wird im Zweifel entscheiden, dass ein Signal da ist, weil er ja die Leistung des Stammnutzers

#### 4 Modifikation von 802.11a für Spectrum Pooling

dort sieht. Um dieses Problem zu umgehen, gibt es mehrere Ansätze. Zunächst weiß der AP schon aus der ersten Boosting-Phase, dass dort ein neuer Stammnutzer ist, und kann deshalb in der zweiten Phase die Messergebnisse dort als unzuverlässig einstufen. In diesem Beispiel wäre das das erste Auftreten der Boosting-Positionen sechs bis zehn. Sollte der Pool relativ „gutmütig“ sein, dann tauchen die Boosting-Positionen aber - wie auch im Beispiel hier - mehrfach auf. Der AP kann sich dann also auf ein Messergebnis in einem anderen Bereich verlassen. Sollten sehr viele Positionen mit neuen Stammnutzern belegt sein, so kann ein Boosting auf diesen Positionen nicht erfolgreich durchgeführt werden. Das ist aber für das Mietnutzersystem kein allzu schlimmes Ereignis. Schlimmstenfalls sind einige Boosting-Positionen immer mit neuen Stammnutzern überdeckt. Der AP wird also stets Leistung auf diesen Frequenzen messen und glauben, dass Jam-Signale gesendet wurden. Er wird also die entsprechenden Stammnutzerbereiche nicht frei geben. Somit ist zumindest ein voreiliges Übernehmen von Stammnutzerfrequenzen ausgeschlossen. In der nächsten Mapping-Phase sind dann die jetzt neuen Stammnutzer Teil des Belegungsvektors und somit ergeben sich keine Probleme beim Mapping, es sei denn, es sind wieder ungewöhnlich viele Stammnutzer zusätzlich eingetreten. Da aber mit so schnellen und häufigen Veränderungen auf Stammnutzerseite nicht gerechnet wird, ist dies eine akzeptable Lösung. Ein anderes Problem ergibt sich, wenn der Belegungsvektor sehr lang ist, und der Pool voller Stammnutzer ist, so dass es gar nicht genug gültige Träger im Pool gibt, die für die Durchnummerierung als Boosting-Positionen vorhanden wären. Dann wird das Mapping mehrmals hintereinander wiederholt, und die Nummerierungen werden fortgesetzt.

##### 4.1.2 Broadcast mit dem Zeit-Frequenzverfahren

Nach diesen Zeitabschnitten der Messung, des Boosting und Mapping sollte der AP über die aktuelle Belegung im Pool informiert sein. Nun ist es seine Aufgabe, über den neuen Belegungsvektor zu entscheiden, und ihn anschließend an alle STAen im Mietnutzersystem zu verteilen. Hierfür kann Boosting nicht eingesetzt werden, da z.B. aufgrund von Multipath-Fading keine gesicherte Übertragung zwischen AP und STAen auf jeder Frequenz existiert. Außerdem ist es von großer Wichtigkeit, dass alle STAen im System stets über denselben BV informiert sind, da sonst entweder Stammnutzer gestört werden, oder die Datenübertragung nicht funktioniert. Der AP muss also eine Übertragung dieser Information wählen, die sehr zuverlässig und schnell ist. Als Basis für die Auswahl, welche Frequenzbereiche für diese Übertragung eine Rolle spielt, kann nur der letzte BV dienen. Dies ist die einzige Information, die garantiert alle STAen im System haben. Die vorangegangenen Messungen, die alle STAen gemacht haben, ist ja für jede einzelne STA nicht vollständig, da man nicht sicher sein kann, dass jede STA jeden STN sieht (deshalb gibt es ja das Boosting und Mapping!). Nun wäre es denkbar, den Belegungsvektor einfach in ein Paket zu betten, und dieses mit einer sehr guten Fehlerkorrektur, also einer extrem hohen Redundanz, auf der alten Belegung zu verschicken. Sollte jedoch die Zugriffsbreite der Stammnutzer sehr groß sein, so gibt es Schwierigkeiten mit der Kanalcodierung. Ein Pool mit 64 OFDM-Trägern und STN-Zugriffsbreite von 8 Trägern und einer Stammnutzerbelegungsänderung von 4 nach 5 Stammnutzern würde eine Bitfehlerrate von 0.125 bedeuten. Bei schlechteren Konstellationen kann es noch schlimmer werden. Hier stellt sich die Frage, welche sinnvolle Kanalcodierung eine so miserable Fehlerrate auffangen soll. Die Übertragung würde in jedem Fall

extrem lange dauern. Das Übertragungsverfahren muss also an die speziellen Voraussetzungen ausgerichtet und für minimale Übertragungszeit entworfen werden. Das Verfahren ist in Abbil-

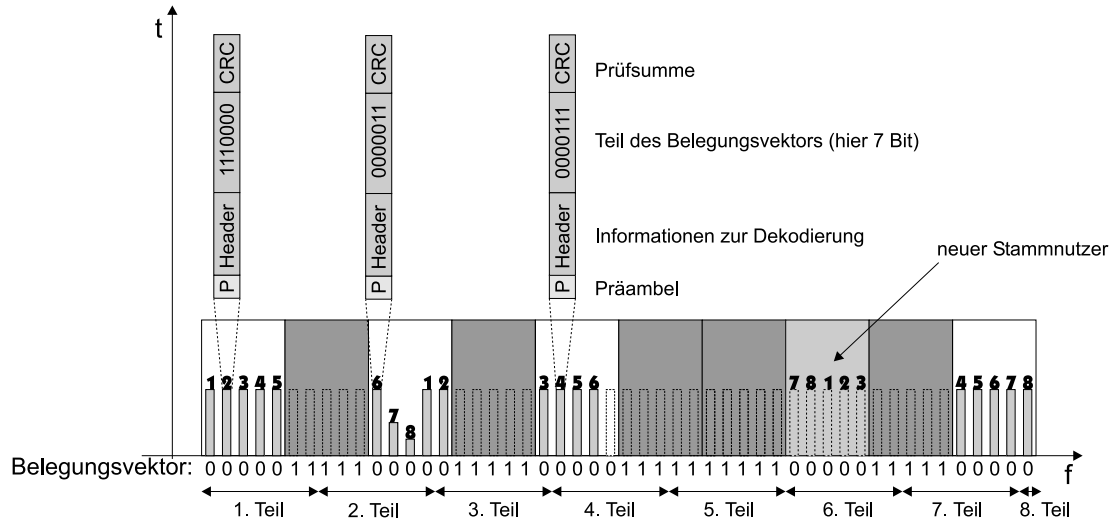


Abbildung 4.7: Broadcast-Verfahren für den Belegungsvektor

dung 4.7 zu sehen. Zunächst wird der Belegungsvektor in Teile zerschnitten. Diese Teile bilden jeweils mit einem sie umgebenden Rahmen aus Decodierungsinformation und Prüfsumme einzelne Pakete. In diesem Beispiel ergeben sich also aus den acht Teilen des BV acht Pakete, die nun gesendet werden. Dafür wird jedes einzelne Paket auf nur einem OFDM-Träger in Zeitrichtung seriell verschickt. Dabei wird es mit Rate 1/2 und *BPSK* übertragen. Jedes Paket wird außerdem nicht nur auf einem Träger, sondern stets auf mindestens 3 Trägern redundant wiederholt. Die Zahlen auf den OFDM-Trägern in Abbildung 4.7 geben an, welcher Teil des BV auf welchem Träger verschickt wird. Das dreifache Verschicken bringt Sicherheit, dass ein Empfänger auch sämtliche Teile des BV zusammensammeln kann. Sollte er z.B. auf einem Kanal Fading-Einbrüche haben, so hat er noch an zwei anderen Stellen die Chance, eben dieses Paket zu bekommen. Genauso können neue Stammmutzer die Übertragung stören, da auch hier immer noch der alte BV verbindlich ist. Hier kann der AP jedoch schon darauf achten, die redundanten Pakete so zu positionieren, dass sie nicht mehrfach in neue Stammmutzer fallen. Da die Pakete ja eine laufende, individuelle Nummer enthalten, ist ihre Position im Pool beliebig. Sie sind in sich stets eindeutig identifizierbar. Da jedes Paket auf nur einem Träger verschickt wird, ist eine Decodierung dieser Sendung auch *ohne* gültigen BV möglich. Dazu muss nur einfach auf allen Trägern die Information decodiert werden. Diejenigen Träger, auf denen keine Pakete kamen, werden daran erkannt, dass der Faltungsdecoder Fehler meldet oder der CRC nicht stimmen wird. Dies ist vor allem für neu in das System tretende Stationen wichtig. Denn sie besitzen ja den letzten, gültigen BV nicht. Eine Schwierigkeit ist hier allerdings, die Präambel für diese Pakete so zu wählen, dass sie auch ohne Kenntnis des BV funktioniert. In Kapitel 4.2 wird darauf genau eingegangen.

Es bleiben noch einige Parameter offen, die optimiert werden können, um die Übertragung so

#### 4 Modifikation von 802.11a für Spectrum Pooling

schnell wie möglich zu machen. Es ist z.B. unklar, wie viele Teile der BV idealerweise haben sollte. Es ist auch unklar, ob eine feste Anzahl von Teilen oder eine flexible besser ist. Es gibt aber auch feste Randbedingungen, die hier vorgegeben werden sollen, um die Berechnungen für den idealen Aufbau dieser Signalisierung zu begrenzen. So muss ein Pool stets mindestens 16 freie Träger besitzen, ansonsten wird er nicht weiter für Spectrum Pooling verwendet. Genauso ist jedes Paket mindestens auf 3 Trägern zu senden. Der CRC wird hier stets mindestens 1/4 der Länge der Infodaten haben. Es sind natürlich (besonders für sehr kurze Pakete) auch andere Blockcodes anstelle des CRC denkbar. Ein Rechenbeispiel zeigt die Berechnung der Länge dieser Pakete bei fester Anzahl von Teilen des BV:

- Es wird ein Pool der Breite 64 Träger angenommen, die Stammnutzer greifen stets auf 2 Träger zu. Somit ist der komprimierte BV  $32\text{Bit}$  lang.
- Da dreifache Versendung erwünscht ist, sind also im *besten Fall*  $64/3 = 21,33$  also 21 Träger für die Übertragung vorhanden.
- Im *schlechtesten* Fall wären es die immer vorhandenen 16 Träger, also  $(16/3 = 5,33)$  5 Träger.
- Bei 5 Trägern und einer festen Anzahl an Teilen für den BV ergeben sich also  $3\text{Bit}$  für die Bezeichnung des Teils, dann  $32/5 = 6,4$ , also  $7\text{Bit}$  in jedem Teil des BV. Mit  $3\text{Bit}$  CRC sind das  $13\text{Bit}$ .

Soll die Anzahl der Teile des BV flexibel gehalten werden, so ergibt sich folgende Rechnung:

- Bei einer flexiblen Aufteilung muss neben der Nummer, die den Teil des BV angibt, jedes Paket noch die Zahl beinhalten, die angibt, wie viele Teile des BV gebildet wurden.
- Erlaubt man eine Aufteilung in bis zu 8 Teile, so wird für die Nummerierung  $6\text{Bit}$  benötigt. (3 für die Zahl, wie viele Teile des BV es sind, und 3 für die laufende Nummer, welcher Teil des BV gerade gemeint ist).
- Ist der Pools völlig frei, so ergeben sich wieder 21 nutzbare Träger. Teilt man den BV dann in 8 Teile, so ist jeder Teil noch  $32/8 = 4\text{Bit}$  lang. Der CRC ist dann auf 3 Bit zu wählen. Zusammen sind das  $6 + 4 + 3 = 13\text{Bit}$ .
- Ist der Pools maximal belegt, so ist die Sendung - wie schon oben berechnet - auf 5 Trägern zu vollziehen. Es ist also eine Zerlegung in nur maximal 5 Teile möglich.  $32/5 = 6,4$ , also 7 Bit. Der CRC ist dann 4 Bit lang. Die Gesamtlänge ist jetzt  $6 + 7 + 4 = 17\text{Bit}$ .

Man sieht also schon an diesem Beispiel, dass eine flexible Unterteilung zwar auf den ersten Blick interessant scheint, aber - besonders dann, wenn die Zugriffsbreite der Stammnutzer groß ist - keine Vorteile bringt.

Tabelle 4.1 soll einen Überblick verschaffen, warum die Entscheidung für eine fixe Aufteilung sinnvoll ist. Die Vorteile, die eine flexible Aufteilung bringt, sind nur in den Konstellationen zu finden, in denen die Poolbreite im Vergleich zur Stammnutzerbreite relativ hoch ist. Stammnutzerzugriffe der Breite von einem oder zwei OFDM-Trägers sind kritisch. Dies wird in Kapitel 4.4 aufgedeckt werden. Deshalb fällt die Entscheidung für weitere Betrachtungen zur Vereinfachung für die fixe Aufteilung in 5 Teile. Die daraus resultierenden Übertragungszeiten sind in Tabelle 4.2 zu sehen. Es muss jedoch generell beim Systementwurf neu entschieden werden, was

Poolbreite - STNbreite	64-1	64-2	64-4	128-1	128-2	128-4
feste Teilung in 4 Teile	23	13	9	43	23	13
feste Teilung in 5 Teile	20	13	9	37	20	13
Teilung in bis zu 8 Teile/Pool frei	12	13	10	27	18	13
Teilung in bis zu 8 Teile/Pool voll	24	17	13	40	24	17
Teilung in bis zu 16 Teile/Pool frei	15	13	12	20	15	13
Teilung in bis zu 16 Teile/Pool voll	27	19	15	43	25	19

Tabelle 4.1: Länge der Pakete in Bit für die Übertragung des BV im Zeit-Frequenzverfahren

das sinnvollste Verfahren ist. Ist z.B. der Pool stets wenig von Stammnutzern belastet, kann man damit rechnen, dass die Worst Case-Längen für volle Pools selten oder nie erreicht werden. Dann ist es natürlich schon sinnvoll, eine flexible Aufteilung zu wählen, da sie gerade bei großen Pools die Übertragung erheblich beschleunigen kann.

Hat der AP dann mit diesem Verfahren den neuen Belegungsvektor verschickt, ist ab diesem Zeitpunkt der neue Belegungsvektor gültig. Damit jede Station noch einmal überprüfen kann, ob die Übertragung des BV an sie vollständig gelungen ist, nimmt sich der AP nach der Übertragung mit dem Zeit-Frequenz-Verfahren noch einmal die Priorität im Zugriffsverfahren und verschickt einen besonders kurzen Beacon-Rahmen, der auch den neuen BV im Datenteil enthält. Alle Stationen, die dieses Beacon empfangen konnten und deren aktueller Wissensstand über die Belegung genau dem BV in diesem Beacon entspricht, dürfen weiter am Datenverkehr teilnehmen.

Poolbreite - STNbreite	64-1	64-2	64-4	128-1	128-2	128-4
feste Teilung in 5 Teile	160	104	81	296	160	104

Tabelle 4.2: Länge der Pakete in  $\mu s$  für die Übertragung des BV im Zeit-Frequenzverfahren

## 4.2 Synchronisation

Die Synchronisation ist in einem OFDM-System von großer Bedeutung. Ohne gute Synchronisation ist eine Datenübertragung nicht möglich. Die wichtigsten Aufgaben der Synchronisation sind:

1. Synchronisation des Symbolbeginns bzw. Rahmenbeginns
2. Korrektur des Trägerfrequenzversatzes zwischen Sender und Empfänger
3. Synchronisation des Abtasttaktes
4. Synchronisation der Trägerphase

Die Synchronisation des Abtasttaktes ist eine bekannte Aufgabe aus der Datenübertragung. Hierfür kommen Taktregelkreise und Taktrückgewinnungsverfahren zum Einsatz. Eine wichtige Rolle hierfür spielt der Verwürfler im Sender. Auch die Synchronisation der Trägerphase ist in der Datenübertragung eine häufige Aufgabe. Bei digitaler Übertragung können die bekannten Signalraumkonstellationen die Regelung für die Phase unterstützen. Der 802.11a Standard sieht vor, für die Phasenkorrektur ausschließlich die Pilote einzusetzen. Auf diese zwei Synchronisationsprobleme soll hier nicht weiter eingegangen werden. Stattdessen sollen Rahmenbeginn und Trägerfrequenzoffset als die zentralen Probleme untersucht werden. Blickt man zurück auf das Systemdesign von 802.11a, so werden diese Aufgaben dort vollständig auf den Einsatz von dafür zurechtgelegten Präambeln zurückgeführt. Daher ist es naheliegend, auch in einem Spectrum Pooling-System diese Aufgaben mit Präambeln zu lösen. In 802.11a ist der Ablauf dieser Synchronisationen relativ klar. Wie schon in Abschnitt 3.5.3 erklärt wurde, besteht die Präambel aus 10 kurzen gefolgt von 2 langen Trainingssymbolen. Durch die Autokorrelation des Empfangssignals mit einem verzögerten Empfangssignal kann der Rahmenanfang gefunden werden. Diese Autokorrelation wird nämlich in der Präambel große Werte haben, da aufeinanderfolgende, identische Symbole miteinander korreliert werden. Es wird also für die Suche nach den Rahmenanfang der Betrag der Korrelationssumme gebildet und dann eine Maximumsuche durchgeführt. In [ALM01] wird neben dem Betrag auch die Phase der Korrelationssumme herangezogen. Dies ist aber für den Fall von Spectrum Pooling - wie Simulationen gezeigt haben - nicht einsetzbar, da bei den schlechten SNR, die zu erwarten sind, keine gute Phasenberechnung möglich ist. Die Abtastwerte sind durch einen Frequenzversatz moduliert, wobei es egal ist, ob dieser vom Sender oder Empfänger stammt. Es dreht sich nur um die Gleichlaufdifferenz  $\Delta f_c$ ! Die Phase der Abtastwerte  $y(k)$  im Empfänger nimmt durch den Frequenzversatz ständig zu:

$$y(k) = x(k) \cdot e^{j2\pi\Delta f_c T_A k}$$

Die Korrelationssumme mit dem gleichen, zeitverzögerten Signal ist:

$$\begin{aligned} KS &= \sum_{k=0}^{N-1} y(k) \cdot y^*(k+N) \\ &= \sum_{k=0}^{N-1} x(k) \cdot e^{j2\pi\Delta f_c T_A k} \cdot x(k) \cdot e^{-j2\pi\Delta f_c T_A (k+N)} \end{aligned} \quad (4.1)$$

$$\begin{aligned}
&= \sum_{k=0}^{N-1} |x(k)|^2 \cdot e^{j2\pi\Delta f_c T_A k} \cdot e^{-j2\pi\Delta f_c T_A k} \cdot e^{-j2\pi\Delta f_c T_A N} \\
&= e^{-j2\pi\Delta f_c T} \sum_{k=0}^{N-1} |x(k)|^2
\end{aligned} \tag{4.2}$$

$T = NT_A$  ist die Dauer der Korrelation. Es läßt sich nun der Frequenzversatz ausrechnen:

$$\Delta f_c = \frac{1}{2\pi T} \arg\left\{ \frac{KS^*}{|KS|} \right\} \tag{4.3}$$

Nun ist es klar, dass mit Hilfe dieser Formel keine Frequenzversätze ausgerechnet werden können, die mehr als einen halben Trägerabstand betragen. Die Berechnung des Winkels am Schluss ist ja  $2\pi$  periodisch und kann somit nur Werte zwischen  $-\pi$  und  $\pi$  zurückliefern. Deshalb hat 802.11a die zehn kurzen Trainingssymbole vorgesehen. Hier ist die Periodizität des Signals ein Viertel der FFT-Länge ( $64/4=16$  Abtastwerte) und somit wird aus der Korrelationssumme:

$$KS_{1/4} = \sum_{k=0}^{N/4-1} y(k) \cdot y^*(k + N/4) = e^{-j2\pi\Delta f_c T \cdot \frac{1}{4}} \sum_{k=0}^{N/4-1} |x(k)|^2 \tag{4.4}$$

und somit aus der Berechnung für den Versatz:

$$\Delta f_c = \frac{4}{2\pi T} \arg\left\{ \frac{KS_{1/4}^*}{|KS_{1/4}|} \right\} \tag{4.5}$$

Durch die 4 im Zähler können jetzt also größere Frequenzversätze berechnet werden. Man muss allerdings auch sehen, dass dieser Wert aus einer Korrelation von nur 16 Werten stammt, und deshalb nicht sonderlich genau ist. Mit einem Rundungstrick [OFD00] kann man die beiden Ergebnisse zu einem Schätzwert kombinieren:

$$\Delta f_c = \frac{1}{T} \left[ \frac{4}{2\pi} \arg\left\{ \frac{KS_{1/4}^*}{|KS_{1/4}|} \right\} \right] + \frac{1}{2\pi T} \arg\left\{ \frac{KS^*}{|KS|} \right\} \tag{4.6}$$

Will man dieses einfache mathematische Modell auf Spectrum Pooling übertragen, so stößt man zunächst auf ein Hindernis. Es wird nämlich in einem solchen System nicht immer möglich sein, die kurzen Trainingssymbole zu senden. Eine Verkürzung der Zeitdauer auf  $1/4$  der ursprünglichen Länge bedeutet eine Verringerung der Frequenzauflösung ebenfalls auf  $1/4$ . Es hat also nur noch jeder vierte OFDM-Träger einen Modulationswert ungleich Null. Aufgrund der geringen Zahl von gültigen Trägern und der nicht vorhersehbaren Verteilung der Stammnutzer, kann es nicht garantiert werden, dass dieses Signal überhaupt erzeugt werden kann. Es müssen schliesslich die Träger, auf denen Stammnutzer präsent sind, ausgespart werden. Wenn von diesen 16 dann auch noch einige wegfallen, ist eine Korrelation nicht mehr sinnvoll.

Das Verfahren der kurzen Symbole muss also durch ein anderes ersetzt werden. Deshalb zunächst einige grundlegende Feststellungen:

In Spectrum Pooling-Mietnutzersystemen, denen 802.11a zugrunde liegt, hat der AP eine besondere Stellung. Im Gegensatz zu dem Kommunikationsverlauf in LANs, wo 802.11a normalerweise eingesetzt wird, ist dieser bei Spectrum Pooling typischerweise ein anderer. In Spectrum Pooling Systemen, die z.B. Mobilkommunikation oder mobile Anschlüsse an Datennetzen



der Präambel gut auf einen Träger synchronisieren konnte, aber noch zwei ganze Träger daneben liegt. Dies kann nun ausgeregelt werden und die Frequenzsynchronisation ist gelungen.

Im laufenden Betrieb wird dieses Zeit-Frequenzverfahren für den neuen Belegungsvektor nur jeweils nach der Messphase angesetzt. Das bedeutet für die STA im System die Forderung, dass sie die Frequenzsynchronität innerhalb der Zeit bis zu den nächsten Zeit-Frequenz-Paketen vom AP unter einem halben Trägerabstand halten müssen.

Die Frequenzkorrektur, die mit den langen Trainingsymbolen arbeitet, muss aufgrund der großen Störsignale durch Stammnutzer auf ihre Effektivität untersucht werden. Auch die Rahmensynchronisation wird ein Ziel genauerer Betrachtungen sein:

#### 4.2.2 Rahmen- und genaue Frequenzsynchronisation

Als erster Ansatz soll versucht werden, die Verfahren von 802.11a zur Synchronisation von Rahmen und Frequenz direkt zu übernehmen. Es wird hierfür also eine Präambel zum Einsatz kommen, die nun mehrere, gleiche OFDM-Symbole enthält, die die Suche nach dem Rahmenbeginn lösen. Diese Symbole sind nicht verkürzt, da die Erzeugung der verkürzten Symbole -wie schon erwähnt- nicht möglich ist. Die Präambel muss auch ermöglichen, den Frequenzversatz zu berechnen. Dazu werden zwei gleiche, aufeinanderfolgende Symbole benötigt, die nicht durch ein Guard-Intervall getrennt sind. In Abbildung 4.9 ist das typische Aussehen einer solchen Präam-

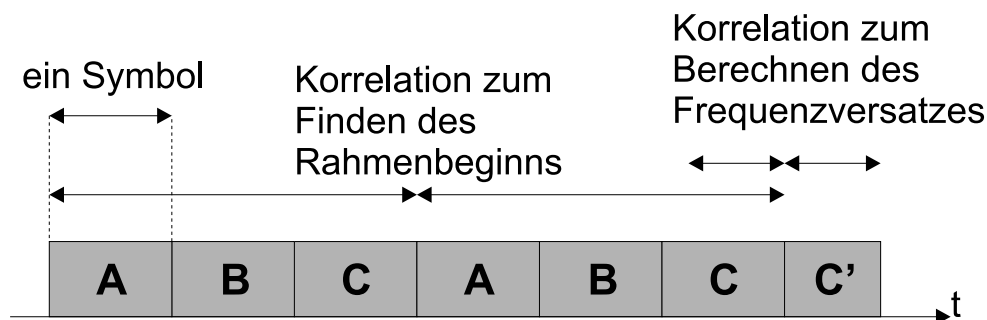


Abbildung 4.9: Präambel zur Synchronisation von Rahmen und Trägerfrequenz

bel dargestellt. Sie besteht hier aus drei sich wiederholenden Symbolen, gefolgt von einem zusätzlichen, das die Kopie der letzten Abtastwerte des letzten Symbols ist. Befindet man sich z.B. in einem System wie 802.11, so wären die Symbole A,B,C jeweils 80 Abtastwerte lang, und C' nur 64 Abtastwerte. Notwendig ist diese verkürzte Korrelationslänge von C' für die Berechnung des Frequenzversatzes. Im Prinzip müssen A,B und C nicht einmal richtige OFDM-Symbole sein, da sie lediglich als Abtastwerte durch einen Korrelator wie in Abbildung 3.11 laufen. Es muss nur bekannt sein, nach wie vielen Abtastwerten sich die Sequenz wiederholt, damit die richtige Verzögerung eingestellt werden kann.

Das Problem der Präambel ist, dass mit zunehmender Quote von Stammnutzern im Pool, immer mehr Anteile des Zeitsignals von Stammnutzern kommen und das SNR für die Korrelation verschlechtern. Abbildung 4.10 zeigt, wie die Korrelation sich verschlechtert, wenn der Pool

#### 4 Modifikation von 802.11a für Spectrum Pooling

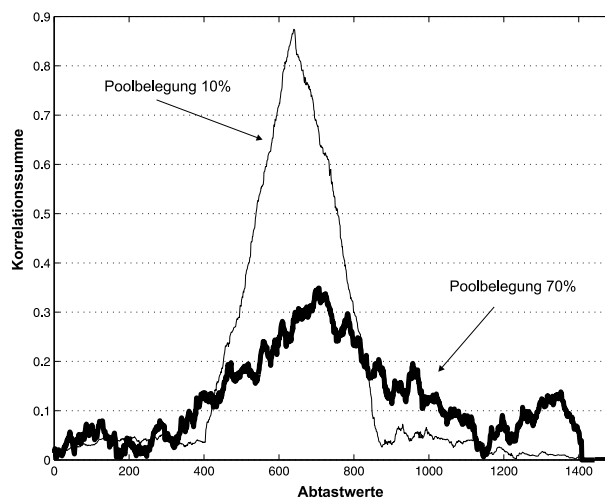


Abbildung 4.10: Vergleich von Autokorrelationskurven bei verschiedenen Poolbelegungen - Korrelationslänge: 3 Symbole

mehr Stammnutzer enthält. Es wurde für dieses Beispiel eine Korrelationslänge von 3 Symbolen gewählt, die Stammnutzerleistung ist doppelt so hoch wie die Mietnutzerleistung, das Mietnutzersystem hat ein SNR von  $25\text{dB}$ . Die Belegungen sind (wie eingezeichnet) 0,1 und 0,7. Diese Autokorrelationskurven müssen nun die Rahmendetektion ermöglichen. Neben der reinen Feststellung, dass eine Präambel vorliegt, muss auch der genaue Anfangszeitpunkt ermittelt werden. Bei diesem Beispiel wäre die Korrelationsspitze (für die Bestimmung des Rahmenbeginns) beim Abtastwert 640 zu erwarten. Die 10% -Kurve hat diesen Werte recht gut erreicht. Die 70% -Kurve ließe vermutlich mit einer cleveren Heuristik noch zu, die Existenz der Präambel festzustellen, aber die genaue Bestimmung des Anfangszeitpunktes wäre nicht möglich. Dieser hat aber im OFDM-System sehr wenig Spielraum. Die Länge des Guardintervalls beträgt bei z.B: bei 802.11 sechzehn Abtastwerte. Diese sind eigentlich zum Ausgleichen der Effekte der Mehrwegeausbreitung gedacht. Sollte die Schätzung des Anfangszeitpunktes sogar schon mehr als 16 Punkte daneben liegen, ist eine deutliche Degradierung des SNR im Empfänger schon alleine aufgrund des falschen Anfangszeitpunktes zu erwarten. In Abbildung 4.11 sieht man, unter sonst gleichen Bedingungen, wie die Erhöhung der Korrelationslänge auf jetzt 8 Symbole doch bessere Ergebnisse liefern kann. Auch die Sendeleistung der Stammnutzer hat einen entscheidenden Einfluss auf die Qualität der Korrelationskurven. Es muss nun ermittelt werden, wie die Faktoren

- Frequenzversatz
- Stammnutzerleistung
- Korrelationslänge
- Poolbelegung

auf die Aufgaben der Präambel einwirken. Die Stammnutzerleistung ist als mittlere Empfangsleistung im Empfänger des Mietnutzersystems zu verstehen. Sie wird relativ zur mittleren Emp-

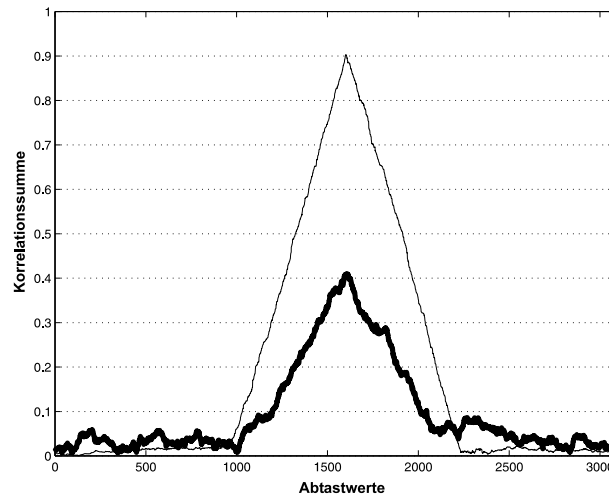


Abbildung 4.11: Vergleich von Autokorrelationskurven bei verschiedenen Poolbelegungen - Korrelationslänge: 8 Symbole

fangsleistung der Mietnutzersendungen verstanden. Empfängt also eine STA die Signale aus dem Mietnutzersystem im Mittel mit z.B.  $1mW$  und die Signale der Stammnutzer im Mittel mit  $2mW$ , so wird die Stammnutzerleistung relativ in  $dB$  angegeben:  $10 \cdot \log_{10}\left(\frac{2mW}{1mW}\right)dB = 3dB$ . Die Poolbreite ist wieder 64 Träger und das  $SNR$  im Mietnutzersystem  $25dB$ .

Simulationen haben gezeigt, dass der Frequenzversatz einen unerheblichen Beitrag zur Qualität der Korrelationskurven hat. Dass dies auch mathematisch zu verstehen ist, zeigt Kapitel 4.2.3. In Bild 4.12 ist simulativ die Wahrscheinlichkeit ermittelt worden, mit der die Schätzung des Beginns der Präambel auf  $\pm 8$  Abtastwerten berechnet wurde. Bei einer GI-Länge von 16 Abtastwerten ist somit eine fehlerfreie Datenübertragung gerade noch möglich, wenn keine Einflüsse der Mehrwegeausbreitung vorhanden sind. Die Ergebnisse scheinen zunächst relativ enttäuschend zu sein. Man muss sich allerdings vor Augen führen, dass der Empfang der Präambel einer Korrelation im Zeitbereich entspricht und die Stammnutzer *nicht* herausgefiltert werden. Wie sich die Schätzung des Rahmenbeginns und des Frequenzversatzes mit zunehmender Belastung des Pools durch Stammnutzer verschlechtert, ist in den Abbildungen 4.13 und 4.14 zu sehen. Es zeigt sich vor allem, dass eine Erhöhung der Korrelationslänge keine sichtbaren Vorteile erbringt. Bei niedriger Poolbelegung sind die Resultate durchwegs vertretbar. Dies wird auch letztendlich die Zielanwendung von Spectrum Pooling bestimmen. Pools, die ohnehin relativ frequentiert sind, lohnen sich nicht für Spectrum Pooling. Sollte die Stammnutzerleistung sehr hoch sein, ist dies zwar für die Detektion der Stammnutzer hilfreich, für den Empfang der Präambel aber katastrophal. In Abbildung 4.12 sieht man, dass die Empfangsquote bei einer relativen Stammnutzerempfangsleistung von  $6dB$  und einer Poolbelegung von nur 0,4 bereits unter 50% liegt. Auch die Schätzung des Frequenzversatzes ist unter diesen Bedingungen für OFDM bereits grenzwertig.

Will man also auch Pools für Spectrum Pooling mit 802.11a etablieren, in denen mit hohen Sendeleistungen seitens der Stammnutzer zu rechnen ist, oder bei denen die Poolbelegung auch über

#### 4 Modifikation von 802.11a für Spectrum Pooling

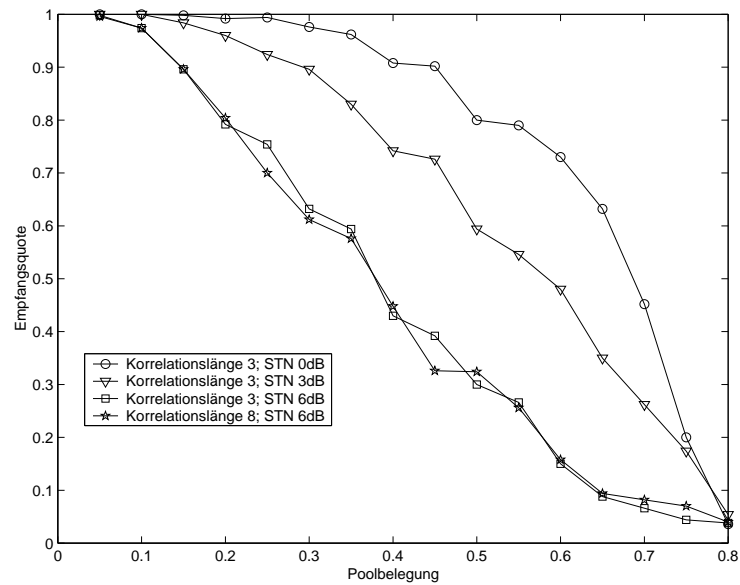


Abbildung 4.12: Quote der richtig empfangenen Präambeln bei verschiedenen Voraussetzungen

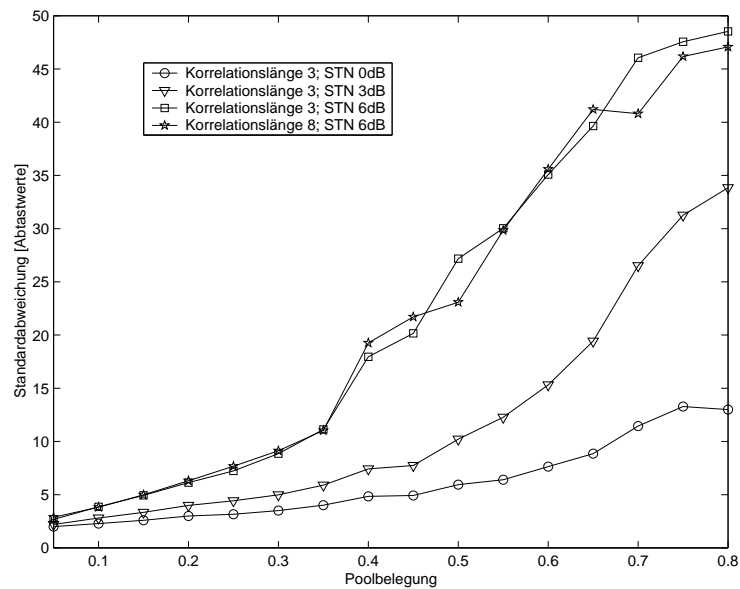


Abbildung 4.13: Standardabweichung der Schätzung des Rahmenbeginns bei verschiedenen Voraussetzungen

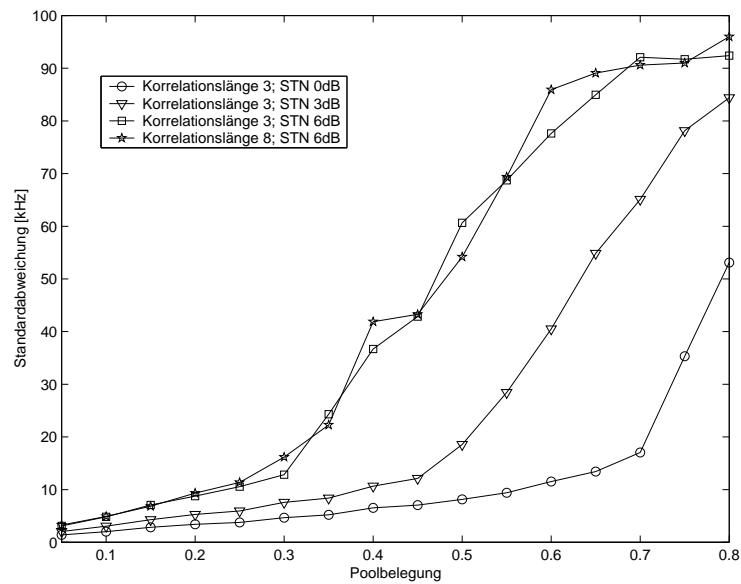


Abbildung 4.14: Standardabweichung der Schätzung des Frequenzversatzes bei verschiedenen Voraussetzungen

längere Zeit 20% überschreitet, braucht man eine alternative Lösung zur einfachen Korrelation mit demselben, zeitverzögerten Signal, wie es hier geschehen ist.

Da das OFDM-System ohnehin mit einem FFT / IFFT - Baustein versehen ist, liegt es nahe, die Fouriertransformation zu nutzen, um eine digitale Filterbank herzustellen, die die Stammnutzer herausfiltert. Die Idee ist also, diejenigen Frequenzen, auf denen Stammnutzer detektiert wurden, *vor* der Korrelation durch Filterung zu dämpfen. Könnte man mit dieser Filterung die Stammnutzerleistungen vollständig beseitigen, wäre keine Degradierung des SNR im Mietnutzersystem mehr zu erwarten. Es würde lediglich die Anzahl an Trägern geringer, auf die die Signale der Präambel verteilt sind.

Der Rechenaufwand steigt mit diesem Verfahren allerdings deutlich. Wurde vorher das Signal lediglich mit dem zeitverzögerten korreliert, was durch eine einfache rekursive Technik erfolgen konnte, ist jetzt neben der Korrelation auch noch eine Filterung nötig, die zusätzlich auch noch eine Zeitverzögerung des Ergebnisses erzeugt. Ist die Präambel a priori bekannt, kann die Korrelation mit dem zeitverzögerten Signal durch eine Korrelation mit der bekannten Präambel erfolgen. Dies soll im weiteren Verlauf - im Gegensatz zur bisherigen *Autokorrelation* - als *Kreuzkorrelation* bezeichnet werden. Abbildung 4.15 zeigt im Vergleich mit Abbildung 4.9, wie das Verfahren der Autokorrelation die Präambel verkürzt. Der Wiederholungsteil (C-C') ist nur noch für die Berechnung des Frequenzversatzes nötig. Welche Vorteile der Kreuzkorrelation mit welchen Einsatzbeschränkungen erkauft werden, soll das folgende Kapitel klarstellen.

#### 4 Modifikation von 802.11a für Spectrum Pooling

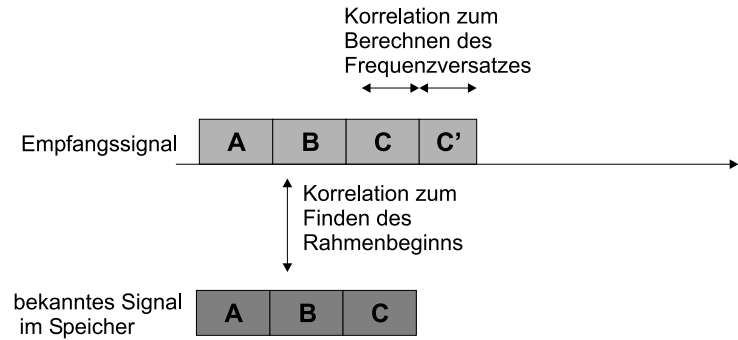


Abbildung 4.15: Kreuzkorrelation der empfangenen Prambel mit der gespeicherten Version

#### 4.2.3 Kreuz- und Autokorrelation in der Anwendung fur Prambeln

Wie schon im Kapitel 4.2 soll die Berechnung der Korrelationssumme mathematischen Aufschluss uber die zu erwartende Qualitat der Prambel liefern. Das gesendete Signal  $x(k)$  wird im Empfanger durch Frequenzversatz und unbekannte Phase zu

$$y(k) = x(k)e^{j2\pi\Delta f_c T_A k + j\varphi}$$

Bei der Autokorrelation wird die Korrelationssumme zu (4.2):

$$KS_{auto} = \sum_{k=0}^{N-1} y(k) \cdot y^*(k+N) = e^{-j2\pi\Delta f_c T} \sum_{k=0}^{N-1} |x(k)|^2$$

Die Phase fallt bei der Berechnung heraus. Bei der Kreuzkorrelation wird das empfangene Signal  $y(k)$  mit dem ursprunglichen Signal  $x(k)$ , das keinen Frequenzversatz oder Phasenfehler beinhaltet, korreliert:

$$KS_{kreuz} = \sum_{k=0}^{N-1} x(k) \cdot y^*(k) \quad (4.7)$$

$$\begin{aligned} &= \sum_{k=0}^{N-1} x(k) \cdot x(k) \cdot e^{-j2\pi\Delta f_c T_A k - j\varphi} \\ &= e^{-j\varphi} \sum_{k=0}^{N-1} |x(k)|^2 \cdot e^{-j2\pi\Delta f_c T_A k} \end{aligned} \quad (4.8)$$

Zur Berechnung des Frequenzversatzes wie in Formel 4.3 ist dieses Ergebnis nicht geeignet. Dafur muss also weiterhin eine Autokorrelation eingesetzt werden. Fur die Rahmensynchronisation wird nun der Betrag gebildet:

$$|KS_{kreuz}| = \left| \sum_{k=0}^{N-1} |x(k)|^2 \cdot e^{-j2\pi\Delta f_c T_A k} \right| \quad (4.9)$$

Jetzt wird klar, dass der Betrag der Korrelationssumme vom Frequenzversatz  $\Delta f_c$  und der Korrelationsdauer  $T$  abhängt. Wie man in Formel 4.9 sieht, kann der Modulationsterm, der jetzt noch von  $k$  abhängt, nicht aus der Summe herausgezogen werden. Dies war bei der Autokorrelation nicht der Fall. Man wird also eine Verschlechterung des Korrelationspeaks mit zunehmendem Term  $\Delta f_c T$  erwarten. Dies ist in Abbildung 4.16 zu sehen. Die Voraussetzungen entsprechen

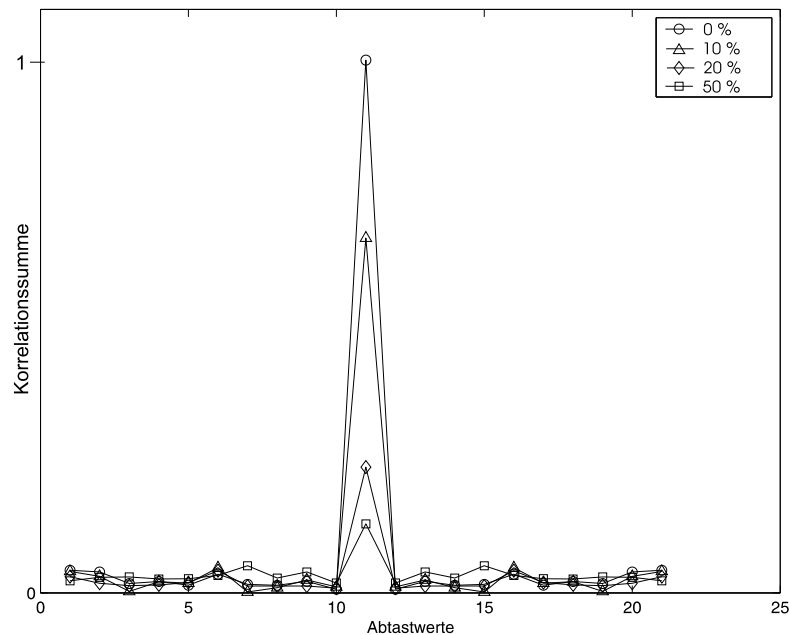


Abbildung 4.16: Verschlechterung der Kreuzkorrelation mit zunehmendem Frequenzoffset

hier wieder einem typischen 802.11a-System. Es wurde eine Korrelationslänge von 4 OFDM-Symbolen gewählt. Man sieht, wie die Korrelationsspitze mit Erhöhung des Frequenzversatzes abnimmt. Bei 50% Trägerversatz (bezogen auf die Breite eines Unterträgerabstandes) geht die Spitze praktisch im normalen Rauschen unter. Dies bedeutet für den Empfänger, dass er bei hohen Frequenzoffsets  $\Delta f_c$  keine Chance mehr hat, die Präambel zu empfangen. Dieses Ergebnis legt fest, dass diese Präambel nicht für die Aquirierungsphase geeignet ist, in der die Station noch keinerlei Synchronisation zum System besitzt. Die Präambel des Zeit-Frequenzverfahrens muss also im alten Stil mit einer Autokorrelation realisiert werden.

Die Kreuzkorrelation ist also nur im laufenden System sinnvoll, wenn die Stationen schon synchronisiert sind. Es ist nicht zu erwarten, dass eine Station dann zwischen zwei Paketen einen Frequenzversatz in der Größenordnung von einem halben Träger entwickelt. Hier kann die Kreuzkorrelation eingesetzt werden, und ihre Vorteile können voll genutzt werden. Diese liegen vor allem im typischen Aussehen der Korrelationskurven. In Abbildung 4.17 wurden OFDM-Symbole der Länge 2 im Abstand von 3 OFDM-Symbolen im Rauschen bei  $9\text{dB}$  SNR gesucht. Bei den Kurven der Autokorrelation, wie z.B. in Abbildung 4.11 ist stets eine Dreiecksform vorhanden. Je mehr sich der Korrelator dem tatsächlichen Beginn der Präambel nähert, desto größer wird die Korrelationssumme. Bei der Kreuzkorrelation sind die Verhältnisse anders. Sollte nämlich der

#### 4 Modifikation von 802.11a für Spectrum Pooling

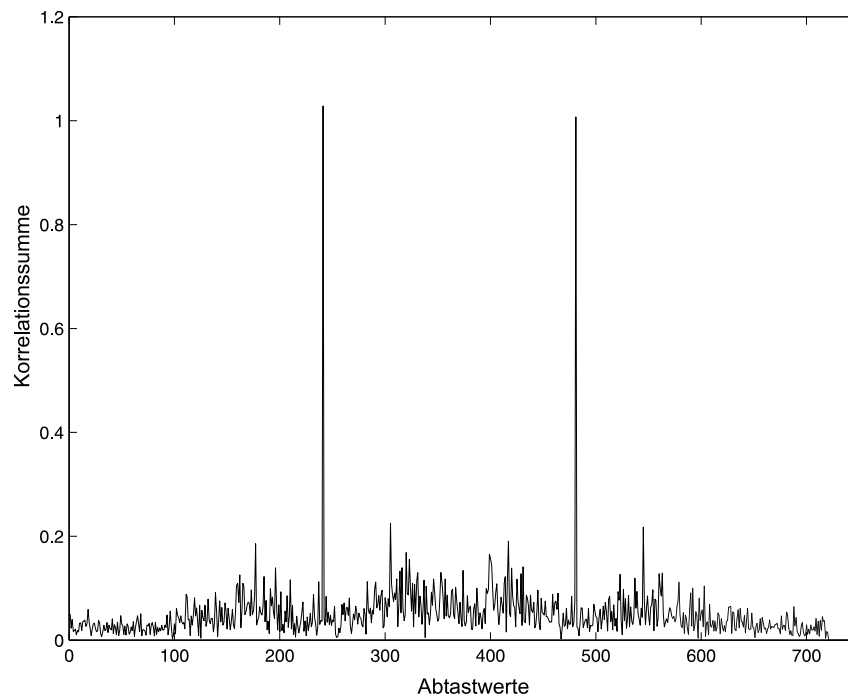


Abbildung 4.17: Typisches Aussehen einer Korrelation mit bekanntem Signal

Startpunkt der Korrelation nicht mit dem tatsächlichen übereinstimmen, werden die zwei Vektoren der Abtastwerte und der gespeicherten Werte genauso schlecht miteinander korrelieren, wie weisses Rauschen. Bei der geringsten Verschiebung gegeneinander ist keine Ähnlichkeit mehr vorhanden. Dies bedeutet für das System, dass, wenn die Frequenz- und Phasensynchronitäten einigermaßen hergestellt sind (wie dies in einem laufenden System stets der Fall sein wird), der Empfang der Präambel den exakten Rahmenbeginn automatisch mitliefert. Wenn also überhaupt eine Präambel empfangen wurde, dann ist damit der Rahmenbeginn automatisch 100%ig synchronisiert. Die Suche nach dem Korrelationspeak fällt auch leichter. Vorher musste das „Korrelationsdreieck“ mit Hilfe von Tiefpässen geglättet und dann das unklare Maximum geschätzt werden. Nun kann einfach laufend eine Schwelle aus dem Rauschen (wie in Bild 4.17) berechnet werden. Wenn diese Schwelle schlagartig und extrem weit überschritten wird, dann ist die Spitze gefunden. Zum Berechnen der Schwelle wurden in der Simulation laufender Mittelwert und Varianz des Rauschens verwendet. Abbildung 4.18 zeigt eine weitere Möglichkeit, die Fehlalarmrate zu verringern und die Sicherheit der Detektion zu erhöhen. Es wird von den empfangenen Werten nicht eine lange Korrelation zum Finden der Präambel berechnet, sondern zwei kurze. Damit kann hier Symbol B zweimal einen Beitrag zur Korrelation leisten. Wenn beide Suchen nach Symbolen einen erkennbaren Peak erzeugt haben, und dieser auch *genau* den Abstand von einem OFDM-Symbol hat, ist die Präambel gefunden.

Die Herausfilterung der Stammnutzer war Voraussetzung für das Verfahren der Kreuzkorrelation. Es kann trotz bekanntem Belegungsvektor dennoch passieren, dass nicht erkannte Stammnutzer

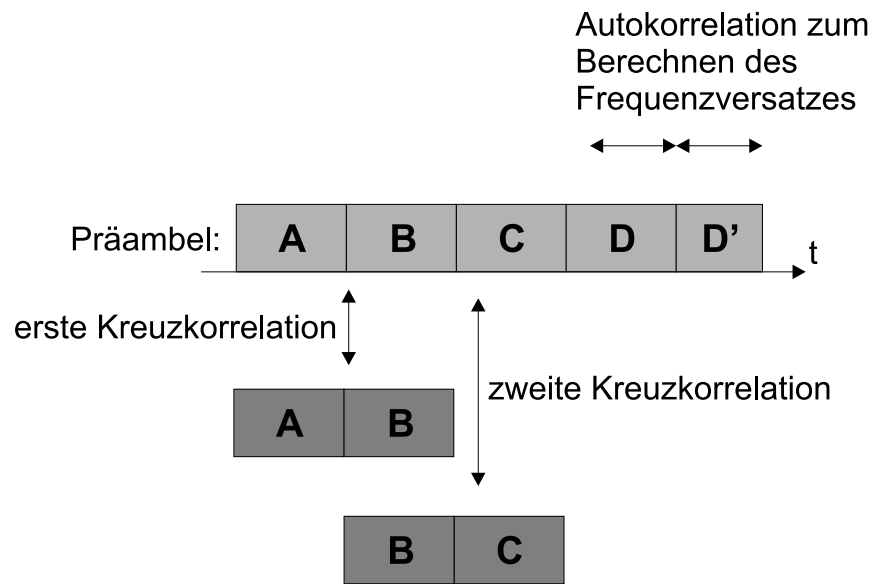


Abbildung 4.18: Mehrfache Korrelation zur Erhöhung der Sicherheit

im Pool existieren. Das ist z.B. immer dann der Fall, wenn sich die Belegung mit Stammnutzern im Pool erhöht. Bis zur nächsten Messphase sind dann die neuen Stammnutzern als nicht erkannte Störquelle präsent und stören die Datenübertragung und den Empfang der Präambeln. Damit die Stationen nicht ständig aus der Synchronisation fallen, sollte die Präambel in der Lage sein, eine gewisse Quote nicht erkannter Stammnutzern zu verkraften. Diese muss allerdings auch mit der Fehlerrate verglichen werden, die der Faltungsdecoder im Empfänger noch korrigieren kann. Es macht keinen Sinn, die Präambel erheblich robuster auszulegen als den Decoder. Selbst wenn diese Präambel dann unter schlechten Bedingungen gefunden würde, könnte der Datenteil nicht mehr interpretiert werden. Besonders die dann unbekannte Länge des Paketes würde dazu führen, dass die Station mit hoher Wahrscheinlichkeit ihre Synchronisation zum AP verliert. Dies liegt vor allem an der Asynchronität des Zugriffsverfahren. Selbst wenn eine Station eine gute Synchronisation hatte, kann ein verpasstes Paket dazu führen, dass eine neue Aquirierung mit dem Zeit-Frequenzverfahren nötig ist. Die Wiederholungen der Messphase sind zwar periodisch, aber der genaue Anfangszeitpunkt kann aufgrund noch laufender Übertragung verschoben sein. Es ist der gleiche Effekt wie bei dem Versenden von Beacons in Abbildung 3.7.

In Tabelle 4.3 sind die Ergebnisse einer Simulation des Faltungsdecoder nach [IEEE9, S.17] mit einer Gedächtnislänge 7 und Rate  $1/2$  zu sehen.

Setzt man voraus, dass der Interleaver der PHY-Schicht gute Arbeit leistet, so sollten Bündelfehler selten oder nie auftreten. Rechnet man z.B. mit 10 % Fehlerrate bei der Übertragung, entspräche das bei einem halbvollen Pool der Breite 64 etwa 3 Trägern, die von ungesesehenen Stammnutzern gestört würden. Da man typischerweise mit Zugriffsbreiten der Stammnutzern von einigen OFDM-Trägern rechnet, ist also die Anzahl der ungesesehenen Stammnutzern, die der Co-dierer noch verkraftet, zwar poolbreitenabhängig, aber sicherlich im niedrigen, einstelligen Be-

#### 4 Modifikation von 802.11a für Spectrum Pooling

Länge des Bündelfehlers	Anzahl der darauffolgenden, richtigen Bits	Fehlerrate
1	5	16,6 %
2	15	11,7 %
3	31	8,8 %
4	42	8,7 %

Tabelle 4.3: Länge der korrigierten Bündelfehler

reich. Immer vorausgesetzt, dass keine zusätzlichen Fehler durch normales Rauschen etc. dazukommen. Ausserdem ist es natürlich von der Statistik der Stammnutzer abhängig, ob die Konstellation, dass zwischen zwei Messphasen so viele Stammnutzer dazugekommen sind, überhaupt wegen ihrer Häufigkeit relevant ist.

Abbildung 4.19 liegt eine Präambel der Länge 3 OFDM-Symbole zugrunde. Bei der oberen Kurve ist die relative Stammnutzerleistung  $2dB$ , der Frequenzoffset ist  $-40kHz$ . Bei der unteren Kurve ist die Leistung  $10dB$  und der Versatz  $+30kHz$ . Die Graphik läßt keinen Zweifel an der Überlegenheit des Kreuzkorrelationsverfahrens. Bei der  $2dB$ -Kurve ist die Empfangsquote der Präambel über weite Bereiche hervorragend. Selbst bei einer unrealistischen Poolbelegung von  $0,8$  und einem übersehenen Stammnutzer liegt sie noch über  $90\%$ . Erwähnenswert ist hier, dass die Empfangsquote bei z.B. [Poolbelegung= $0,8$  ; neue Stammnutzer = $0$ ] abhängig von den Stammnutzerleistungen variiert. Eigentlich sollten die Stammnutzer ja durch die Filterung keine Anteile mehr im Signal hinterlassen. Warum diese Filterung aber offensichtlich nicht ganz gelingt, wird in Kapitel 4.4 näher untersucht. In Abbildung 4.20 sieht man die Ergebnisse der Berechnungen für den Frequenzversatz. Es liegt hier eine relative STN-Leistung von  $3dB$ , SNR von  $25dB$  und  $-40kHz$  Versatz zugrunde. Bei Poolbelegungen bis  $0,7$  sind hier gute Ergebnisse zu erzielen. Man sollte sich als Vergleich die Ergebnisse der Autokorrelation vor Augen führen. Im Vergleich mit Abbildung 4.13 zeigt sich, dass hier auch bei niedrigen Poolbelegungen die Standardabweichung mindestens auf die Hälfte reduziert werden konnte. Bei der Autokorrelation liefern schon Poolbelegungen über  $0,55$  sehr schlechte Ergebnisse. Jetzt ist in diesem Bereich die Berechnung noch genauso gut wie im leeren Pool. Die Standardabweichung sollte in jedem Fall unter  $5kHz$  liegen. Nimmt man nämlich die Schätzungswerte für den Frequenzversatz als normalverteilt an, so kann man bei einer Standardabweichung von  $5kHz$  mit  $80\%$  Sicherheit davon ausgehen, dass die Synchronisation im OFDM-System besser als  $2\%$  vom Trägerabstand ist. Will man diese Wahrscheinlichkeit auf  $90\%$  erhöhen, so braucht man  $4kHz$  Standardabweichung. Größere Werte für die Standardabweichung bedeuten also eine größere Unsicherheit in der Frequenzsynchronität, was sich auf die Orthogonalität der Träger und somit auf das SNR im Empfänger auswirkt.

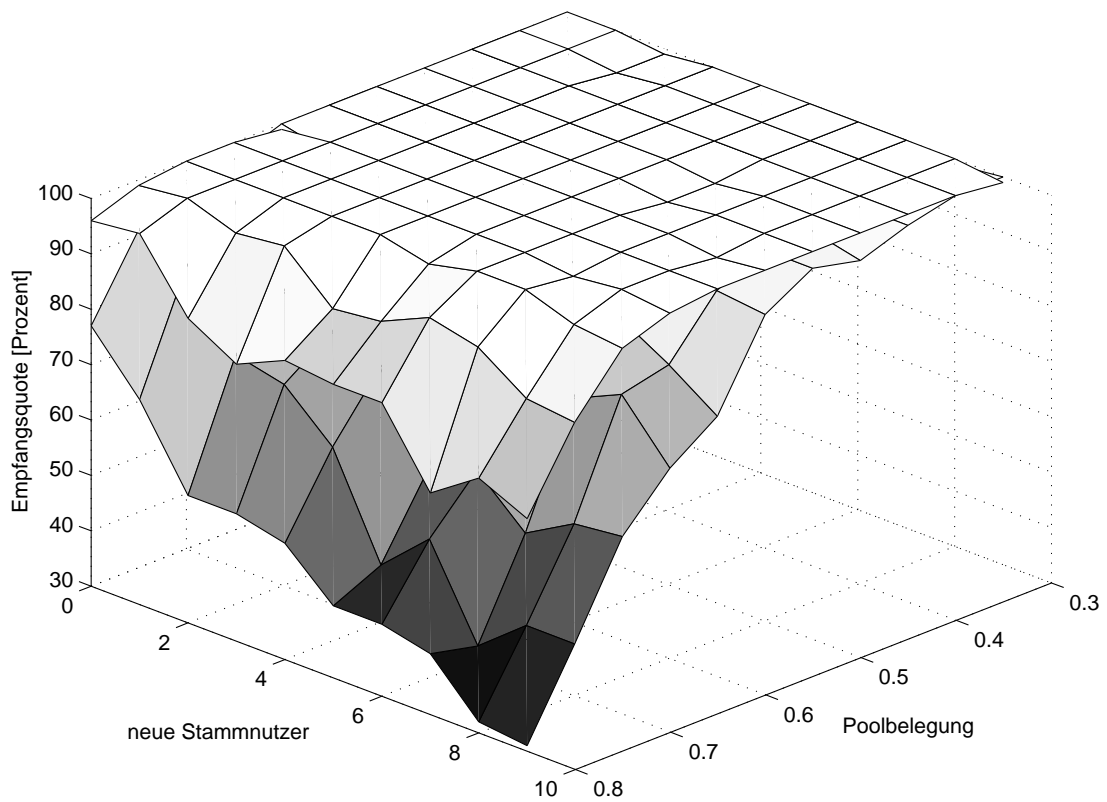


Abbildung 4.19: Empfangsquote der Präambel für zwei Stammmutzerleistungen

#### 4 Modifikation von 802.11a für Spectrum Pooling

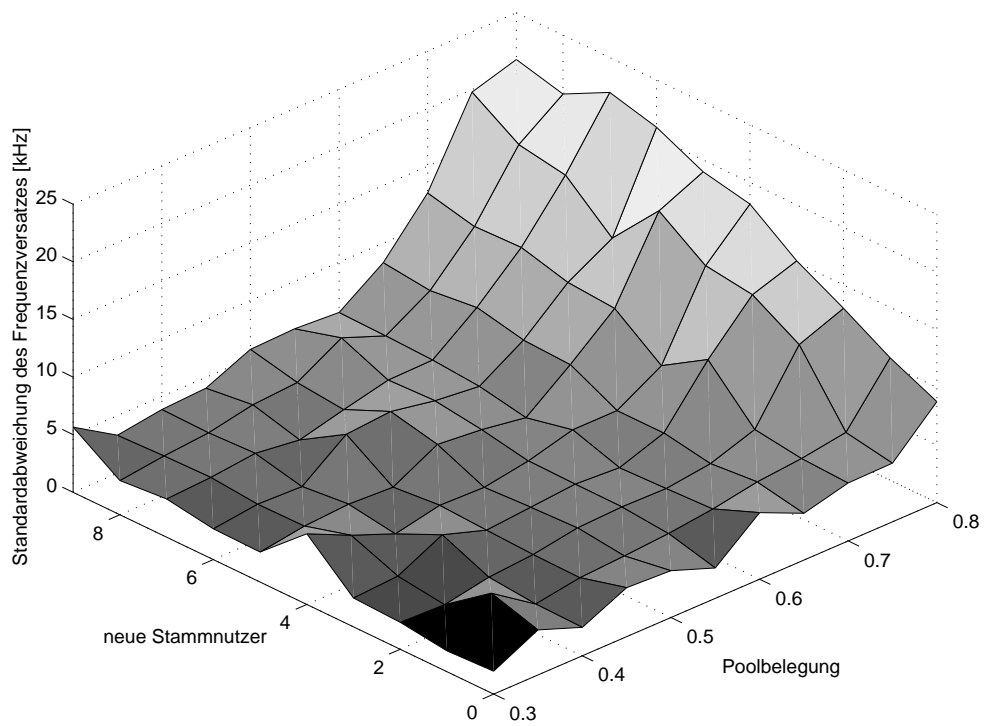


Abbildung 4.20: Standardabweichung des Frequenzversatzes

#### 4.2.4 Master-Synchronisation

Die Synchronisation im Spectrum Pooling System muss -wie erwähnt- während dem laufenden Betrieb möglichst gut aufrecht erhalten werden. Hier ist vor allem der Trägerversatz zwischen den Stationen bedeutsam. Erstens degradiert die Kreuzkorrelationsqualität mit zunehmendem Frequenzversatz (wie in Abbildung 4.16 gezeigt), und außerdem verschlechtert sich mit zunehmendem Versatz auch die Korrekturleistung und damit auch nach der Korrektur im Empfänger insgesamt die Orthogonalität der OFDM-Träger. Zwei Stationen können z.B. zum AP jeweils einen halben Träger Versatz haben, aber untereinander einen ganzen. Dies kann beim Empfang von Präambeln im verteilten Zugriffsverfahren zu Problemen führen. Denn die Stationen empfangen ja auch die Rahmen von den anderen Stationen und nicht nur vom AP.

Ein Synchronisationstrick soll hier Abhilfe schaffen. Wenn die Synchronisation stets auf eine Station ausgerichtet würde, so wäre die Synchronisation im verteilten Zugriffsverfahren besser. Durch den starren Ablauf im Spectrum Pooling System ist dies möglich. Der erste Schritt einer Station ist stets die Anmeldung beim AP. Hierfür muss sie den Belegungsvektor mit Hilfe des Zeit-Frequenzverfahrens erfassen. Gleichzeitig kann sie ihre Schwingkreise auf die Frequenz des AP einregeln bzw. mathematisch die Abtastwerte korrigieren. Nach dem Zeit-Frequenzverfahren kennt die Station also ihren Frequenzversatz zum AP. Mit dem darauffolgenden Beacon vom AP wird diese Berechnung noch präzisiert. Verwendet die Station ihren (nach der Regelung) übrig gebliebenen Frequenzversatz auch bei der Sendung, so ist die maximale Synchronität zum AP erreicht. Die sendende Station würde also nach der IFFT-Erzeugung der zeitlichen Abtastwerte, diese noch mathematisch rotieren und dann erst verschicken. Damit wäre erreicht, dass der AP eine Vorzugsrolle in der Frequenzsynchronisation erhält. Er ist *Master* in der Synchronisation. Alle Stationen, die ja auch die Rahmen anderer Stationen empfangen, werden stets Rahmen erhalten, die möglichst gut auf die Frequenz des AP eingestellt sind. Diese Schwingfrequenz wird also systemweit implizit durch das Zeit-Frequenzverfahren verteilt und ist anschliessend auch beim Senden verbindlich.

#### 4.2.5 Vergleich des Rechenaufwandes von Auto- und Kreuzkorrelation

Für die Autokorrelation wird das einkommende Signal mit sich selber zeitverzögert korreliert. Da hier keine Filterungen oder sonstige Operationen im Frequenzbereich nötig sind, kann die Korrelationssumme 4.1 durch eine einfache Rekursion laufend berechnet werden. Dafür müssen nur doppelt so viele Werte im Speicher gehalten werden, wie die Korrelationslänge lang ist.

Es sei  $KS_0$  die Korrelationssumme zum Zeitpunkt  $t = 0$ . Dann ergibt sich im nächsten Abtastzeitpunkt  $t = 1$  die Korrelationssumme  $KS_1$  zu:

$$KS_1 = KS_0 - x(-2N) \cdot x^*(-N) + x(-N + 1) \cdot x^*(1) \quad (4.10)$$

Pro Zeitschritt werden also eine komplexe Multiplikation und zwei komplexe Additionen durchgeführt. Die Kreuzkorrelation benötigt hingegen erheblich mehr Aufwand:

Aus der Korrelationssumme 4.7 wird durch Umformung und Umkehrung der gespeicherten Werte durch  $z(M - k) = x(k)$ ;  $M = N - 1$  eine Faltung:

#### 4 Modifikation von 802.11a für Spectrum Pooling

$$\begin{aligned}KS_{kreuz} &= \sum_{k=0}^{N-1} x(k) \cdot y^*(k) \\ &= \sum_{k=0}^{N-1} z(M-k) \cdot y^*(k) \\ &= z(k) * y(k) \Big|_M\end{aligned}\tag{4.11}$$

Die Korrelationssumme kann im Zeitbereich also als eine Faltung verstanden werden, was bedeutet, dass stattdessen auch die im Frequenzbereich korrespondierende Multiplikation verwendet werden kann. Nun könnte man in *einem* Filter die Stammnutzfilterung und Korrelation vereinen. Die Filterlänge wäre mindestens die Korrelationslänge. Für ein einfaches FIR-Filter mit der Korrelationslänge 3 (wie für die Simulationen häufig verwendet) ergibt sich also ein Rechenaufwand von 240 komplexen Multiplikationen. Durch schnelle Faltung [KAM98, S.246ff] im Frequenzbereich lässt sich dies noch weiter auf nur 38 Multiplikationen pro Abtastwert reduzieren:

- Der Aufwand für eine N-FFT ist  $N \cdot \text{ld}(N)$
- Bei einer Länge von 3 OFDM-Symbolen ergibt sich wegen Zeropadding eine Filterlänge von  $3 \cdot 80 \cdot 2 = 480$
- Blockweise Transformation in den Frequenzbereich:  $480 \cdot \text{ld}(480) = 4276$  Multiplikationen
- Im Frequenzbereich wird die Filterung zur Multiplikation, also 480 Multiplikationen
- Rücktransformation über FFT: wieder 4276 Multiplikationen
- Insgesamt sind das 9032 Multiplikationen über eine Zeit von 3 Symbolen, also 38 Multiplikationen pro Abtastwert.

Nachteilig ist allerdings, dass das Ergebnis der Korrelation immer blockweise hergestellt wird, und sich somit Verzögerungen bis zu 3 Symbolen ergeben können. Will man dies vermeiden, so ist in jedem Schritt eine vollständige Filterung und Korrelation nötig, was dann wieder auf die FIR-Filterung führt.

### 4.3 Ergebnisse des Präambeldesigns für Spectrum Pooling

Da die Bedingungen für den Empfang der Präambeln im Mietnutzersystem sehr weit variieren, ist es sinnvoll, zwei verschiedene Einsatzzeiten zu unterscheiden. Die erste ist die Verwendung der Präambel in der *Aquirierungsphase*. Diese betrifft alle Stationen, die noch nicht beim AP angemeldet sind, und auch noch keine weiteren Synchronisationen durchgeführt haben. Auch Stationen, die aufgrund von starken Stammnutzerschwankungen den Anschluss an den AP verloren haben, müssen die Aquirierung wieder durchlaufen. Das zweite Einsatzgebiet für Präambeln ist während des normalen Betriebs. Die beteiligten Stationen haben Synchronisation mit dem AP durchgeführt und haben Kenntnis über den Belegungsvektor. Die Eigenschaften dieser Umgebungen und der Präambel sind:

## 4.3 Ergebnisse des Präambeldesigns für Spectrum Pooling

### 1. Aquirierungsphase

- Die Stationen haben keine oder sehr vage Kenntniss über den Belegungsvektor.  
⇒ Das Wissen über den Belegungsvektor kann nicht vorausgesetzt werden.
- Der Frequenzversatz zum AP kann extreme Werte bis einige Trägerabstände haben.  
⇒ Zeit-Frequenzverfahren für die grobe und Korrelation für die genaue Frequenzsynchronisation.
- Diese Phase muss für Stationen im Normalfall nur einmal durchlaufen werden.  
⇒ Die Zeitdauer dieser Präambel und alles, was an Berechnungen dazu nötig ist, ist *nicht* sonderlich zeitkritisch.
- Die Stationen haben keine Rahmensynchronität zum AP.  
⇒ Die Präambel muss sicher von anderen Daten unterscheidbar sein. (Das Zeit-Frequenzverfahren besitzt eine eigene Codierung in Zeitrichtung plus CRC auf der MAC-Schicht)
- Der genaue Anfangszeitpunkt der Daten ist nicht so kritisch, da *BPSK* mit schlechteren SNR auch noch gut arbeiten kann.  
⇒ Die einfache Autokorrelationsstruktur im Zeitbereich ist ausreichend.

### 2. Laufender Betrieb

- Die Präambel ist der Beginn jedes Paketes auf der physikalischen Schicht.  
⇒ Die Länge sollte auf das Mindeste reduziert werden, um den Durchsatz nicht unnötig zu verschlechtern.
- Der Anfangszeitpunkt der OFDM-Symbole muss genau bestimmt werden, um hochstufige *QAM*-Verfahren einsetzen zu können und um das Guard Intervall für die Mehrwegeausbreitung zu nutzen.  
⇒ Das Verfahren mit der Kreuzkorrelation gibt den Anfangszeitpunkt stets genau an.
- Der Belegungsvektor ist, bis auf neue Stammnutzer seit der letzten Messphase, bekannt.  
⇒ Die Kenntnis des Belegungsvektors kann vorausgesetzt und beim Empfang mit verarbeitet werden.
- Der Frequenzversatz ist aufgrund der schon erfolgten Synchronisation und durch die Master-Synchronisation gering.  
⇒ Es genügt eine Synchronisation durch Korrelation über ein OFDM-Symbol. (Dies deckt Frequenzversätze bis zu einem halben Trägerabstand ab).

Angesichts der Voraussetzungen scheint es klar, dass die Autokorrelationsvariante für die Aquirierung, und die Kreuzkorrelationsvariante für den laufenden Betrieb am besten geeignet sind. Die jeweilige Korrelationslänge ist natürlich dem Pool anzupassen. Hier spielen besonders Rauschleistung und typische Poolbelegung entscheidende Rollen. In den Simulationen hat sich die Länge 3 als Faustregel bewährt. Das heißt, dass bei der Autokorrelation  $2 \cdot 3$  OFDM-Symbole für den Rahmenbeginn und 1 Symbol für die Frequenzoffsetbestimmung, also 7 Symbole benötigt werden. Im laufenden Betrieb sind es 3 (die Kreuzkorrelation benötigt ja keine Wiederholung) plus 1 für die Offsetbestimmung, also 4 OFDM-Symbole. Der Standard 802.11a sieht vor, mit

#### 4 Modifikation von 802.11a für Spectrum Pooling

Hilfe der Präambeln auch Kanalschätzungen durchzuführen. Hierfür wird eine spektrale Schätzung der Übertragungsfunktion des Kanals mit Hilfe einer Kreuzkorrelation gewonnen. Man kann dafür in beiden Präambelvarianten einfach eines der Symbole herauswählen, und mit Hilfe einer gespeicherten Version diese Kanalschätzung durchführen. Es wird also keine zusätzliche Verlängerung der Präambel erfordern.

### 4.4 FDMA - OFDM - Nebeneffekte

Sollen ein FDMA-System auf Stammnutzerseite und ein OFDM-System auf Mietnutzerseite im Frequenzbereich miteinander arbeiten, so ist eine strikte Trennung der Frequenzbänder nötig. Die Stammnutzer verwenden als FDMA-System Sende- und Empfangsbandpässe, die eine genügende Sperrdämpfung außerhalb des erlaubten Bereichs ermöglichen. Bei OFDM ist dies nicht der Fall. Jeder Träger sendet Leistung nicht nur auf seiner Frequenz, sondern im ganzen Frequenzbereich des Pools. Aufgrund der Orthogonalität der Träger ist dieser Effekt im Mietnutzersystem ohne weitere Konsequenzen. Im Stammnutzersystem werden diese Leistungen jedoch aufgrund der Unsynchronität zum Mietnutzersystem zu Buche schlagen. Sie verwenden ja keinen synchronisierten OFDM-Empfänger, der die Schaltpunkte im Sender durch die Zeitfensterung genau ausspart. Auf Mietnutzersystemseite entstehen aufgrund der kurzen Zeitfensterung für ein OFDM-Signal durch Leckeffekt Streuleistungen von Stammnutzern, die sich im SNR des Mietnutzersystems bemerkbar machen. Diese beiden Effekte, die aus dem Zusammentreffen von OFDM und FDMA kommen, sollen nun getrennt untersucht werden.

#### 4.4.1 Nebeneffekte zum Nachteil der Mietnutzer

Unerwünschte Störungen, die sich als Nachteil der Mietnutzer herausstellen, können nur beim Empfang von Signalen entstehen. Hier muss man sich genau klar machen, was in einem OFDM-System beim Empfang für Abläufe stattfinden, und wie sie sich auf die Signale auswirken. Blickt man z.B. auf Abbildung 4.4, so hat es den Anschein, als würden die Stammnutzer durch ihre Sendefilter nur jeweils einen kleinen Bandpassbereich besetzen. Dies ist auch richtig. Die Sendefilter sind ja genau deshalb so ausgelegt. Jetzt soll der Ablauf in einem Empfänger des Mietnutzersystems in den wesentlichen Einzelheiten zusammengestellt werden. Es werden wieder Bedingungen wie für 802.11a vorausgesetzt:

1. Heruntermischen des Signals in die Tiefpasslage
2. Abtasten des Signals mit 20Mhz
3. Synchronisation mit Präambel
4. Zerstückeln des Stroms der Abtastwerte in 80er Pakete
5. Entfernen des Guardintervalls
6. FFT mit den übrigen 64 Werten vollziehen
7. Interpretation der Werte im Frequenzbereich anhand der bekannten Signalraumkonstellationen
8. Deinterleaven, Decodieren, Descrambeln
9. Daten an die MAC-Schicht weiterreichen

Punkt 6 ist der problematische. Das eintreffende Signal wird einer kurzen FFT der Länge 64 unterzogen. Dadurch wird das Spektrum, was durch die Abtastung noch richtig dargestellt wird, einer Zeitfensterung unterzogen. Das diskrete Spektrum (Periodogramm), was nun vorliegt, entspricht nicht mehr ganz dem ursprünglich gesendeten. Das Signal wird im Zeitbereich mit einem Rechteckfenster bewertet, und entsprechend im Frequenzbereich mit der Transformierten des Rechteckfensters gefaltet. Der Erwartungswert des Periodogramms ist nach [KAM98, S. 315]:

$$E\{Per_N(\Omega)\} = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{1}{N} \left[ \frac{\sin(\Theta \cdot N/2)}{\sin(\Theta/2)} \right]^2 S_{XX}(e^{j(\Omega-\Theta)}) d\Theta \quad (4.12)$$

Hierbei ist  $\Omega = \frac{\omega}{f_A}$ . Es zeigt sich, dass das Periodogramm asymptotisch erwartungstreu ist:

$$\lim_{N \rightarrow \infty} E\{Per_N(\Omega)\} = S_{XX}(e^{j\omega}) \quad (4.13)$$

Es ist nach 4.12 klar, dass für kleine N die Wirkung der Fensterung im Zeitbereich sehr groß ist. Diesem Effekt könnte man natürlich durch die Wahl eines günstigeren Fensters im Zeitbereich entgegenwirken. Dies würde allerdings die Orthogonalität der Träger aufheben, da diese ja auch alle mit der entsprechenden Fensterfunktion im Frequenzbereich gefaltet würden. Der Einsatz von Fenstern ist also ausgeschlossen. Stattdessen ist es nun von Interesse, wie sich die Zeitfensterung der Signale von den Stammnutzern in der Praxis darstellt. In Abbildung 4.21 sieht man,

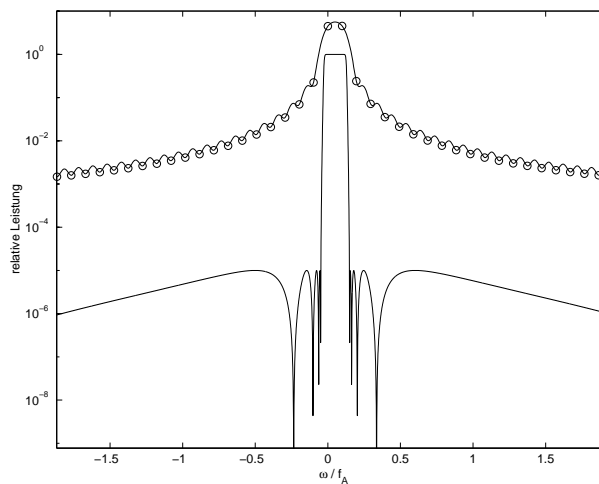


Abbildung 4.21: Vergleich Periodogramm ↔ kontinuierliches Spektrum

dass das eigentliche, gesendete Spektrum (untere Kurve), das im Sperrbereich eine Dämpfung von  $> 50dB$  hat, durch die Kurzzeit-FFT stark verändert wird (obere Kurve). Die Achse „relative Leistung“ ist nicht absolut zu verstehen! Die abgetastete Leistung im Stammnutzerband ist nicht höher als die tatsächliche! Vielmehr sind beide Kurven getrennt dargestellt und können nicht in ein gemeinsames Koordinatensystem gesetzt werden. Sie haben ja auch verschiedene Einheiten. Es geht hier nur um den Verlauf der Kurven und die Darstellung des Effektes der

#### 4 Modifikation von 802.11a für Spectrum Pooling

Zeitfensterung. Es werden erhebliche Leistungsanteile weit aus dem eigentlichen Stammnutzerband mathematisch gestreut. Die Kreise sind dann die Abtastwerte der FFT vom zeitgefensterten, kontinuierlichen Signal; also die Werte, die dann im Empfänger vorliegen. Wieviel Leistung im Einzelnen wo gemessen wird, hängt natürlich von dem Sendefilter des Stammnutzers ab, und auch von der (zeitlichen!) Länge der FFT, die dem OFDM-System zu Grunde liegt.

Betrachtet man die Leistungsanteile relativ, so ändern sie sich auch nicht mit Änderung der Poolbreite, solange die FFT-Dauer die Gleiche bleibt. Der Effekt hängt nur von der Dauer des Zeitfensters ab. Will man eine wirkliche Verbesserung erreichen, muss das Zeitfenster länger gewählt werden, was dann automatisch einen engeren Unterträgerabstand mit sich bringt. Dies ist aus Synchronisationsgründen vielleicht nicht mehr realisierbar. Denn je enger die Träger liegen, desto besser muss die Frequenzsynchronisation sein, um Orthogonalität zu garantieren. Legt man wieder die Parameter von 802.11a zugrunde, kann man die relativen Leistungsanteile der Stammnutzerleistung berechnen, wenn man sein Sendefilter kennt. Da dies nicht der Fall ist, wurde für weitere Berechnungen und Simulationen schlicht ein mittleres Ergebnis aus sehr verschiedenen Sendepässen erzeugt. Hier waren Cauerfilter, sowie Filter nach dem Chebycheff II - und Butterworthentwurf im Einsatz. Die Filterordnungen lagen zwischen 5 und 9, die Dämpfungen im Sperrbereich zwischen 20 und 50 dB. Dass diese Filter natürlich sehr unterschiedliche Ergebnisse erzielen würden, ist klar.

Position des Trägers	relativer Leistungsanteil
auf dem Stammnutzer	85,4%
1.Nebenträger	4,41%
2.Nebenträger	1,01%
3.Nebenträger	0,47%
4.Nebenträger	0,28%
5.Nebenträger	0,18%
6.Nebenträger	0,13%
7.Nebenträger	0,10%
22.Nebenträger	0,01%
23.Nebenträger	0,01%

Tabelle 4.4: Relative, mittlere Leistungsanteile eines Stammnutzers auf den FFT-Abtastwerten

Tabelle 4.4 zeigt auszugsweise die Ergebnisse der Berechnungen für diese relativen Leistungen bei einer Stammnutzerbreite von einem Träger. Will man Stammnutzer mit einer Zugriffsbreite größer als eins modellieren, so kann man einfach mit der gleichen Tabelle arbeiten und den breiteren Stammnutzer als Summe von einfachen superponieren. Hier hat es sich gezeigt, dass aufgrund der starken Unterschiede der Bandpässe zwischen verschiedenen Stammnutzern, die Modellierung über Superposition gar nicht nötig ist. Man kann als gute Näherung (solange die Stammnutzerbreite vier OFDM-Träger nicht überschreitet) wieder die Tabelle 4.4 nehmen. Man

teilt einfach die Leistung des Hauptträgers (85,4%) auf die Breite des Stammnutzers auf, und fährt auf beiden Seiten dann mit den Werten der Tabelle fort.

Weiss man nun durch Näherung über die Tabelle oder durch genaue Berechnungen und Messungen von bekannten Stammnutzersendefiltern, auf welchem Träger wieviel Leistung empfangen wird, stellt sich die Frage, welche Träger nun abgeschaltet werden müssen. Abbildung 4.22 ver-

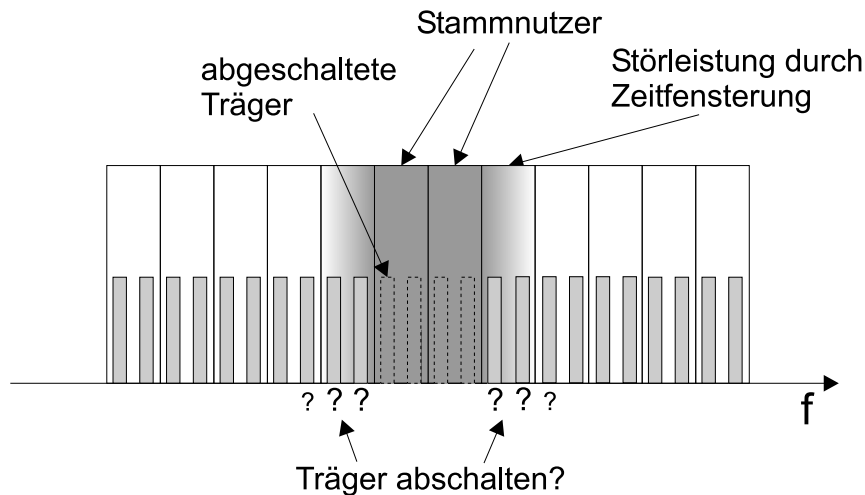


Abbildung 4.22: Stammnutzer im Mietnutzerpool

deutlicht noch einmal diese Fragestellung. Es genügt unter Umständen nicht mehr, nur diejenigen OFDM-Träger zu deaktivieren, die direkt von den Stammnutzern belegt sind. Auch Nachbarträger sind evtl. so stark mit Störleistungen belastet, dass es nötig ist, sie ebenfalls abzuschalten. Um der Entscheidung, ob zusätzliche Träger abgeschaltet werden müssen, näher zu rücken, macht es Sinn, die Veränderung des SNR im Mietnutzersystem zu betrachten. Dies wird natürlich auf den übrig gebliebenen Trägern besser werden, je mehr Träger, die von Stammnutzern benachbart sind, abgeschaltet werden. Das SNR wird sich aber auch zwischen den OFDM-Trägern stark unterscheiden. Die Träger, die näher an Stammnutzern sind, werden mehr Störleistung als weiter entfernte erfahren. In Abbildung 4.23 sieht man, wie sich das SNR für die Mietnutzer trotz Abschalten von Trägern verschlechtert. Es handelt sich um einen 128er Pool mit relativer Stammnutzerleistung von  $3dB$ ; die Stammnutzerzugriffsbreite ist zwei, der Rauschpegel ist  $-30dB$ . Die oberen drei, stärker durchgezogenen Kurven geben das mittlere SNR im Pool abhängig von der Poolbelegung an. Sie unterscheiden sich durch die Anzahl der abgeschalteten Träger um einen existierenden Stammnutzer. Bei der mit dem Viereck markierten Kurve sind außer den OFDM-Trägern, die direkt auf dem Stammnutzer liegen, auch noch die nächsten zwei abgeschaltet. Bei der mit dem Stern markierten Kurve sind nur die Träger abgeschaltet, die im Frequenzbereich genau auf den Stammnutzern liegen. Dass diese triviale Art, den Stammnutzern aus dem Weg zu gehen, die schlechtesten Ergebnisse erzielt, ist klar. Die Träger, die direkt neben einem Stammnutzer liegen, erfahren ja nach Tabelle 4.4 immerhin noch gut 4% der Leistung des Stammnutzers als zusätzliche Störleistung. Dies sieht man besonders deutlich auf den Kurven der Worst Case-Träger in Graphik 4.23. Diese Kurven geben an, wie im Mittel das SNR auf dem

#### 4 Modifikation von 802.11a für Spectrum Pooling

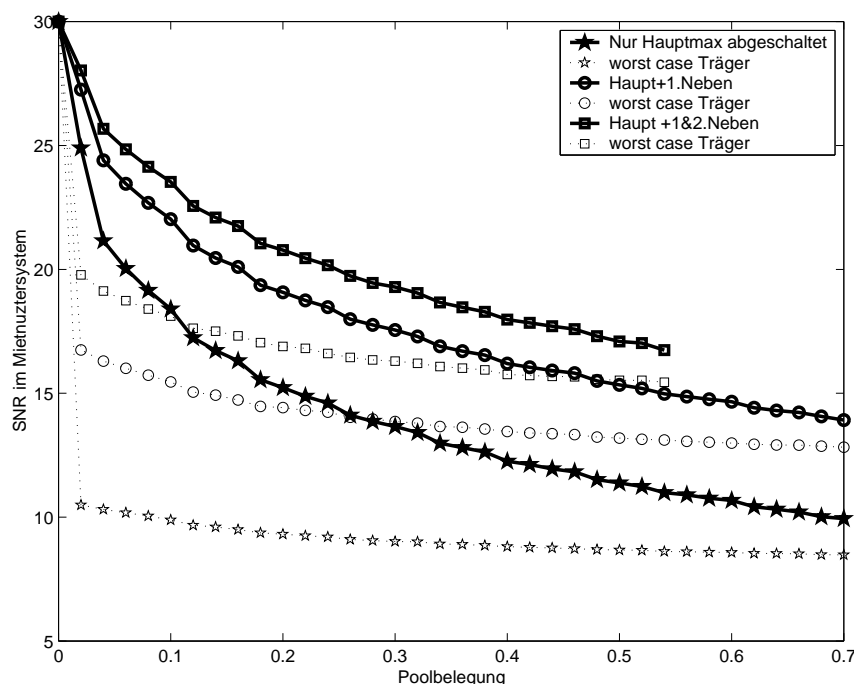


Abbildung 4.23: SNR im Pool wegen Störleistungen durch Zeitfensterung

Träger im Pool ist, der am meisten Störungen bekommt. Die Unterschiede zum mittleren SNR im Pool sind teilweise gravierend. Hier muss abgewägt werden, ob der eingesetzte Faltungscodierer noch in der Lage ist, die zu erwartenden Fehler abzufangen. Abbildung 4.23 zeigt auch, dass die Erfolge, die durch zusätzliches Abschalten von Trägern erzielt werden können, besonders auf den Worst Case-Trägern deutlich sind. So bewegt sich der schlechteste Träger ohne zusätzliches Abschalten um die  $10\text{dB}$  SNR. Schaltet man nur einen Nachbarträger der Stammnutzer zusätzlich ab, so gewinnt man auf diesem Träger im Mittel schon rund  $5\text{dB}$  SNR.

Diese SNR-Verbesserungen, die durch Abschalten weiterer Träger erzielt werden, bringen jedoch einen Nachteil mit sich: es sind danach natürlich insgesamt *weniger* Träger im Mietnutzertersystem übrig, die für den Datenverkehr genutzt werden können. Schaltet man z.B. bei einem Pool mit STN-Zugriffsbreite 1 jeweils zusätzlich zwei benachbarte Träger ab, so wird es bei exakter Gleichverteilung der Stammnutzer schon bei einer echten Poolbelegung von 20% dazu kommen, dass kein einziger Träger mehr fürs Mietnutzertersystem übrig bleibt.

Es muss also eine Strategie entwickelt werden, die dynamisch je nach Poolbelegung angibt, wieviel Nebenträger abgeschaltet werden sollen, um den *gesamten Durchsatz* zu maximieren. Es macht unter Umständen z.B. Sinn, zwei Träger neben den Stammnutzern abzuschalten, um dann auf allen noch übrigen Trägern ein so gutes SNR zu haben, dass  $64\text{-QAM}$  möglich ist. Andererseits ist dies bei Pools mit viel Stammnutzeraufkommen nicht möglich, weil die Gesamtzahl der übrigen Träger im Mietnutzertersystem zu gering würde. Hier sind noch Studien nötig, die eben diese Zusammenhänge herausstellen, mit dem Ziel, den größten Durchsatz zu erreichen.

## 4.4.2 Nebeneffekte zum Nachteil der Stammnutzer

Ähnlich wie im vorangegangenen Kapitel, erweist sich die Kombination von FDMA und OFDM auch im Hinblick auf die Störungen für die Stammnutzer als problematisch. Die Mietnutzer erzeugen auf den einzelnen, orthogonalen Trägern durch die Zeitfensterung der OFDM-Symbole das für OFDM typische  $\frac{\sin(x)}{x}$  - Spektrum, das sich aus dem periodischen Umschalten der Sinusschwingungen ergibt. Da die OFDM-Sender keine Sendefilter einsetzen, um die Orthogonalität der Träger nicht zu verschlechtern, kann dieses Spektrum auch in seinem Aussehen *nicht* verändert werden. Jeder Träger verteilt also Leistung im gesamten Band. Dem OFDM-System bereitet dies keine Probleme, da die Orthogonalität der Träger und das synchrone Empfangen dafür sorgen, dass die Spektralanteile im Abtastpunkt der benachbarten Träger (aus Sicht der Mietnutzer) Null sind. Die Stammnutzer, die kein OFDM-System betreiben und nicht auf die Mietnutzer synchronisiert sind, bekommen diese Leistungsanteile allerdings voll mit. Abbildung 4.24 zeigt

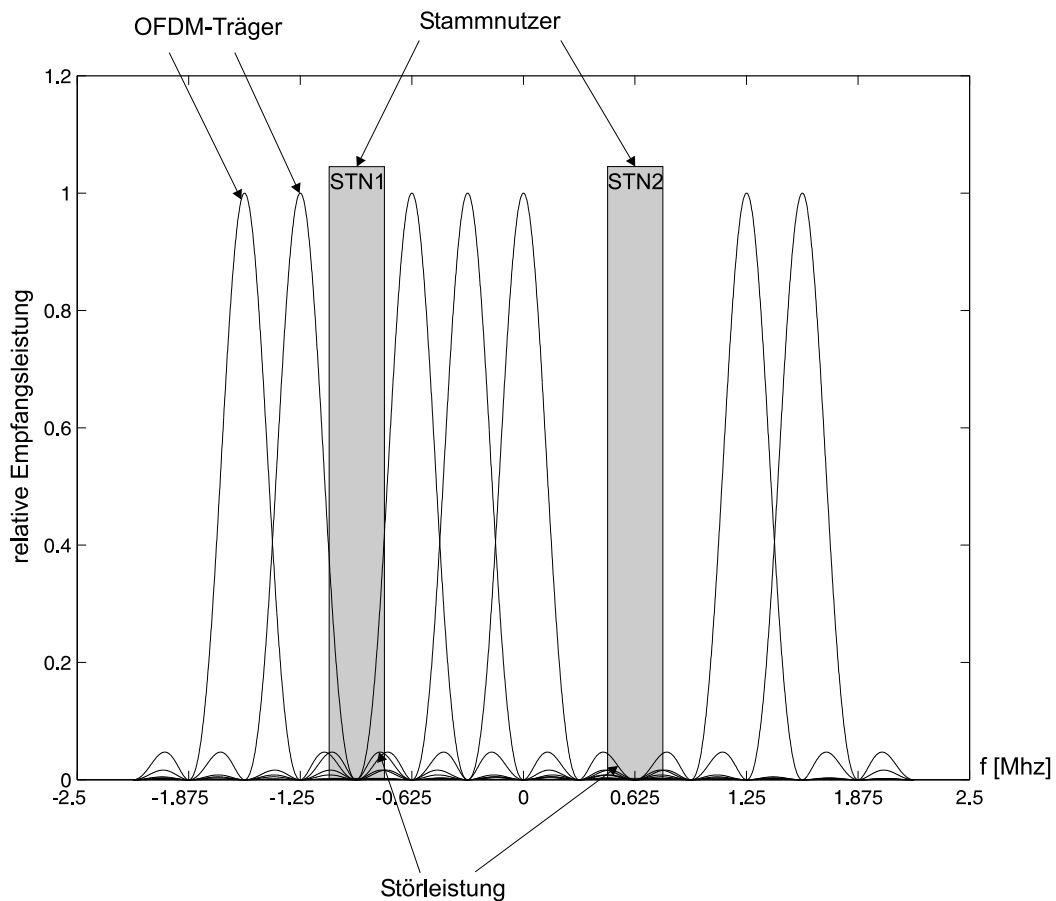


Abbildung 4.24: Empfangsleistung aus der Sicht eines Stammnutzers

die Details dieses Effekts. Die Stammnutzer belegen einen Träger und haben genau die Breite eines Trägerabstandes. Stammnutzer 1 (STN1) bekommt durch die benachbarten OFDM-Träger Störanteile in seinen Bandbereich gestreut. Bei Stammnutzer 2 sieht es etwas besser aus, weil

#### 4 Modifikation von 802.11a für Spectrum Pooling

auch die benachbarten Mietnutzerträger abgeschaltet wurden. Damit wird die Störleistung natürlich reduziert. Genauere Berechnungen, welche Leistungsanteile auf welche Träger treffen, und wie sich das Abschalten weiterer Träger auch hier als vorteilhaft herausstellt, sind in [HIL02] zu finden.

### 4.5 Weitere Modifikationen auf der physikalischen Schicht

#### AGC

Die Empfangleistungsregelung (*AGC, Automatic Gain Control*) ist eine wichtige Aufgabe der physikalischen Schicht. 802.11a sieht hierzu vor, die kurzen Trainingssymbole der Präambel zu nutzen, um die Regelung durchzuführen. Von einem empfangenen Signal würde also mit wenigen Abtastwerten die mittlere Leistung geschätzt und die Empfangsverstärkerstufe entsprechend eingestellt. Dieser Vorgang wird evtl. einige Male wiederholt. Die Einregelung auf den stets gleichen, internen Empfangspegel ist vor allem für die linearen Bauteile und die A/D-Wandlung wichtig. Der A/D-Wandler kann z.B. ein Signal von  $-500mV$  bis  $500mV$  in 8 Bit, also 128 Werte auflösen. Sollte die Empfängerleistungsregelung das Empfangssignal nur auf  $\pm 250mV$  verstärken, sind nur 7 Bit, also 64 Werte des A/D-Wandlers im Einsatz, man hat also nur noch die halbe Auflösung!

Genau hier ist das Problem bei Spectrum Pooling. Das empfangene Signal ist die Überlagerung von Stammnutzersignalen und Mietnutzersignalen. So addieren sich im Mittel die Leistungen. Die Empfangsleistungsregelung muss auf die mittlere, *gesamte* einfallende Leistung aussteuern. Die Stammnutzer werden erst anschließend mit Hilfe einer Filterung entfernt. Ist die Stammnutzerempfangsleistung z.B. 9 mal so groß wie die der Mietnutzer, muss das gesamte Empfangssignal dennoch auf die 8 Bit ausgesteuert werden, um kein Clipping zu bekommen. Die Mietnutzer, die leistungsmäßig nur ein Neuntel zum Signal beitragen, haben im Mittel nur ein Drittel der vollen Amplitude und nutzen somit von 128 Stufen nur 42! Die Auflösung hat sich also von 0,8% auf 2,4% verschlechtert. Diesem Effekt kann man nichts entgegenstellen, als die Auflösung der eingesetzten A/D-Wandler zu verbessern.

#### CCA

Der Carrier Sense-Mechanismus, der in der physikalischen Schicht von der *CCA (Clear Channel Assessment Function)* bereitgestellt wird, soll nach [IEEE9, S.32] innerhalb von  $4\mu s$  einen Pegel von  $-82dBm$  mit einer Zuverlässigkeit von 90% als eine Sendung einer anderen Station erkennen. Dies ist für das konkurrierende Zugriffsverfahren ein notwendiger Bestandteil. Für 802.11a ist hier vorgesehen, schlicht die Empfangsleistung an der Antenne zu bewerten (nach Bandpassfilterung) und so die Entscheidung zu fällen.

Bei Spectrum Pooling ist dies nicht so einfach möglich. Das Empfangssignal als Überlagerung von Mietnutzer- und Stammnutzersignalen hat in seiner gesamten Leistung keine Aussagekraft für den konkurrierenden Zugriff. Es müssen erst die Stammnutzer herausgefiltert werden. Hierfür kann z.B. die FFT (schnelle Faltung im Frequenzbereich) im Empfänger verwendet werden.

#### 4.5 Weitere Modifikationen auf der physikalischen Schicht

Nach der Filterung wird dann die Mietnutzer-Empfangsleistung berechnet. Aber auch hier bleiben, wie nach Kapitel 4.4.1 klar ist, noch Stammnutzer-Leistungsanteile auf den Mietnutzerträgern zurück, die Probleme bereiten können.

In Abbildung 4.25 sieht man das Verhältnis der gesamten Empfangsleistungen zwischen Miet-

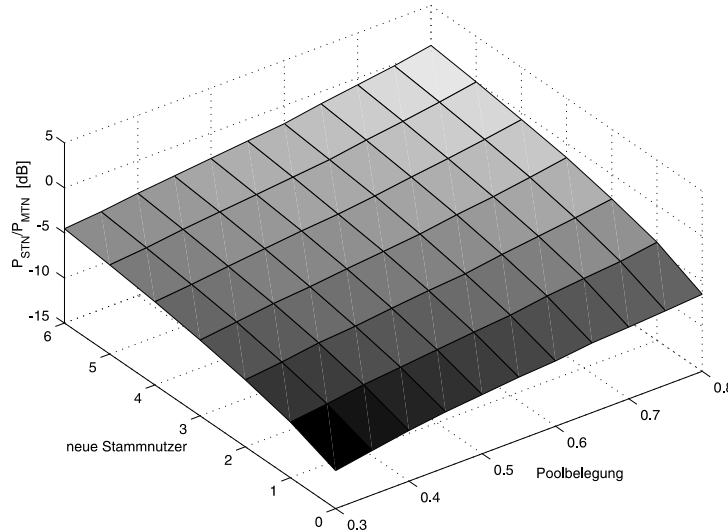


Abbildung 4.25: Verhältnis der Empfangsleistungen

nutzern und Stammnutzern. Die Empfangsleistungen wurden nur auf den gültigen Trägern des Mietnutzersystems gemessen. Es wurden *keine* zusätzlichen Schutzträger neben den Stammnutzern abgeschaltet. Die Stammnutzer haben im Mittel eine 4mal größere Leistung. Man sieht, dass selbst bei diesen überaus pessimistischen Vorgaben, es praktisch nicht passiert, dass die Streuleistung (durch FFT-Effekte) der Stammnutzer die  $0dB$  Marke überschreitet. Sollte sie das nämlich tun, dann würde eine Station vermuten, dass eine Sendung einer anderen Station vorhanden ist, die eigene Sendung nicht starten, und versuchen, eine Präambel zu decodieren. Es muss also sichergestellt werden, dass die Streuleistung inklusive der neuen Stammnutzer nie an diejenige Leistung heranreicht, die eine Station dazu bringen würde, den Carrier Sense-Status auf „belegt“ zu setzen. Nun kann man aber nicht immer von einer mittleren Verteilung von Miet- und Stammnutzern ausgehen. Sollte ein Stammnutzer z.B. sehr nah an einem Mietnutzer sein, so kann die relative Empfangsleistung schnell auf das zehnfache bis hundertfache ansteigen. Dann würde die STA zwangsläufig eine Sendung vermuten. Dies ist für den Durchsatz im System zwar nicht erfreulich, dafür gibt es einen sehr positiven Nebeneffekt. Diejenigen Stationen, die sehr nahe, neue Stammnutzer haben, werden aufgrund der CCA-Funktion *nicht* senden, da sie das Medium fälschlicherweise für belegt halten. Somit bleiben diese Stammnutzer von den großen Störungen, die von einer nahen Mietnutzerstation ausgehen würden, verschont.

Ist der AP in eine solche Konstellation geraten, muss ein weiterer Mechanismus dafür sorgen, dass er dennoch seine Sendung des Detektionsrahmens irgendwann beginnt. Es muss also eine Möglichkeit geben, festzustellen, dass die vermeindliche Sendung einer anderen Station gar

#### 4 Modifikation von 802.11a für Spectrum Pooling

keine solche ist. Nur der Nichtempfang der Präambel kann hierfür nicht genügen. Eine Lösung wäre, stets eine Anzahl von Trägern aus der Berechnung für den CS-Mechanismus herauszuhalten. Hier würden diejenigen gewählt, die die größte Leistung haben. Liegen die restlichen Träger (die dann nur noch Mietnutzerträger sind) dann leistungsmäßig über einer bestimmten Schwelle, so wird dies von einem Paket aus dem Mietnutzersystem kommen. Einzelne starke Störer würden so den CS-Mechanismus nicht gefährden.

#### Pilote

Durch die flexible Nutzung des gesamten Pools und die ständige Änderung der Zugehörigkeit der Träger, kann auch die Position der Pilotöne nicht statisch sein. Sie muss sich vielmehr der aktuellen Situation im Pool ständig anpassen. Damit für alle teilnehmenden Stationen hier Einigkeit über die Positionierung besteht, kann der Verteilung der Pilote nur eine Information zugrunde liegen: der Belegungsvektor. Ausgehend vom BV müssen also die Pilote gesetzt werden, damit jede andere Station, die den aktuellen BV auch hat, weiß, wo Pilote anzutreffen sind. Es würde sich z.B. eine äquidistante Aufteilung in den gültigen Trägern anbieten. Jede Heuristik, die die Pilote aufgrund des BV eindeutig verteilt, ist möglich. Hier ist noch Platz für weitere Untersuchungen.

Während der Aquirierung mit Zeit-Frequenzverfahren ist ein Einsatz von Piloten nicht möglich. Es ist weder die lokale Poolbelegung noch der gültige BV verfügbar. Hier muss also eine Signalformung eingesetzt werden, die auch ohne perfekte Phasensynchronisation auskommt. Da für das Zeit-Frequenzverfahren *BPSK* vorgesehen ist, sind damit schon alle Forderungen erfüllt. *BPSK* kann nämlich einfach als Basis für eine differentielle Codierung verwendet werden, und die absolute Phase spielt dann überhaupt keine Rolle.

### 4.6 Ergebnisse und Zusammenfassung für das Systemdesign

Der typische Systemaufbau für Spectrum Pooling auf 802.11a-Basis würde einen AP umfassen, der einige gut verteilte Boosting-Stationen um sich hat. Die Zellengröße entspricht den typischen Szenarien für 802.11 LANs. Da aufgrund des verteilten, asynchronen Zugriffsverfahrens, es garantiert sein muss, dass jede Station nicht nur Kontakt zum AP hat, sondern auch zu allen anderen, bestimmt dies die Zellengröße.

Die „besten“ Stammnutzer für den Einsatz von Spectrum Pooling sind wohl solche, die nicht zu schnell ihre Präsenz ändern und auch keine hohen (viel mehr als das 4-fache) Leistungen im Vergleich zu den Mietnutzern haben. Idealerweise sollten sich die Stammnutzer gar nicht räumlich in der Zelle selber befinden. Ein typischer Fall wäre z.B. Sprechfunk zwischen Taxis. Wenn man auf diesen Frequenzen z.B. in einer Messehalle Spectrum Pooling betreibt, so sind die Veränderungen in den Leistungen der Stammnutzer nicht allzu extrem, da sich die Taxis ja nie *in* der Halle aufhalten. Dies wäre für die Empfangsleistungsregelung vorteilhaft.

Die Problembereiche, die im Spectrum Pooling System zu erwarten waren, wurden ursprünglich in die Themen *Detektion*, *Synchronisation* und *FFT-Nebeneffekte* aufgeteilt. Hier sollen die

## 4.6 Ergebnisse und Zusammenfassung für das Systemdesign

vorgeschlagenen Lösungen nocheinmal vollständig zusammengefasst werden.

**Detektion** Die Detektion befasst sich mit der Erkennung der Stammnutzer. Da das Zusammenspiel zwischen Miet- und Stammnutzer einer anonymen Koexistenz entspricht, ist die zuverlässige Erkennung der Stammnutzer ein wichtiger Anteil am Funktionieren des Gesamtsystems. Es wurde für die Messung ein Diversity-Ansatz gewählt, bei dem alle anwesenden Mietnutzerstationen gleichzeitig eine Messung durchführen. Diese Messung wird vom AP durch den Detektionsrahmen eingeleitet. Das anschließende Boosting und Mapping sammelt die verteilten Messergebnisse wieder im AP, der den neuen Belegungsvektor generiert und ihn mit Hilfe des Zeit-Frequenzverfahrens wieder verteilt.

**Synchronisation** Neben den Synchronisationen der Trägerphase und des Abtasttaktes, die im betrachteten System keine ungewöhnliche Schwierigkeit darstellen, wurde vor allem Frequenzversatzkorrektur und Rahmensynchronisation untersucht. Die Frequenzversatzkorrektur setzt sich zusammen aus der Lösung für die grobe Korrektur mit Hilfe des Zeit-Frequenzverfahrens und der feinen Korrektur durch Autokorrelation über ein OFDM-Symbol. Die Rahmensynchronisation wird je nach Zustand der Station (assoziiert oder nicht) durch ebenfalls eine Autokorrelation oder Filterung mit Kreuzkorrelation gelöst.

**FFT-Nebeneffekte** Die Nebeneffekte, die sich durch Zeitfensterung und Kurzzeit-FFT ergeben, verschlechtern das SNR für die Mietnutzer bzw. erhöhen die Störleistung für die Stammnutzer. Es bleibt hier noch zu untersuchen, inwiefern andere Basisbandmodulationen neben OFDM im Hinblick auf Durchsatz und Effizienz in Erwägung gezogen werden sollten.

Die Probleme auf der Physikalischen Schicht sind also aufgedeckt und weitgehend gelöst. Nun muss es Ziel weiterer Untersuchungen sein, welche Modifikationen (z.B. bezüglich QoS) in der MAC-Schicht nötig sind, um ein Spectrum Pooling System vollständig aufzubauen.

### 4.6.1 PHY-Schicht

In Abbildung 4.26 sieht man, welche neuen Funktionsgruppen in der physikalischen Schicht benötigt werden. Sie sind in der Abbildung dunkler unterlegt. Die Darstellung ist eine rein funktionelle, d.h. die abgebildeten Funktionsgruppen unterscheiden sich von den tatsächlich physikalischen Baugruppen. (Die FFT-Baugruppe wird in einer technischen Realisierung mit Sicherheit mehrfach genutzt werden). Die Baugruppe „Zeit-Frequenzverfahren“ beinhaltet z.B. noch einen Speicher, da die einlaufenden Daten nicht wie für OFDM üblich in Frequenzrichtung, sondern in Zeitrichtung encodiert wurden. Ausserdem ist dort auch eine Decodierung notwendig. Die Funktionsgruppe „(Filterung) & Korrelationen“ beinhaltet ein Filter und die Auto- bzw. Kreuzkorrelation.

### 4.6.2 MAC-Schicht

Im Gegensatz zu 802.11 kann eine Station jetzt nicht mehr selber ein BSS initiieren. Sie muss stets nach einem vorhandenen AP suchen. Diese Suche ist jetzt - im Gegensatz zu 802.11 - nur noch *passiv*; sie beschränkt sich auf die Suche einer Präambel eines Zeit-Frequenzpaketes.

#### 4 Modifikation von 802.11a für Spectrum Pooling

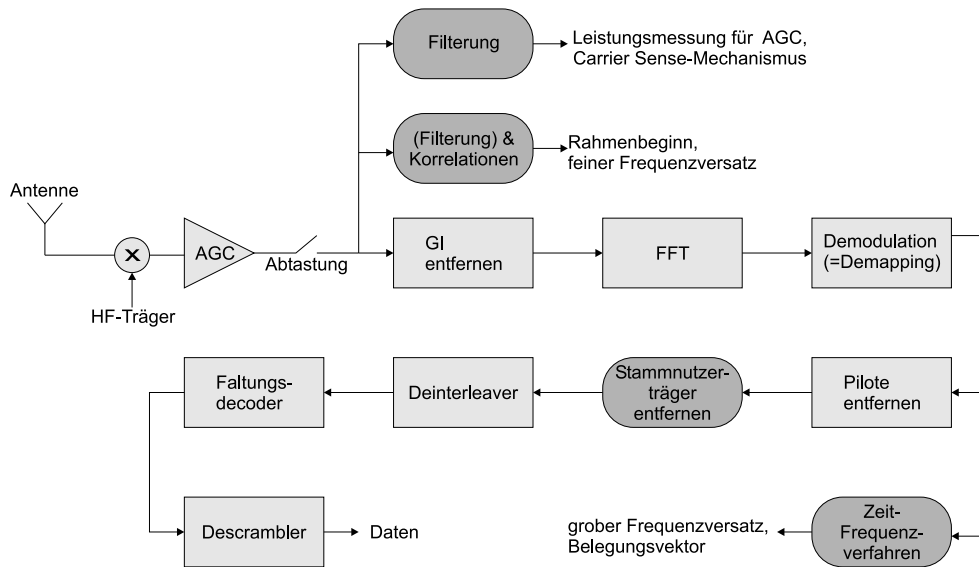


Abbildung 4.26: Physikalische Schicht mit Erweiterungen für Spectrum Pooling

Die MAC-Schicht muss Perioden festlegen, in denen besondere Pakete erwartet werden. Diese Perioden sind wichtig, um im Falle des Nichtempfangs der Pakete, selbständig den Status „nicht assoziiert“ einzunehmen. Diese Perioden werden benötigt für Beacons, Detektionsrahmen, Zeit-Frequenz-Signalisierung. Aufgrund der unterschiedlichen Stammnutzerpräsenz (denkt man z.B. an Truppenfunk, so wird dieser nachts weniger sein), ist es sinnvoll, diese Intervalle variabel zu halten. Eine neu eintretende Station wartet die Zeit-Frequenzsignalisierung für den BV und wird dann über alle anderen Perioden informiert. Auch die Leistung, mit die Jam-Signale im Boosting gesendet werden, wird flexibel gehalten. Die ideale Boosting-Leistung wird einen Mittelweg zwischen Stammnutzerstörung und Detektionssicherheit anstreben.

Die MAC-Schicht muss weiterhin garantieren, dass die Intervalle für Detektion, Beacons oder Zeit-Frequenzverfahren nicht übertrieben lange verzögert werden. Durch das asynchrone Zugriffsverfahren kann eine genaue zeitliche Positionierung dieser Pakete zwar nie garantiert werden, aber es sollte aufgrund einer noch laufenden Übertragung nie einer der angesprochenen Rahmen mehr als eine ganze Periode verzögert werden. Dafür muss die maximale Paketlänge entsprechend der gültigen Träger beschränkt werden. Rechenbeispiel (zunächst für 802.11a):

Ein MAC-Rahmen ist maximal  $2348\text{Byte}$ , also  $18784\text{Bit}$  lang.

Mit der Präambel und dem PHY-Rahmen zusammen sind es rund  $19000\text{Bit}$ . Bei langsamster Übertragung ( $BPSK, Rate 1/2$ ) auf 48 OFDM-Trägern ergibt sich eine Übertragungszeit von ca.  $3,2\text{ms}$ .

Dies ist für Spectrum Pooling im Normalfall zu lange. Typische Messintervalle sind hier z.B.  $1\text{ms}$ , es macht also Sinn, die maximale Paketlänge z.B. auf  $500\mu\text{s}$  zu beschränken. Dann würde sich für einen MAC-Rahmen eine maximale Infodatenmenge von  $400\text{Byte}$  ergeben. Dies gilt für Coderate  $1/2$  und  $BPSK$  auf 48 Trägern. Sind mehr Träger zur Verfügung oder ein höheres Modulationsverfahren möglich, so können natürlich mehr Daten in einen MAC-Rahmen gepackt

## 4.6 Ergebnisse und Zusammenfassung für das Systemdesign

werden. Will man stets die Paketlänge bei ca  $500\mu s$  halten, und die OFDM-Symboldauer ist  $4\mu s$ , so ist die Anzahl an Infodatenbytes  $D$ , die ein MAC-Rahmen tragen kann, grob nach folgender Formel zu berechnen:

$$D = \frac{500\mu s}{4\mu s} \cdot \frac{b \cdot q}{8} \quad (4.14)$$

dabei ist  $b$  die Anzahl der Infobits/Träger (abhängig vom Modulationsverfahren), und  $q$  die Anzahl der verfügbaren Träger. Hat man z.B. einen Pool mit 128 Trägern, der zu 70% belegt ist, und überträgt mit  $QPSKRate1/2$ , dann ist  $q = 38$ ,  $b = 1$ . Es ergibt sich für  $500\mu s$ -Pakete eine Infodatenmenge  $D \approx 600$  Byte.

Die Wartezeiten, die im verteilten Zugriffsverfahren von 802.11 die wesentliche Rolle für die Priorisierung spielen, können auch zusätzlich für die Detektion „missbraucht“ werden. Da die wartenden Stationen sowieso das Umgebungsrauschen auf Leistungen aus dem Mietnutzersystem beobachten müssen, ist es denkbar, diese Abtastwerte vor der Filterung der Stammnutzerkanäle zu speichern und sie bei der nächsten Detektionsphase mitzuverwerten. Dadurch ergibt sich eine starke Erhöhung der Abtastwerte, was die Detektion erheblich verbessert. Die eigentliche Messphase im Detektionsrahmen kann dann verkürzt werden, was sich positiv auf den Durchsatz im System auswirkt.

### 4.6.3 Ungünstige Sonderfälle

Für theoretische Untersuchungen und Simulationen wurden meist statistische Größen wie Mittelwerte oder Standardabweichungen verwendet oder bestimmt. Für ein gut funktionierendes System müssen allerdings auch für eine Reihe von Extremfällen Lösungen vorliegen.

1. Stationen, die aufgrund von hohen Stammnutzerfluktuationen oder anderen Störungen den Kontakt zum AP verloren haben, müssen diesen Zustand selbständig feststellen. Hierfür dient die bekannte Beacon-Periode. Sollte eine STA seit z.B. 3 Beacon-Perioden kein Beacon-Paket mehr empfangen haben, oder seit 3 Zeit-Frequenzperioden kein BV-Paket mehr empfangen haben, so darf sie nicht weiter am Zugriffsverfahren teilnehmen. Sie muss sich neu beim AP anmelden. Das heißt, dass sie zuerst das nächste Zeit-Frequenzpaket abwarten muss, um wieder einen gültigen BV zu erfassen.
2. Sollte der Pool durch Stammnutzeraufkommen so belastet sein, dass das Mietnutzersystem komplett ausfällt (Poolbelegung über 80%), dann werden alle Stationen selbständig ihren Zustand registrieren, und (s.o.) auf eine BV-Signalisierung warten. Es liegt nun in der Hand des AP, das Zeit-Frequenzpaket auf den Weg zu schicken, wenn der Pool wieder genügend Freiraum bietet. Allerdings kann er jetzt nicht mehr auf die Messunterstützung von Boosting- oder normalen Stationen zurückgreifen. Die Detektionsschwelle für die Stammnutzererkennung muss dann für diesen Fall im AP angepasst werden.

#### *4 Modifikation von 802.11a für Spectrum Pooling*

## 5 Abschliessende Bemerkungen und Zukunft von Spectrum Pooling

Spectrum Pooling ist sicherlich ein Ansatz, der außergewöhnliche Szenarien und deren Probleme in den Griff bekommt. Man muss jedoch auch stets an die Realisierung und die politische und finanzielle Dominanz der meisten Stammnutzer denken. Zwar ist es mit dem System, wie es in dieser Arbeit vorgestellt wurde (neben kleinen noch nötigen Untersuchungen), möglich, *ohne* zusätzlichen Signalisierungskanal zu arbeiten, was den tatsächlichen Einsatz erheblich erleichtert, dennoch bleibt es ungewiss, ob Spectrum Pooling bei den Pooleigentümern Akzeptanz gewinnen wird. Es kann finanziell für die Stammnutzer zwar interessant sein, es bleiben aber neben Spectrum Pooling auch noch andere Alternativen offen. So ist auch eine Neuausstattung mit Mobilfunkgeräten, die Kanalvergaben mit den zukünftigen Mietnutzern *aushandeln*, nicht völlig auszuschließen. Einfache Mobilfunkgeräte sind dank der Massenfertigung von Handys keine Großinvestition mehr. So werden die aufwendige Technik und die Ideen von Spectrum Pooling als anonyme Koexistenz sicherlich eine Übergangslösung bleiben. Eine ganz andere Sichtweise soll der nächste Abschnitt aufzeigen.

### Spectrum Pooling auch ohne Stammnutzer

Es scheint zunächst völlig sinnlos, über Spectrum Pooling *ohne* die Existenz von Stammnutzern zu reden. Man kann aber die Funktionalität, die Spectrum Pooling bietet, auch von einer anderen Seite interpretieren. Spectrum Pooling bietet nämlich eine sichere Übertragung in Bandbereichen, die schmalbandige Störer besitzen. Diese wurden normalerweise als Stammnutzer betrachtet. Sieht man diese Bandbereiche nicht mehr als Stammnutzer, sondern schlicht als Störer, so kann man Spectrum Pooling für erweiterte Robustheit gegen schmalbandige Störer einsetzen. Die freien Bänder, in denen Funk-LANs wie 802.11 operieren, sind auch für andere Geräte frei. So gibt es eine Vielzahl von Sprechfunk- und Videoübertragungsgeräten, die nicht den vollen Bandbereich nutzen, und genau solche schmalbandigen Störer darstellen. Setzt man Spectrum Pooling Mechanismen und Protokolle für solche Bänder ein, so kann eine erhöhte Effizienz erreicht werden.

Verwendet man dann 802.11a als Basissystem, so kann man sogar spezielle Mischnetze realisieren. Solange in einem System keine Störer auftauchen, kann das „alte“ System (ohne Spectrum Pooling-Erweiterung) normal arbeiten. Der moderne AP würde dennoch mit Detektionsrahmen die Umgebung beobachten. Alle Stationen, die in diesem Netz schon die neuen Erweiterungen für Spectrum Pooling besitzen, werden an den Spectrum Pooling-Abläufen teilnehmen. Die alten

## 5 Abschliessende Bemerkungen und Zukunft von Spectrum Pooling

Stationen können vom Detektionsrahmen dennoch den Header lesen, und werden das Mischnetz möglicherweise sogar erkennen können. Hierzu müssten diese Stationen lediglich über den Detektionsrahmen als besonderen Rahmen durch ein Softwareupdate informiert werden. (Es ist keine Änderung am PHY-Layer nötig!)

Sollten dann ein oder mehrere Störer auftreten, so können die alten Stationen keine Übertragung mehr aufrechterhalten, und die modernen Stationen im Netz gehen fließend zu Spectrum Pooling über, bis die Störer wieder unter die Messgrenze fallen.

### 5.1 Zukünftige Einsatzgebiete für Spectrum Pooling

Geräte, die selbstständig freie Funkbänder lokalisieren können, ohne die dort bestehenden Systemen nennenswert zu stören, werden sicherlich immer interessant bleiben. Die zunehmende Elektronisierung im Haushalt und von Alltagsgegenständen greift fast nur noch auf Funkübertragungen zurück. Sollte sich die Anzahl solcher Geräte schnell vervielfachen, ist bald keine Übertragung mehr möglich. Hier sind Spectrum Pooling-Techniken sehr interessant. So kann sich ein neues Gerät in seiner Umwelt (dem Spektrum) einpassen, ohne dass die Übertragungsstrukturen sämtlicher Konkurrenten neu organisiert werden müssen. Datenverkehr, der sich auf eine kleine räumlich Ausdehnung beschränkt, dort aber mit hohem Funkaufkommen zu kämpfen hat, ist idealer Einsatzort von Spectrum Pooling. Kombiniert man Ideen und Protokollmechanismen von Spectrum Pooling mit flexiblen Übertragungen und Modulationen, wie es in *software radio* schon lange diskutiert wird, so kommt man der ursprünglichen Idee des *open spectrum access* von Noam [NOA95] einen großen Schritt näher. Die Strukturen der Nutzung des elektromagnetischen Spektrums müssen flexibler gestaltet werden, um den zukünftigen Bedürfnissen zu genügen. Die Forderungen, die Systeme an die Funkstrecken stellen, werden stark von Ort zu Ort variieren. Die Dienste, die über Funkstrecken realisiert werden, sind so unterschiedlich, dass eine starre Vergabe von Band- oder Zeitbereichen immer uninteressanter wird. Auch die Kurzlebigkeit mancher Anwendungen (durch technologischen Fortschritt) benötigt schnelle Zuweisung von Ressourcen ohne großen behördlichen Aufwand. Kurzlebigkeit von Übertragungsbedürfnissen kann auch schlicht durch die Mobilität des Anwenders entstehen. Spectrum Pooling zeigt sich hier als moderne Idee in der schnelllebigen Welt der mobilen Kommunikation und kann viele Probleme der Ressourcenvergabe lösen.

# Abbildungsverzeichnis

3.1	802.11Komponenten . . . . .	8
3.2	Schichtenmodell von 802.11 . . . . .	9
3.3	MAC-Datenrahmen und Inhalte . . . . .	10
3.4	MAC-Managementrahmen . . . . .	11
3.5	CSMA/CA in 802.11 . . . . .	15
3.6	Hidden Terminal und RTS/CTS-Mechanismus . . . . .	16
3.7	Zeitsynchronisation mit Beacon-Frames . . . . .	18
3.8	Bandbreitenvorteil bei OFDM . . . . .	20
3.9	Aufbau des PHY-Rahmen . . . . .	22
3.10	Aufbau der Präambel in 802.11a . . . . .	23
3.11	Empfängerstruktur für Präambeln . . . . .	23
4.1	Koexistenz von Stamm- und Mietnutzern . . . . .	26
4.2	Typische Problemfälle bei der Detektion . . . . .	29
4.3	Detektionsrahmen . . . . .	29
4.4	Aufbau eines Pool mit Stammnutzer und OFDM-System . . . . .	30
4.5	Boosting neuer Stammnutzer . . . . .	31
4.6	Mapping in der zweiten Boosting-Phase . . . . .	33
4.7	Broadcast-Verfahren für den Belegungsvektor . . . . .	35
4.8	Verfahren für die grobe Frequenzversatzkorrektur . . . . .	40
4.9	Präambel zur Synchronisation von Rahmen und Trägerfrequenz . . . . .	41
4.10	Vergleich von Autokorrelationskurven bei verschiedenen Poolbelegungen - Korrelationslänge: 3 Symbole . . . . .	42
4.11	Vergleich von Autokorrelationskurven bei verschiedenen Poolbelegungen - Korrelationslänge: 8 Symbole . . . . .	43
4.12	Quote der richtig empfangenen Präambeln bei verschiedenen Voraussetzungen . . . . .	44
4.13	Standardabweichung der Schätzung des Rahmenbeginns bei verschiedenen Voraussetzungen . . . . .	44
4.14	Standardabweichung der Schätzung des Frequenzversatzes bei verschiedenen Voraussetzungen . . . . .	45
4.15	Kreuzkorrelation der empfangenen Präambel mit der gespeicherten Version . . . . .	46
4.16	Verschlechterung der Kreuzkorrelation mit zunehmendem Frequenzoffset . . . . .	47
4.17	Typisches Aussehen einer Korrelation mit bekanntem Signal . . . . .	48
4.18	Mehrfache Korrelation zur Erhöhung der Sicherheit . . . . .	49

## Abbildungsverzeichnis

4.19	Empfangsquote der Präambel für zwei Stammnutzerleistungen . . . . .	51
4.20	Standardabweichung des Frequenzversatzes . . . . .	52
4.21	Vergleich Periodogramm $\leftrightarrow$ kontinuierliches Spektrum . . . . .	57
4.22	Stammnutzer im Mietnutzerpool . . . . .	59
4.23	SNR im Pool wegen Störleistungen durch Zeitfensterung . . . . .	60
4.24	Empfangsleistung aus der Sicht eines Stammnutzers . . . . .	61
4.25	Verhältnis der Empfangsleistungen . . . . .	63
4.26	Physikalische Schicht mit Erweiterungen für Spectrum Pooling . . . . .	66



# Tabellenverzeichnis

3.1	Bedeutung der Adressfelder im MAC-Rahmen . . . . .	11
3.2	Datenraten und Parameter . . . . .	21
4.1	Länge der Pakete in Bit für die Übertragung des BV im Zeit-Frequenzverfahren .	37
4.2	Länge der Pakete in $\mu s$ für die Übertragung des BV im Zeit-Frequenzverfahren .	37
4.3	Länge der korrigierten Bündelfehler . . . . .	50
4.4	Relative, mittlere Leistungsanteile eines Stammnutzers auf den FFT-Abtastwerten	58



# Abkürzungsverzeichnis

Akronym	Beschreibung
ACK	acknowledgement
ADSL	asymmetric digital subscriber line
AGC	automatic gain control
AP	access point
ATIM	ad hoc traffic indication message
BSS	basic service set
BSSID	basic service set identifier
BV	Belegungsvektor
CF	coordination function
CFP	contention free period
CDM	code division multiplex
CP	contention period
CS	carrier sense
CSMA/CA	carrier sense multiple access with collision avoidance
CTS	clear to send
CW	contention window
DA	destination address
DAB	digital audio broadcast
DCF	distributed coordination function
DIFS	distributed inter frame space
DLL	data link layer
DS	distribution system
DSS	distribution system service
DSSS	direct sequence spread spectrum
ESS	extended service set
EIFS	extended inter frame space
FDM	frequency division multiplex
FH	frequency hopping
GI	guard interval
HDSL	high-bit-rate digital subscriber line
HDTV	high definition television
IBSS	independent basic service set

Akronym	Beschreibung
LAN	local area network
MAC	media access control
MLME	mac layer management entity
MSDU	mac service data unit
MTN	Mietnutzer
NAV	network allocation vector
OFDM	orthogonal frequency division multiplex
OSA	open system access
PC	point coordinator
PCF	point coordination function
PHY	physical layer
PIFS	point coordination function inter frame space
PLCP	physical medium layer convergence procedure
PLME	physical layer management entity
PMD	physical medium dependent
PSDU	physical service data unit
PSK	phase shift keying
QAM	quadratur amplitude modulation
QoS	quality of service
RA	receiver address
RTS	request to send
SA	source address
SAP	service access point
SIFS	short inter frame space
SNR	signal to noise ratio
SSID	service set identifier
STN	Stammnutzer
TA	transmitter address
TDM	time division multiplex
TIM	traffic indication map
TSF	timing synchronization function
WEP	wired equivalent privacy



# Literaturverzeichnis

- [ALM01] V. Almenar, S. Abedi, R. Tafazolli, „Synchronization Techniques for HIPERLAN/2“, IEEE Vehicular Technology Conference 54th , Vol 2,S. 762 -766, Fall 2001
- [BIA96] G. Bianchi, L. Fratta, M. Oliveri, „Performance evaluation and enhancement of the CSMA/CA MAC Protokoll for 802.11 Wireless LANs“, Proceedings PIMRC 1996, Taipei, Taiwan, S. 392-396, Oktober 1996.
- [CAL00] F. Calí, M. Conti, E. Gregori, „IEEE 802.11 Protocol: Design and Performance Evaluation of an Adaptive Backoff Mechanism“, IEEE Journal on selected areas in communication, Vol 18., No.9, S. 1774-1786, September 2000.
- [HIL02] J.Hillenbrand, „Erweiterung des HIPERLAN/2 Standards für den Einsatz in Spectrum Pooling Systemen“, Diplomarbeit am Institut für Nachrichtentechnik, Universität Karlsruhe, September 2002
- [IEEE8] The Institute of Electrical and Electronics Engineers, Inc, „International Standard ISO/IEC 8802-11, Wireless LAN Medium Access Control and Physical Layer specifications“, First edition, 1999.
- [IEEE9] The Institute of Electrical and Electronics Engineers, Inc, „Supplement to IEEE Standard for Information Technology, IEEE Std. 802.11a-1999, Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 Ghz Band“, Sep 1999
- [JON99] F. Jondral, „Nachrichtenübertragung“, Vorlesungsskript, Universität Karlsruhe, März 1999.
- [KAM98] K.D. Kammeyer, K. Kroschel, „Digitale Signalverarbeitung“, Teubner Studienbücher Elektrotechnik, 4. Auflage, Stuttgart 1998.
- [MIT99] J. Mitola, „Cognitive Radio for Flexible Mobile Multimedia Communications“, IEEE International Workshop on Mobile Multimedia Communications, 1999.
- [NOA95] E. Noam, „Taking the next step beyond spectrum auctions: open system access“, IEEE Communications Magazine, 33(12), Dezember 1995

## *Literaturverzeichnis*

- [OFD00] Y. Chiu, D. Markovic, H. Tang, N. Zhang „OFDM Reciver Design“, University of California at Berkeley Dept of Electrical Engineering and Computer Sciences, EE225C VLSI Signal Processing Fall 2000
- [RIC00] R. van Nee, R. Prasad „OFDM wireless multimedia communications“, Arctech House universal personal communications library, 2000.
- [SCH00] J. Schiller, „Mobile Communications“, Addison-Wesley, 2000.
- [TAS01] F. Capar, T. Weiss , I. Martoyo, „Transceiver Architekturen bei Spectrum Pooling, Meilenstein 1“, Juli 2001.

# Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Diplomarbeit

*Erweiterung des IEEE802.11 Standards für den Einsatz in Spectrum Pooling Systemen*

selbständig und ohne unzulässige fremde Hilfe angefertigt habe. Die verwendeten Literaturquellen sind im Literaturverzeichnis vollständig zitiert.

Karlsruhe, den 13.09.2002

Albert Krohn