DIPLOMARBEIT

Kanalzuweisung und verteilte Antennen in IEEE 802.11 Infrastruktur-Netzwerken

Robert Sombrutzki

Humboldt-Universität zu Berlin
Mathematisch-Naturwissenschaftliche Fakultät II
Institut für Informatik
Lehrstuhl für Systemarchitektur

Gutachter:

.....

.....

Betreuer: Dr. Anatolij Zubow

Berlin, 5. November 2009

Zusammenfassung

Moderne drahtlose Geräte nach IEEE 802.11a/g Standard ermöglichen Datenraten von bis zu 54 Mbit/s und mehr, der erreichte Durchsatz liegt jedoch aufgrund von Paketfehlern bzw. -verlusten meist deutlich darunter. Eine Ursache für diese Übertragungsfehler sind Interferenzen zwischen Geräten, die auf der gleichen Frequenz operieren. Der IEEE 802.11 Standard unterteilt das verfügbare Frequenzband in mehrere Kanäle, deren Verwendung die Störung zwischen parallelen Übertragungen reduziert. Die Kanalzuweisung ist dabei ein entscheidender Faktor und beeinflusst die Gesamtleistung des drahtlosen Netzwerkes erheblich. Ein weiterer Grund für Übertragungsfehler ist das Kanal-Fading infolge von Abschattung und Mehrwegausbreitung. Es ist ortsabhängig und so kommt es infolge von Mobilität zu Schwankungen im Kanal. Da das drahtlose Medium ein Broadcast-Medium ist, d. h. die gesendeten Pakete von mehreren Geräten empfangen werden, lassen sich mehrere Empfänger zu einer sogenannten verteilten Antenne zusammenfassen. Die bei den Empfängern auftretenden Fehler sind meist unabhängig voneinander und deshalb kann eine verteilte Antenne die Fehlerrate gegenüber einem einzelnen Empfänger reduzieren.

Beide Verfahren, Kanalzuweisung und verteilte Antennen, lassen sich jedoch nicht ohne weiteres miteinander kombinieren, da Ersteres von der Verwendung von vielen verschiedenen Kanälen profitiert, zweiteres jedoch voraussetzt, dass die Empfänger, welche eine verteilte Antenne bilden, den Kanal des Senders verwenden. Je mehr Kanäle verwendet werden, desto weniger Möglichkeiten gibt es also, verteilte Antennen zu bilden.

In dieser Arbeit werden Kanalzuweisung und verteilte Antennen mit Hilfe von Simulationen in verschiedenen Szenarien evaluiert. Dabei werden beide zunächst getrennt und anschließend in Kombination miteinander untersucht und ermittelt, welchen Einfluss sie auf den Durchsatz und die Latenz in einem drahtlosen Netzwerk haben.

Die Ergebnisse zeigen, dass besonders bei hoher Netzwerklast die Verwendung von mehreren Kanälen in Verbindung mit einer effizienten Kanalzuweisung den mittleren Durchsatz deutlich erhöht. Von verteilten Antennen profitieren besonders Verbindungen mit hohen Paketverlustraten. Hier kann sowohl die Latenz verringert als auch der Durchsatz gesteigert werden. Jedoch zeigt sich bei der Kombination von verteilten Antennen und Kanalzuweisung, dass in einem drahtlosen Netzwerk von mehreren Kanälen deutlich mehr profitiert wird als von verteilten Antennen und somit eine Reduzierung der Anzahl verwendeter Kanäle zugunsten besserer verteilter Antennen keinen Vorteil bringt.

Schlagwörter: Verteilte Antennen, Kanalzuweisung, Infrastruktur-Netzwerk, IEEE 802.11

Inhaltsverzeichnis

Kapitel 1

Einleitung

Drahtlose Netzwerke wurden in den vergangenen Jahren immer beliebter, bieten sie doch eine bequeme Möglichkeit, Zugang zum Internet oder z. B. dem Netzwerk der eigenen Firma zu erhalten. An vielen öffentlichen Orten wie beispielsweise Flughäfen, Bibliotheken und Einkaufszentren wird den Menschen die Möglichkeit geboten, kostenlos oder gegen Bezahlung über ein drahtloses Netzwerk im Internet zu surfen, E-Mails abzurufen oder mit Freunden zu chaten. Verschiedene Firmen u. a. T-Mobil richten dazu an stark frequentierten Plätzen sogenannte Hotspots ein[40]. Die Firma Fon[24] bietet sogar Geräte mit spezieller Software an, mittels derer die Kunden einen Teil der Bandbreite ihres privaten Breitband-Anschlusses mit anderen Menschen über einen drahtlosen Zugang teilen.

Der IEEE 802.11 Standard[1] definiert mehrere Möglichkeiten, wie ein solches drahtloses Netzwerk aufgebaut sein kann. Die beiden bekanntesten sind der *Ad-hoc-Modus* und der *Infrastruktur-Modus*. Letzterer findet bei den oben beschriebenen Szenarien am häufigsten Anwendung. Bei Infrastruktur-Netzwerken kommunizieren die Clienten über bzw. mit einem zentralen Gerät, dem sogenannten *Access Point* (AP). Dieser stellt zudem die Verbindung zum Intra- bzw. Internet zur Verfügung.

Immer mehr Geräte, wie z. B. Handys und Organizer, sind mit 802.11-fähiger Hardware ausgestattet und bieten so die Möglichkeit, auf das Internet zuzugreifen, um z. B. gemachte Fotos unmittelbar auf eine Webseite zu stellen. Die Anzahl der Benutzer solcher Geräte und Anwendungen wächst stetig. Zudem wächst der Bedarf an Bandbreite bei vielen Anwendungen, wie z. B. Video Streaming und Voice over IP (VoIP), da die Benutzer immer höhere Qualität verlangen. Moderne Hardware nach 802.11a/g Standard ermöglicht zwar Datenraten von bis zu 54 Mbit/s, jedoch liegen die tatsächlich erreichten Übertragungsraten meist deutlich darunter, da Interferenz und Fading (Abschattung, Multipath, ...) zu fehlerhaften Übertragungen und somit zu Paketverlusten führen.

Interferenz kann durch andere 802.11-Geräte verursacht werden, die auf dem selben Kanal operieren. Zwar wird versucht diese durch Zugriffsverfahren wie der *Distributed Coordination Function* (DCF) und der *Point Coordination Function* (PCF) zu reduzieren, jedoch können auch diese z. B. Kollisionen durch *Exposed Nodes* nicht vollständig verhindern. Interferenzen werden aber auch durch andere Geräte verursacht, welche im selben Frequenzband operieren, wie z. B. *Bluetooth*-Geräte und Mikrowellenherde. Fading wird u. a. durch Mehrwegausbreitung verursacht. Die Signale breiten sich über mehrere Pfade aus und treffen zeitlich verzögert und phasenverschoben beim Empfänger ein. Dort überlagern sie sich je nach Phasenlage destruktiv bzw. konstruktiv. Weitere Gründe für das Fading sind Pfadverlust aufgrund der Entfernung zwischen dem Sender und dem Empfänger und Abschattung (Shadowing) aufgrund der Sichtverhältnisse (Bäume, Wände etc.) im Ausbreitungspfad zwischen Sender und Empfänger. Das Fading kann sich zeitlich ändern und sowohl vom Ort als auch der Frequenz abhängig sein. Deshalb verursacht z. B. Mobilität Schwankungen des Fading und somit der Signalqualität.

Die Interferenz in einem drahtlosen Netzwerk kann durch die Verwendung mehrerer (nicht überlap-

Abbildung 1.1: Die Besucherzahlen öffentlicher Hotspots (z. B. Sonycenter in Berlin) unterliegen zeitlichen Schwankungen. Dadurch ergeben sich unterschiedliche Anforderungen an das Netzwerk.

pender) Kanäle minimiert werden, da die Geräte sich so weniger stören (Co-Channel Interferenz) und mehr Übertragungen parallel vorgenommen werden können. Jedoch ist die Anzahl der Kanäle beschränkt[2, 3] und besonders bei sehr großen Netzen muss die Wahl der Kanäle sehr gut geplant sein. Die Festlegung der geografischen Position, der Kanäle und der Sendeleistung der einzelnen APs in einem drahtlosen Infrastruktur-Netzwerk wird heutzutage häufig mit Hilfe von Software[42, 6], welche z. T. sogar in den Access Points oder einem zentralen Gerät des Netzwerken integriert ist[19], vorgenommen. Da sich in einem drahtlosen Netzwerk die Störungen aber stark und z. T. zeitlich schnell ändern können, sind solche statischen Einstellungen jedoch nicht optimal. Die Anzahl der Benutzer und somit auch die Stärke der Interferenz in einem drahtlosen Netzwerk kann zum Beispiel zeitlich variieren (siehe Abbildung 1.1). Dynamische Systeme versuchen durch Analyse des Netzwerkverkehrs die optimale Wahl der Kanäle für die einzelnen APs zu finden und erkennen dabei z. T. auch externe temporäre Störquellen und berücksichtigen diese Information bei der Auswahl und Zuweisung der Kanäle.

Fehlübertragungen werden, wie bereits erwähnt, durch Interferenzen und Fading verursacht. Letzteres ist dabei vom Ort und somit vom Empfänger abhängig. Eine Interferenzquelle hingegen kann u. U. bei mehreren räumlich getrennten Empfängern zu Störungen führen. Beispiele dafür wären z. B. Mikrowellenherde oder Radargeräte. Häufig ist jedoch auch die Wirkung einer Interferenzquelle auf kleinere Bereiche begrenzt und führt nur bei einzelnen bzw. wenigen Empfängern zu Störungen. Besonders bei Netzwerken mit geringer Dichte, sind die Schwankungen im Kanal, die zu Fehlübertragungen führen, meist abhängig vom Empfänger und somit ist es unwahrscheinlich, dass die selben Fehler bei allen Empfängern auftreten. Die Paketfehler sind also wenig korreliert. Die Wahrscheinlichkeit von Paketfehlern kann deshalb bei Verwendung zusätzlicher Empfänger insgesamt reduziert werden. Dabei wird die Broadcast-Eigenschaft des Mediums bei der drahtlosen Kommunikation genutzt, indem mehrere Empfänger, z. B. die APs in einem Infrastruktur-Netzwerk (Abbildung 1.2) eine verteilte Antenne bilden. Hier schlägt eine Übertragung nur dann fehl, wenn keiner der an der verteilten Antenne teilnehmenden APs das Paket erfolgreich empfangen konnte. Die APs sind über eine schnelle Datenleitung, z. B. Ethernet, mit einem Server verbunden. Dieser erkennt und verwirft zudem Pakete, die mehrfach, d. h. von mehreren APs empfangen wurden und bietet gleichzeitig den Zugang in andere Netze, z. B. dem Internet.

Die Verwendung einer Vielzahl von Kanälen in Verbindung mit effizienter Kanalzuweisung verringert die Störungen zwischen den drahtlosen Geräten und erhöht somit die Parallelität, d. h. es können mehr Übertragungen im selben Raum gleichzeitig vorgenommen werden. Mehrere Empfänger, welche den glei-

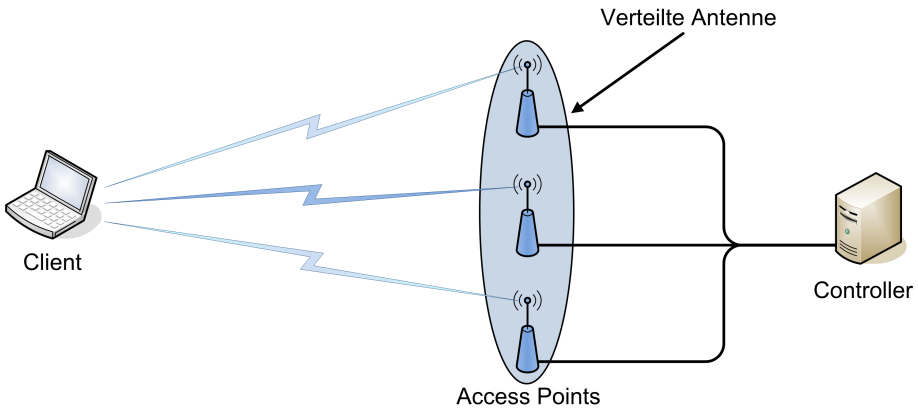

Abbildung 1.2: Prinzip einer verteilten Antenne: Mehrere APs sind mit einem zentralen Controller verbunden und leiten die empfangenen Pakete an diesen weiter. Eine Übertragung schlägt dabei nur fehl, wenn keiner der APs das Paket des Clienten empfangen hat.

chen Kanal verwenden, können zu einer verteilten Antenne gruppiert werden. Dadurch kann die Anzahl der Übertragungsfehler reduziert werden. Beide Verfahren erhöhen also die Übertragungsrate. Durch den Einsatz beider Verfahren könnte besonders in großen Infrastruktur-Netzwerken, wie z. B. öffentlichen Hotspots, der Durchsatz erhöht und die Latenz verringert werden. Jedoch lassen sich die beiden Ansätze nicht ohne Weiteres miteinander kombinieren. Wie bereits erwähnt, müssen die Empfänger innerhalb einer verteilten Antenne, also z. B. die Access Points in einem Infrastruktur-Netzwerk, den gleichen Kanal verwenden wie der Sender, während bei der Kanalzuweisung versucht wird, besonders nahe gelegenen APs möglichst verschiedene Kanäle zuzuweisen. Es muss also je nach Situation im Netzwerk, z. B. die Anzahl der Kanäle so gewählt und diese den einzelnen Geräte zugewiesen werden, dass entweder mehr verteilte Antennen gebildet werden können oder die Interferenz reduziert wird. Dabei ist u. a. die Frage zu klären, ob es Sinn macht, bei wenig Netzwerklast, z. B. einer geringen Zahl von Nutzern, die Anzahl der Kanäle zu verringern bzw. nicht alle zur Verfügung stehenden Kanäle zu nutzen, um so von mehr und besseren verteilten Antennen zu profitieren.

1.1 Ziel der Arbeit

In dieser Arbeit wird untersucht wie eine Kombination von Kanalzuweisung und verteilten Antennen in Infrastruktur-Netzwerken umgesetzt werden kann und unter welchen Voraussetzungen sich daraus ein Vorteil für die Gesamtleistung im drahtlosen Netzwerk ergibt. Dazu werden verschiedene Szenarien mit Hilfe von Simulationen evaluiert. Zunächst werden Kanalzuweisungsverfahren und verteilte Antennen getrennt untersucht. Ersteres ist ein Optimierungsproblem, für welches verschiedene Heuristiken mit geringerer Komplexität untersucht und verglichen werden. Für die Bildung von verteilten Antennen aus einer Gruppe von Access Points werden verschiedene Ansätze vorgestellt, bei denen die Kommunikationsprotokolle der Clienten so wenig wie möglich verändert werden sollen. Mit Hilfe dieser Ergebnisse der Evaluation lässt sich ein dynamisches Verfahren entwerfen, wie es Abbildung 1.3 illustriert und bei welchem lediglich Veränderungen an den Kommunikationsprotokollen der APs benötigt werden. Je nach Situation im drahtlosen Netzwerk, z. B. Anzahl der Benutzer und Netzwerklast, werden beide Verfahren, Kanalzuweisung und verteilte Antennen entsprechend so kombiniert, dass die Leistung des Netzwerkes bezüglich Durchsatz und Latenz optimiert wird.

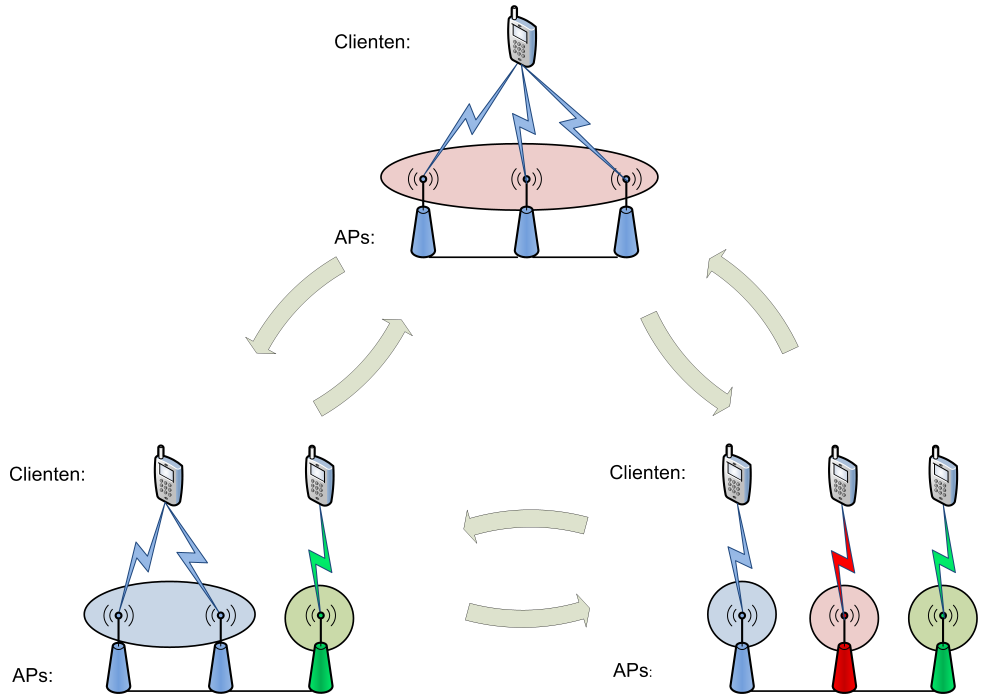

Abbildung 1.3: Die Kanalzuweisung und die verteilten Antennen werden in Abhängigkeit von der Anzahl der Nutzer bzw. der Netzwerklast festgelegt. Bei geringerer Last wird die Anzahl der Kanäle reduziert, um grössere verteilte Antennen realisieren zu können.

1.2 Aufbau der Arbeit

Das folgende Kapitel der Arbeit gibt zunächst einen Überblick über die wichtigsten Grundlagen des IEEE 802.11 Standards. Im Kapitel 3 werden verschiedene Ansätze für die Kanalzuweisung vorgestellt. Es werden außerdem Verfahren zur Bestimmung des für die Kanalzuweisung benötigten Interferenzgraphen erläutert. Im Kapitel 4 werden verschiedene Ansätze und MAC-Protokolle für verteile Antennen vorgestellt. Dabei wird zwischen Protokollen unterschieden, welche keine Änderung am 802.11 Clienten erfordern und solchen die auch dort neue Protokolle benötigen. Im Kapitel 5 wird die Realisierung im Netzwerk-Simulator JiST/SWANS erläutert. Dabei wird insbesondere darauf eingegangen, was bei gleichzeitiger Verwendung von mehreren Kanälen und verteilten Antennen berücksichtigt werden muss. Die Ergebnisse der Simulationen werden in Kapitel 6 dargelegt. Da für verschiedene Teile der Kanalzuweisung und für die verteilten Antennen mehrere Ansätze verfolgt wurden, sollen die Ergebnisse der Simulationen hier zeigen, welcher Ansatz jeweils die besten Ergebnisse hervorbringt. Eine Zusammenfassung der Arbeit und einen Ausblick werden in Kapitel 7 und 8 gegeben.

Kapitel 2

Grundlagen IEEE 802.11

2.1 IEEE 802.11

Die Anzahl und Größe drahtloser Netzwerke (*Wireless Local Area Networks*, WLANs) haben in den letzten Jahren sehr stark zugenommen. Im privaten Bereich schätzen viele die Möglichkeit, überall in der Wohnung, im Haus oder im Garten bequem im Internet zu surfen, sich Videos anzusehen oder E-Mails zu lesen ohne vorher Kabel verlegen zu müssen. Fast alle DSL-Provider liefern heutzutage zu einem DSL-Anschluss einen sogenannten *Access Point* (AP) mit, der es ermöglicht, drahtlos auf das Internet zuzugreifen. Aber auch an öffentlichen Orten wie beispielsweise Bahnhöfen und Einkaufszentren bieten viele Firmen und Geschäfte einen drahtlosen Internetzugang an. Da in immer mehr Geräten eine WLAN-Unterstützung integriert ist und sich viele neue Internetanwendungen auch an mobile Nutzer richten, wird die Anzahl drahtloser Netzwerke und der Benutzer weiter steigen. Dieses Kapitel soll einen kurzen Überblick über die Grundlagen der WLAN-Technologie geben.

Der 802.11 Standard[1] wurde im Juni 1997 verabschiedet und definiert neben einer *Mediumzugriffsschicht* (Medium Access Control Layer, kurz MAC-Layer) drei physikalische Schichten (PHY-Layer), ist also wie alle anderen 802-Standards auf den unteren beiden Schichten des OSI-Modells[37, S.33] angesiedelt. Die verwendeten Übertragungsverfahren Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) und Infrarot ermöglichen Datenraten von 1 und 2 MBit/s. Im Laufe der Zeit wurde dieser 802.11 Standard erweitert. So ermöglicht IEEE 802.11b[3] Datenraten von bis zu 11 MBit/s, 802.11a[2] und 802.11g[4] erreichen sogar 54 Mbit/s. Bei den beiden letztgenannten wird mit Orthogonal Frequency Division Multiplexing (OFDM) ein neues Übertragungsverfahren verwendet. Die Geräte nach 802.11a arbeiten dabei im Gegensatz zu den 802.11b/g-Geräten im 5 GHz- und nicht im 2.4 GHz-Frequenzband. Im weiteren Verlauf dieses Kapitels werden noch weitere 802.11 Standards vorgestellt, die unter anderem ein besseres Management der Geräte ermöglichen.

Der IEEE 802.11 Standard definiert verschiedene Arten von Netzwerken, die von drahtlosen Geräten, den Knoten, gebildet werden können. Die zwei bekanntesten und am häufigsten verwendeten sind, wie bereits erwähnt, Ad-hoc- und Infrastruktur-Netzwerke. Bei ersterem können zwei oder mehr Stationen direkt miteinander kommunizieren (Abbildung 2.1, rechts) und benötigen keine zentrale Kontrolle. Diese Art von Netzwerk eignet sich besonders, wenn es darum geht, spontan eine drahtlose Verbindung aufzubauen. Stationen, die in einem Ad-hoc-Netzwerk auf Grund zu großer Entfernung keine direkte Verbindung haben, können nicht miteinander kommunizieren. Erst zusätzliche Software ermöglicht es, Datenpakete eines Knotens von anderen Teilnehmern im Netz bis zum Ziel weiterleiten zu lassen. Je nachdem auf welcher Schicht das Weiterleiten der Pakete geschieht, spricht man vom *Forwarding* (MAC-Schicht) bzw. *Routing* (Netzwerk-Schicht). Es ermöglicht sehr große drahtlose Netzwerke aufzubauen und somit z. B. ganze Stadtteile drahtlos zu verbinden. Ein Beispiel für derartige Maschennetzwerke (Mesh-Network) ist

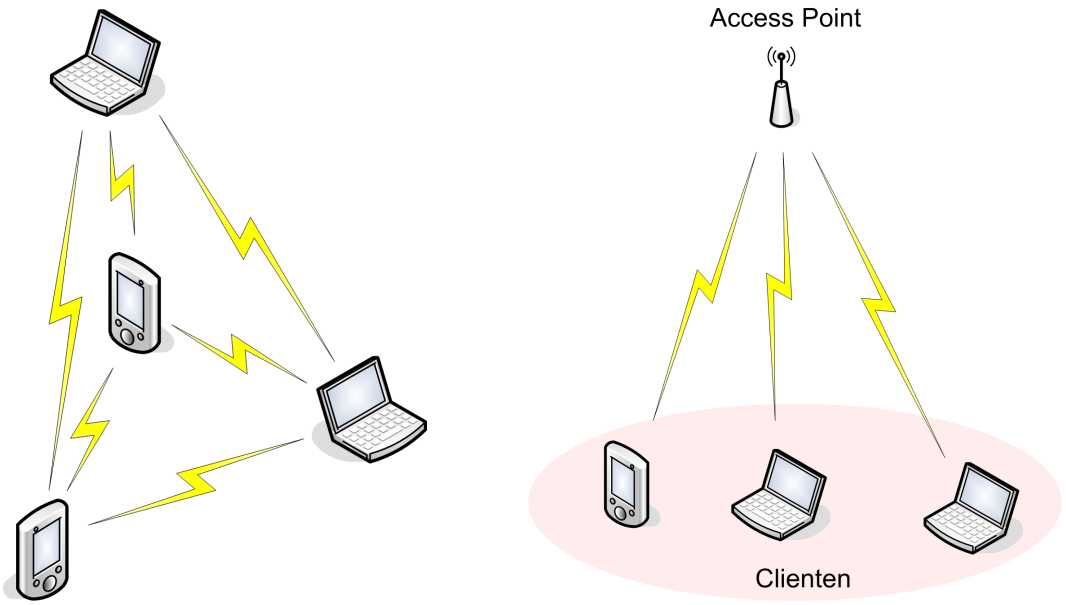

Abbildung 2.1: In einem Infrastruktur-Netzwerk (links) kommunizieren die Clienten mit Hilfe eines Access Points. In Ad-hoc-Netzwerken (rechts) tauschen die einzelnen Geräte die Daten direkt miteinander aus.

das Berliner Projekt "olsrexperiment.de" [34]. Mit 802.11s ist Forwarding in Maschennetzwerken auch im IEEE 802.11 Standard aufgenommen worden.

In Infrastruktur-Netzwerken kommunizieren die Stationen nicht direkt miteinander, sondern mit Hilfe eines ausgezeichneten Knotens, dem *Access Point* (AP) (Abbildung 2.1). Dieser ist meist über ein drahtgebundenes Netzwerk mit einem Gateway bzw. direkt mit dem Internet verbunden und stellt den Stationen (Clienten), einen drahtlosen Zugang zur Verfügung. Diese Art des drahtlosen Netzwerkes findet bei fast allen privaten WLANs Anwendung. Auch bei den meisten öffentlich zugänglichen WLANs handelt es sich um Infrastruktur-Netzwerke. Jedoch kommen hier mehrere, räumlich weit verteilte APs zum Einsatz, welche über ein sogenanntes *Distribution System* (DS) miteinander verbunden sind, um eine größere Fläche abdecken zu können. Der 802.11 Standard gibt nicht vor, ob das DS drahtgebunden oder drahtlos (Wireless Distribution System (WDS)) realisiert sein muss. Meist werden jedoch schnelle, drahtgebundene Netzwerke (Backbone) verwendet, wie es die Abbildung 2.2 exemplarisch zeigt.

2.2 Managementfunktion

Damit eine Station sich mit einem Infrastruktur-Netzwerk verbinden kann, sind einige Schritte nötig, welche in diesem Abschnitt erläutert werden. Zuerst muss die Station in Erfahrung bringen, welche drahtlosen Netzwerke sich in ihrer Reichweite befinden. Dies geschieht durch den *Scanning*-Prozess, wobei man hier zwei Arten unterscheidet: das passive und das aktive Scanning. Ein 802.11-Netzwerk wird über den *Service Set Identifier* (SSID) identifiziert. Dies ist der Netzwerkname und darf bis zu 32 Zeichen lang sein. Die APs in einem Infrastruktur-Netzwerk senden in regelmäßigen Abständen (Beacon-Intervall) sogenannte Beacon-Frames (Beacons) aus, die die grundlegenden Informationen des Netzwerkes enthalten. Dazu gehört unter anderem die SSID, der verwendete Kanal und Informationen zur Verschlüsselung.

Beim passiven Scanning wertet die Station die innerhalb eines bestimmten Zeitraums empfangenen Beacons aus. Sie wiederholt dies, wenn kein bestimmter Kanal eingestellt wurde, für alle verfügbaren

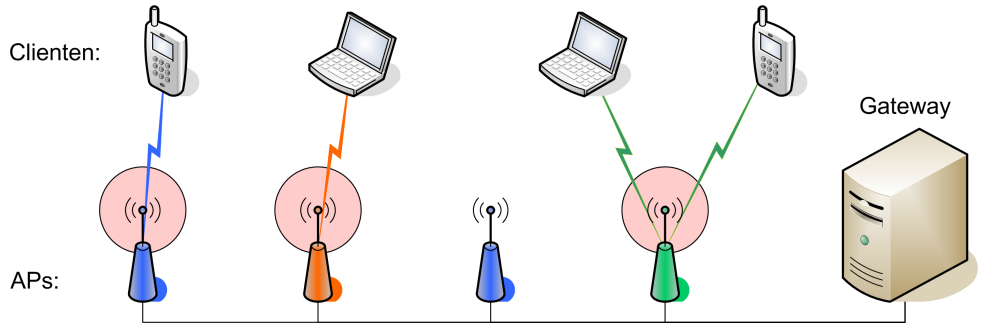

Abbildung 2.2: Infrastruktur-Netzwerk: Die Clienten (Stationen) verbinden sich mit dem Access Point mit der besten Signalqualität. Die Access Points sind über ein schnelles Netzwerk untereinander und mit einem Gateway verbunden, welche die Verbindung zum Internet zur Verfügung stellt und z. T. die APs kontrolliert.

Kanäle. Die Dauer, die eine Station während des Scanning auf einem Kanal verweilt, ist im 802.11 Standard durch die *MinChannel-* und *MaxChannel-Time* festgelegt. Beim aktiven Scanning kann die Station nach einem bestimmten Netzwerk mit einen bekannten Netzwerknamen suchen. Die Station sendet dazu Probe-Request-Frames aus, in denen die gewünschte SSID enthalten ist. Die APs, die diese SSID haben, senden daraufhin ein Probe-Response. Nach dem Aussenden der Probe-Request wartet die Station auf mögliche Probe-Response und wiederholt diesen Vorgang auf allen verfügbaren Kanälen.

Hat eine Station durch aktives oder passives Scanning die Beacon-Frames von mehreren APs empfangen, so wählt sie aus jenen mit der gewünschten SSID den mit der höchsten empfangenen Signalstärke (*Received Signal Strength Indication*, RSSI) aus[37, S.226] und stellt zu diesem eine Verbindung her. Dies geschieht durch die Authentifizierung und eine anschließende Assoziierung.

Es gibt dabei für die Authentifizierung zwei Verfahren: die Open System Authentication und die Sharded Key Authentication. Erstere ist allerdings keine wirkliche Authentifizierung, welche die Identität des Nutzer prüft, sondern das drahtlose Netzwerk ist bei Verwendung dieses Verfahrens für alle frei zugänglich. Bei der Sharded Key Authentication wird ein Challenge-Response-Verfahren mit einem gemeinsamen geheimen Schlüssel verwendet. Dies verhindert, dass Unerlaubte dem Netzwerk beitreten bzw. es benutzen können. Nach der Authentifizierung erfolgt die Assoziierung. Dazu sendet die Station dem AP ein Association-Request-Frame, welcher verschiedene Parameter, wie z. B. unterstützte Bitraten enthält. Der AP sendet der Station ein Association-Response, wenn sie die Anfrage akzeptiert. Dieses Frames enthält die *Association Identity* (AID), mit der die Station eindeutig identifiziert werden kann. Sie bestätigt den Empfang des Association-Response mit dem Senden einer Bestätigung. Der AP kann jedoch die Assoziierung der Station auch ablehnen. In diesem Fall gibt das Statusfeld des Association-Response[37] den Grund für die Ablehnung an (siehe Tabelle 2.1). Sollte der AP eine Station ablehnen, so sucht sich diese einen anderen AP mit der gewünschten SSID.

2.3 802.11 MAC-Schicht

Die MAC-Schicht von IEEE 802.11 stellt neben dem Frameformat auch Zugriffsverfahren zur Verfügung. Da das Medium bei der drahtlosen Kommunikation ein geteiltes Medium ist, muss durch eine Koordination sichergestellt werden, dass nicht von mehreren Teilnehmern gleichzeitig darauf zugegriffen wird. Sollten mehrere Knoten, deren Sendebereiche sich überlappen, gleichzeitig Daten senden, so kommt es zu einer Überlagerung der Signale. Ein Empfänger kann die einzelnen Signale u. U. dann nicht mehr

Tabelle 2.1: Statuscodes im Association-Response und ihre Bedeutung

Statuscode	Bedeutung
0	Erfolgreich
12	Assoziierung abgelehnt. Grund ist nicht im Standard festgelegt.
17	AP kann keine weiteren Stationen mehr annehmen, deshalb ist Assoziierung abgelehnt.
22	Assoziierung abgelehnt. Station unterstützt keine Spektrum-Management-Funktionen nach 802.11h.

erkennen und es kommt zu einer Kollision und somit zu Paketverlusten. Der 802.11 Standard kennt 2 Zugriffsverfahren: *Distributed Coordination Function* (DCF) und *Point Coordination Function* (PCF).

Bei letzterem wird der Mediumzugriff zentral durch einen sogenannten *Point Coordinator* kontrolliert. Dieses Zugriffsverfahren finden nur in Infrastruktur-Netzwerken Anwendung, wobei dort der AP die Rolle des Point Coordinator einnimmt. Die Zeit zwischen den vom AP gesendeten Beacons wird bei der PCF in zwei Phasen unterteilt. Während der *Contention Period* (CP) wird DCF verwendet. Innerhalb der *Contention Free Period* (CFP) bestimmt der AP welcher Client Pakete senden darf. Ein großer Nachteil von PCF ist der benötigte Koordinator, was den Einsatz dieses Zugriffsverfahren in verteilten Ad-hoc-Netzwerken unmöglich macht. Des weiteren ist das Verfahren komplex. Das ist auch der Grund, warum es so wenige Produkte gibt, die es unterstützen.

Die Zugriffsmethode DCF benötigt keine zentrale Koordination und wird somit auch in Ad-hoc-Netzwerken eingesetzt. Sie baut auf das vom leitungsgebundenen Ethernet IEEE 802.3 bekannte CSMA (*Carrier Sense Multiple Access*) auf, um den Zugriff auf das Medium zu regeln. Da ein Knoten jedoch nicht gleichzeitig senden und empfangen kann, kommt im Gegensatz zu 802.3 nicht CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) zum Einsatz, bei dem Kollisionen auf dem Medium erkannt werden, sondern es wird mit Hilfe von CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) versucht, Kollisionen zu vermeiden. Bei CSMA/CA prüft jeder Knoten bevor er Daten senden will, also auf das Medium zugreift, ob dieses schon belegt ist. Erst wenn es als frei erkannt wurde, beginnt das Gerät nach einem Backoff die Übertragung. Um die Fehlerfreiheit sicherzustellen, berechnet die MAC-Schicht mit Hilfe von CRC (*Cyclic Reduncancy Check*) für jedes Paket eine Prüfsumme und fügt diese hinzu. Der Empfänger kann somit die Korrektheit des Paketes überprüfen und quittiert dem Sender korrekt empfangene Pakete durch ein Acknowledgement-Frame (ACK). Der Sender überträgt Pakete, für welche er keine Bestätigung vom Empfänger erhalten hat, erneut (Retransmission), da er von einer Kollision ausgeht, auch wenn z. B. das Datenpaket erfolgreich übertragen wurde, das Acknowledgement-Frame jedoch nicht korrekt empfangen werden konnte. Die Anzahl der Neuübertragungen ist durch ein einstellbares Maximum begrenzt. Pakete, die auch nach der maximalen Anzahl von Neuübertragungen nicht erfolgreich übertragen wurden, verwirft der Sender.

Interframe Spaces

In einem 802.11-Netzwerk haben die gesendeten Daten unterschiedliche Prioritäten. So darf z. B. die Übertragung einer Bestätigung nach dem Empfang eines Paketes nicht durch eine anderen Datenübertragung gestört bzw. blockiert werden. Deshalb definiert der 802.11 Standard verschiedene Zeiten, welche zwischen zwei aufeinander folgenden Übertragungen gewartet werden muss, die sogenannten Interframe Spaces (IFS). Diese Zeit hängt dabei von der Art der Daten ab, welche ein Knoten übertragen will, wobei bei höher priorisierten Daten weniger Zeit gewartet werden muss. Dadurch darf ein Knoten, welcher Daten mit höherer Priorität, z. B. eine Empfangsbestätigung senden will, vor einem Knoten mit Daten

niedriger Priorität auf das Medium zugreifen. Der 802.11-Standard kennt folgende IFS:

- **SIFS (Short Interframe Space)**: Bei Frames mit höchster Priorität wie ACKs und RTS/CTS wartet der Sender die kürzeste Zeit.
- **PIFS (PCF Interframe Space)**: Innerhalb der CF-Periode muss eine Station diese Zeit vor dem Senden warten.
- **DIFS (DCF Interframe Space)**: Diese Zeit muss eine Station, die das Medium als nicht belegt erkannt hat, während der Contention Periode warten, bevor sie ein Paket sendet.
- **EIFS (Extended Interframe Space)**: Nach dem Empfang eines fehlerhaften Paketes muss eine Station diese Zeit warten, bevor sie das nächste Frame senden darf.

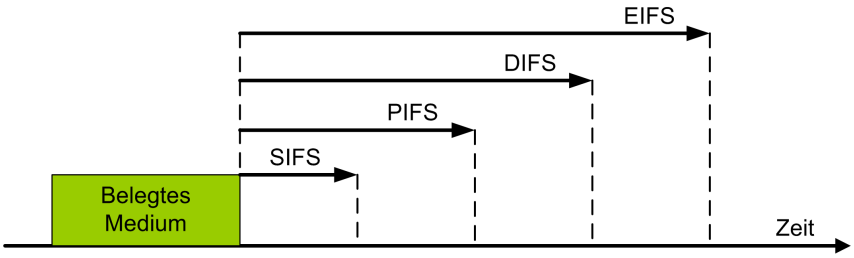

Abbildung 2.3: IEEE 802.11 definiert 4 verschiedene Zeiten, die zwischen 2 Übertragungen gewartet werden muss (Interframe Spaces). (Modifiziert aus [37])

2.4 Weitere IEEE 802.11 Standards

2.4.1 802.11h

In einigen Ländern Europas wird das von 802.11a verwendete 5 GHZ-Frequenzband auch von Radarsystemen und für die Satellitenkommunikation verwendet. Damit ist es dabei nicht zu Störungen kommt, erweitert 802.11h den 802.11a Standard um ein dynamisches Frequenzwahlverfahren (*Dynamic Frequency Selection*, DFS) und der Steuerung der Sendeleistung (*Transmission Power Control*, TPC). Letzteres stellt sicher, dass 802.11h-Geräte die Vorgaben der Europäischen Regulierungsbehörde einhalten. Mit Hilfe von DFS werden von Radar und Satelliten verwendet Frequenzen von 802.11h-Geräten nicht benutzt, um Störungen dieser Technologien zu verhindern. Die Geräte müssen dazu in der Lage sein, die Benutzung von Kanälen durch andere Geräte anhand gewisser Frequenzmuster bzw. Pulsfolgen zu erkennen und gegebenenfalls den Kanal zu wechseln[37]. Damit in Infrastruktur-Netzwerken nicht die Verbindung zwischen den Stationen und dem AP abbricht, wenn dieser den Kanal wechselt, signalisiert er einen Wechsel mit Hilfe der Beacons. Diese haben ein sogenanntes Channel-Switch-Announcement-Informationselement, welches den neuen Kanal, den Modus und die Dauer bis zum Wechsel enthält. Letzteres wird in der Anzahl von Beacons angegeben, die der AP auf dem alten Kanal noch bis zum Wechsel sendet. Der Modus ("Channel Switch Mode"-Feld) regelt, ob bis zum Kanalwechsel noch Daten ausgetauscht werden (0) oder ob die Stationen keine weiteren Daten mehr senden dürfen (1).

2.4.2 802.11k

In einem Infrastruktur-Netzwerk wählen die Clienten den besten AP anhand der Signalstärke der empfangenen Beacons, da davon ausgegangen wird, dass eine höhere Signalstärke in einer besseren Datenübertragung resultiert. Dabei werden zeitliche Schwankungen und Interferenzen jedoch völlig außer Acht gelassen. 802.11k Radio Resource Measurement (RRM) definiert eine Reihe von Messungen, deren Resultate zwischen den einzelnen Geräten (Stationen und APs) ausgetauscht werden können und die ein besseres Ausnutzen der vorhandenen Ressourcen ermöglichen sollen. Im 802.11k-Standard werden folgende Messungen definiert:

- **Beacon-Report**: Ein AP kann eine Station anweisen, ihm eine Zusammenfassung über die Beacons, die sie von einem oder mehreren BSSs auf bestimmen Kanälen empfangen hat, zu schicken. Dieser standardisierte sogenannte Beacon-Report enthält neben Informationen zu den Diensten, die diese APs anbieten, auch die Signalqualitäten.
- **Frame Report**: Dieser Report enthält Informationen über alle Frames, die eine Station von anderen Stationen während der Messung erhalten hat und kann von den APs angefordert werden. Neben der Anzahl der empfangen Pakete gehört zu diesem Report unter anderem auch die durchschnittlichen Signalstärke von jeder anderen Station.
- **Channel Load Report**: Der Channel Load Report enthält Information über die Dauer, während der das Medium von einem Gerät als belegt bzw. benutzt erkannt wurde. Diese Messung wird von einer Station durchgeführt, wenn ein AP diese Information anfordert.
- **Noise Histogram Report**: Diese Messung enthält die gemessene Stärke des Rauschens. Diese Information kann der AP von jeder Station erfragen.
- **Medium Sensing Time Histogram Report**: Mit Hilfe dieser Messung, die von den Stationen durchgeführt wird, erhält der AP Informationen über die statistische Verteilung der Dauer, während das Medium von den Stationen als belegt bzw. frei erkannt wurde.
- **STA Statistics Report**: Dieser Report enthält Informationen über die Verbindungsqualität und den Durchsatz und wird von der Station auf Anfrage an den AP gesendet.
- **Neighbor report**: Diesen Report kann der AP auf Anfrage der Station senden. Er enthält eine Liste von APs, die die Station bei einem Wechsel des APs (Roaming) verwenden kann. Der AP gewinnt die für diesen Report benötigte Information aus den Beacon-Reports aller seiner Stationen. Der AP kann mit diesem Report die AP-Wahl einer Station beeinflussen und so die Last im Netzwerk besser verteilen. Das Roaming wird durch den Neighbor report deutlich verbessert, da eine Station die Kapazität der potentiellen neuen APs schon vor einem Wechsel kennt.

Der 802.11k-Standard definiert zusätzlich, wie solche Messungen angefragt und die Ergebnisse ausgetauscht werden. Eine Station kann z. B. die APs in seiner Nachbarschaft anweisen, jeweils die Netzwerkauslastung zu messen. Auf Grundlage der Antworten kann sich die Station dann den am wenigsten verwendeten AP heraussuchen[38].

2.4.3 802.11v

Die Kontrolle des Netzwerkes durch den Administrator beschränkt sich zum größten Teil auf die APs. Der 802.11v Standard, an welchem seit Anfang 2004 gearbeitet wird, soll dies nun ändern und eine Konfiguration der Station durch das Netzwerk erlauben. Der Standard wird voraussichtlich 2010 fertig gestellt werden und soll folgende Funktionalität bieten:

- Die APs können den Stationen mitteilen, zu welcher SSID sie sich verbinden sollen. Es ist kein manuelles Einstellen der SSID auf Seiten der Stationen mehr nötig.
- "Wake on WLAN" (WoW) ermöglicht das Einschalten von drahtlosen Geräten mit Hilfe spezieller Pakete.
- Um die Netzwerklast besser über das gesamte Netzwerk zu verteilen, können AP die Stationen anweisen, zu einem anderen AP zu wechseln.
- Die APs haben die Möglichkeit, die von den Stationen verwendete Datenrate und den Kanal zu bestimmen.

Kapitel 3

Kanalzuweisung

In einem drahtlosen Netzwerk ist das Übertragungsmedium ein Broadcast-Medium, d. h. jeder, der in Reichweite eines Senders ist, empfängt das Paket oder erkennt zumindest eine Übertragung. Bei parallelen Übertragungen kommt es dabei zu Interferenzen. Der 802.11 Standard unterteilt deshalb das verwendete Frequenzspektrum in verschiedene Kanäle. Das von 802.11b/g verwendete Frequenzband von 2,4 bis 2,4835 GHz wird in 14 Kanäle mit je 22 MHz Breite unterteilt, welche sich z.T. überlappen (Abbildung 3.1). Der Kanal 5 z.B. befindet sich zwischen 2,421 und 2,443 GHz und überschneidet sich u.a. mit Kanal 6 (2,426 bis 2,448 GHz). Insgesamt gibt es bei 802.11b/g nur Kombinationen mit maximal 3 nicht überlappenden Kanälen. Der im 5 GHz operierende 802.11a Standard verwendet mehrere, nicht überlappende Kanäle zwischen 5,180 GHz und 5,835 GHz, die jeweils eine Breite von 20 MHz haben. IEEE 802.11a ist jedoch in Europa weniger verbreitet. Er unterliegt einer strengeren Regulierung und hat aufgrund der höheren Frequenz einen stärkeren Pfadverlust gegenüber 2,4 GHz und somit auch eine geringere Reichweite. Im weiteren Verlauf der Arbeit wird sich deshalb nur auf 802.11b/g bezogen.

Je nachdem, ob es zu Interferenzen zwischen Geräten kommt, welche den selben oder verschiedene Kanäle benutzen, wird zwischen 2 Arten von Interferenz unterschieden: Co-Channel Interferenz und Adjacent Channel Interferenz[28]. Ersteres bezeichnet die Interferenz zwischen zwei Teilnehmern, die die selbe Frequenz verwenden. Adjacent Channel Interferenz wird durch eine starke Abstrahlleistung auf einem benachbarten Kanal verursacht. Zu Adjacent Channel Interferenz kann es dabei auch zwischen Knoten kommen, welche keine überlappenden Kanäle verwenden, wie Zubow et al. in [28] zeigt.

Durch die Verwendung mehrerer nicht überlappender Kanäle kann in einem 802.11 Netzwerk die Interferenz reduziert und die Kapazität erhöht werden. Heutzutage wird dazu häufig jedem Knoten ein Kanal fest zugewiesen. Dabei wird versucht, Knoten, die miteinander interferieren, unterschiedliche, nicht überlappende Kanäle zuzuweisen, was besonders in sehr dichten Netzen nicht immer möglich ist. Dabei handelt es sich um eine statische Kanalzuweisung. Da der Umfang des Netzwerkverkehrs, die Anzahl der Benutzer und auch die Menge an Störungen durch andere Geräte, wie Bluetooth, zeitlich stark variieren, ist dieses Verfahren nicht optimal.

Die Kanalzuweisung muss in einem solchen, sich häufig verändernden Netz immer wieder an die aktuelle Situation angepasst werden. Man spricht deshalb von dynamischer Kanalzuweisung. Dazu muss der aktuelle Netzwerkverkehr analysiert und externe Störquellen erkannt werden. Bei einem zentral kontrollierten Netzwerk, wie man es häufig bei WLANs an öffentlichen Plätzen oder innerhalb von Firmengebäuden finden, ist dies sehr einfach zu realisieren. Ein zentraler Rechner sammelt dazu die Information von allen APs und wertet diese aus. Er kann dabei z. B. fremde Netzwerke oder andere Störquellen entdecken. In [35] stellt Bahl et al. ein System vor bei welchem PCs mit preiswerten WLAN-Adaptern ausgestattet werden und mit Hilfe der von ihnen gesammelten Informationen u. a. die Netzwerkauslastung bestimmt und fremde Netzwerke erkannt werden können. In Infrastruktur-Netzwerken kann durch

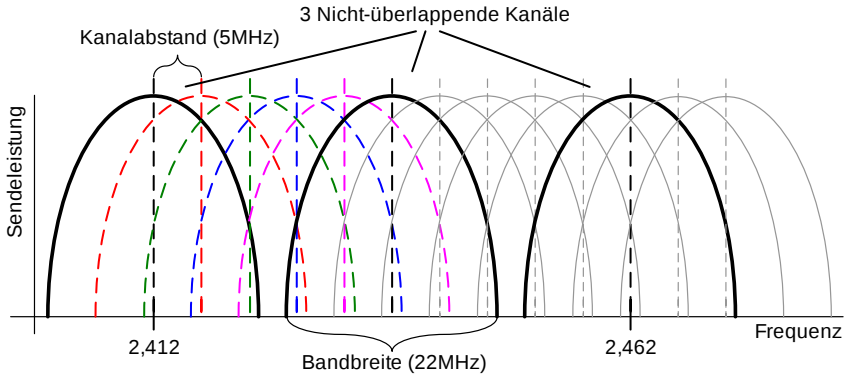

Abbildung 3.1: Die von IEEE 802.11 b/g verwendeten Kanäle im Bereich von 2,4 bis 2,4835 GHz überlappen sich teilweise. Dadurch kann es auch bei Verwendung unterschiedlicher Kanäle zu Interferenzen kommen (Adjacent Channel Interferenz). Die hier stärker gezeichneten Kanäle 1, 6 und 11 überlappen sich nicht.

Messungen, welche die APs selbst durchführen, die Stärke der Interferenz zwischen ihnen bestimmt werden. Durch diese Information kann eine optimale Kanalzuweisung gefunden werden. Durch permanentes Messen und Anpassen dieser Kanalzuweisung entsteht so ein Regelsystem, welches sich der vorliegenden Situation im Netzwerk anpasst.

Im folgenden werden einige Methoden zur Bestimmung der Interferenz vorgestellt, potenzielle Probleme aufgezeigt und mögliche Lösungsansätze diskutiert. Darüber hinaus werden Algorithmen zur Bestimmung der optimalen Kanalzuweisung besprochen. Dabei wird unterschieden, ob diese die Interferenz der Stationen (Clienten) und den Netzwerkverkehr berücksichtigen oder dieses außer Acht lassen. Da diese Algorithmen durch ihre hohe Komplexität sehr zeitaufwändig sind und somit in einem realen System nicht praktikabel sind, werden zusätzlich einige Heuristiken vorgestellt.

Die Kanalzuweisung wird anhand eines Infrastruktur-Netzwerkes erläutert, bei welchen APs den Clienten den Zugang zum Netzwerk zur Verfügung stellen.

3.1 Interferenzgraph

Entscheidend für eine effiziente Kanalzuweisung ist die Genauigkeit, mit der man die Interferenz zwischen den einzelnen Geräten in einem drahtlosen Netzwerk bestimmt. Zur Darstellung der Interferenz wird häufig ein Graph verwendet, der sogenannte Interferenzgraph. Jeder Knoten des Graphen repräsentiert dabei einen Netzwerkteilnehmer. Die Kanten zwischen den Knoten geben an, ob zwischen den entsprechenden Geräten Interferenzen vorliegt. Je nachdem wie detailliert man die Interferenz wiedergeben will, verwendet man verschiedene Arten von Graphen:

- ungerichteter, ungewichteter Graph: Eine Kante zwischen den Knoten entspricht vorhandener Interferenz.
- ungerichteter, gewichteter Graph: Das Gewicht der Kante gibt die Stärke der Interferenz an.
- gerichteter, gewichteter Graph: Das Gewicht der Kante gibt Stärke der Interferenz an, welche asymmetrisch sein kann.

Die Kantengewichte eines gewichteten Interferenzgraphen liegen im Intervall von 0 und 1, wobei ein hoher Wert starke und ein niedriger Wert geringere Interferenz widerspiegelt. Welche Art von Interferenzgraph verwendet wird, hängt davon ab, welche Möglichkeiten zur Bestimmung der Interferenz verwendet werden und welche Information der Algorithmus für die Kanalzuweisung benötigt. Grundsätzlich führt genaueres Wissen über die Interferenz zu besseren Ergebnissen.

3.1.1 Bestimmung des Interferenzgraphen

In diesem Abschnitt sollen verschiedene Verfahren zur Bestimmung des Interferenzgraphen vorgestellt werden. Diese unterscheiden sich sowohl in der Komplexität als in der Genauigkeit, mit der sie die Interferenz wiedergeben. Besonders Störungen von externen Störquellen oder anderen Netzwerken werden nicht von allen erfasst. Ein großer Unterschied liegt auch in der Umsetzbarkeit der einzelnen Verfahren. Einige haben hohe Anforderung an die Hardware, z. T. muss diese auch verändert werden.

Modell

In [21] benutzten Al-Rizza et al. ein Pfadverlustmodell, um die Stärke, mit der eine Station das Signal einer anderen empfängt zu berechnen:

$$PL\left(d_{i,j}\right) = PL_0 + 29,4 \lg\left(\frac{d_{ij}}{d_0}\right) + 6,1 x_a \lg\left(\frac{d_{ij}}{d_0}\right) + 2,4y + 1,3 x_s y$$

Dabei ist $d_{i,j}$ der Abstand zwischen den Knoten i und j, PL_0 ist der Pfadverlust und x_a, x_s und y sind voneinander unabhängige, gaußverteilte Zufallszahlen, welche Effekte wie Abschattung usw. modellieren. Es muss also lediglich die Positionen der einzelnen Knoten bekannt sein. Sollten in einem Infrastruktur-Netzwerk neben den Positionen der APs, auch jene der Stationen bekannt sein, so können diese bei der Kanalzuweisung berücksichtigt werden. Aus der Position und der Sendeleistung eines Knotens, kann die empfangene Signalstärke bei den anderen errechnet werden. Diese gibt bei diesem Modell gleichzeitig die Stärke der Interferenz wieder, wobei eine hohe Signalstärke starke Interferenz bedeutet und visa vi.

Für die Praxis ist ein solches Verfahren wenig sinnvoll. Es kann z. B. nicht angegeben werden, ob zwischen zwei gegebenen Knoten Sichtverbindung herrscht (Line-of-sight, LOS) oder sich zwischen beiden Hindernisse befinden (Non-Line-of-sight, NLOS). Stattdessen werden z. B. Abschattung und Mehrwegausbreitung nur mittels gaußverteilten Zufallszahlen stochastisch modelliert.

RSSI-Messungen

Im letzten Abschnitt wurde die empfangene Signalstärke berechnet, jedoch macht es in realen Netzwerken mehr Sinn, diese direkt zu messen. Die Received Signal Strength Indication (RSSI) ist ein Indikator für die empfangene Signalstärke. Alle Geräte geben diesen Wert für jedes empfangenen Paket an. Er wird, wie in Abschnitt 2.2 beschrieben, u. a. von Clienten verwendet, um den AP mit der besten Verbindung zu bestimmen.

Jeder Knoten sendet eine Reihe von Paketen, während alle anderen die Signalstärke der empfangen Pakete und den Rauschpegel messen. Letzteres ist notwendig, da bei einigen das Signal des Senders evtl. so schwach ist, dass es nicht reicht, um es zu dekodieren. Jedoch können selbst solche schwachen Signale Störungen verursachen. Des weiteren gibt es eine Phase, während keiner der Knoten ein Paket sendet. In dieser Zeit messen alle noch einmal den Rauschpegel. Dies dient als Referenzwert, um eine Erhöhung des Rauschpegel während des Sendevorgangs zu erkennen.

Dieses Verfahren ist relativ einfach zu implementieren. Zudem können in einem Infrastruktur-Netzwerk auch die Clienten berücksichtigt werden, wenn diese an der Messung teilnehmen. Die Qualität der Messung hängt jedoch stark von der Implementierung und der Genauigkeit der Messung der Signalstärke ab.

Auch bei diesem Verfahren ist die empfangene Signalstärke ein Indikator für die Interferenz, wobei hohe Signalstärken starke Interferenzen bedeuten und visa vi.

Koordiniertes Probing

Eine weitere Möglichkeit die Interferenz zwischen zwei Knoten im Netzwerk zu bestimmen, ist das von Ahmed et al. vorgeschlagene *Koordinierte Probing*[7]. Dabei sendet ein Knoten N_1 ein Paket an einen beliebigen dritten Knoten N_3, welche dieses mit einem ACK bestätigt. Zeitgleich zu dieser Bestätigung, sendet der Knoten N_2 ein Paket. Wenn das ACK des dritten Knoten N_3 nicht von dem Knoten N_1 empfangen werden kann, so deutet dies auf Interferenz zwischen den Knoten N_1 und N_2 hin. Das Verfahren benötigt veränderte Hardware bei den Knoten, da sie auf Pakete reagieren müssen, die nicht an sie adressiert sind und dies zeitlich sehr genau abgestimmt sein muss. Des weiteren ist die Korrektheit in Frage zu stellen, da starke Unterschiede zwischen den Signalstärke von N_2 und N_3 die Messung verfälschen können. Sollte die Signalstärke von N_3 deutlich über der von N_2 liegen, so kann N_1 das Paket von N_3 empfangen (Capture-Effekt). Das Signal von N_2 wird von N_1 dann lediglich als Rauschen wahrgenommen. Es wird in diesem Fall jedoch fälschlicherweise davon ausgegangen, dass die beiden Knoten nicht interferieren.

Maximum Throuput-Verfahren

In [23] schlägt Rozner et al. ein einfaches Verfahren zur Bestimmung der Interferenz vor. Ein Knoten A sendet zunächst für eine Zeitdauer t mit maximaler Rate. Aus der Anzahl der gesendeten Pakete und t lässt sich die Rate R_A bestimmen. Der Knoten wiederholt dies, jedoch sendet nun ein weiterer Knoten B ebenfalls mit der maximalen Rate. Der Knoten A erzielt dabei eine Senderate von R_A^{AB} und Station B erreicht R_B^{AB}. Die Stärke der Interferenz zwischen den Knoten A und B kann nun aus dem Verhältnis der Senderaten bestimmt werden. Je stärker die Senderate von A reduziert wurde, als der Knoten B gleichzeitig gesendet hat, desto stärker ist die Interferenz. Das Verhältnis V_A^{AB} gibt also an, wie stark B den Knoten A stört.

$$V_A^{AB} = \frac{R_A^{AB}}{R_A}$$

Der aus dieser Messung resultierende Interferenzgraph ist ein gewichteter und gerichteter Graph. Durch Verwendung des Mittelwerts V^{AB} von beiden berechneten Werten wird der Interferenzgraph ein ungerichteter Graph. Jedoch wird dabei die möglich Asymmetrie der beiden Interferenzen nicht beachtet, welche z. B. durch unterschiedliche Sendeleistung hervorgerufen werden kann.

$$V^{AB} = \frac{\frac{R_A^{AB}}{R_A} + \frac{R_B^{AB}}{R_B}}{2}$$

Das Verhältnis wird umso geringer, je größer die Störung ist, da die Senderate der einzelnen Knoten durch das parallele Senden geringer wird. Bei einem Verhältnis von 1 liegt keine Störung vor, während ein Wert von 0,5 zeigt, dass sich beide Knoten das Medium fair teilen. Für den Interferenzgraphen wird aus dem Verhältnis V^{AB} ein Interferenz-Wert ermittelt:

$$\textit{Linkinterferenz} = 2 - 2 \cdot V^{AB} = 2 \cdot (1 - V^{AB})$$

Dadurch wird zum einem der Wertebereich vergrößert (0 bis 1), zu anderem wird dadurch auch die Bedeutung umgekehrt: Kleine Werte geben kleine Interferenzen an und umgekehrt.

Für einen vollständigen Interferenzgraphen muss jeder der n Knoten im Netzwerk alleine und mit jedem anderen gemeinsam Pakete senden. Das Verfahren ist somit zeitlich sehr aufwendig. Es hat eine zeitliche Komplexität von $O(n^2)$, d. h. die Anzahl der durchzuführenden Messungen steigt quadratisch mit der Anzahl der Knoten im Netz:

$$\begin{aligned} F &= n + \binom{n}{2} \\ &= \frac{n^2 + n}{2} \end{aligned}$$

Da die Stärke der Interferenz auf verschiedenen Kanälen unterschiedliche sein kann, muss die Messung auf allen verwendeten Kanälen wiederholt werden. Da diese Methode zur Bestimmung der Interferenz auf gängiger Hardware sehr einfach zu implementieren ist und dabei eines der genauesten, der hier vorgestellten Verfahren ist, wird es im weiteren Verlauf der Arbeit verwendet. Die anderen Ansätze können jedoch ebenfalls verwendet werden.

3.1.2 Externe Störquellen

Die Messung des maximalen Durchsatzes, welche im vorherigen Kapitel beschrieben wurde, ermöglicht auch das Erkennen von externen Störquellen. Da diese auf den verwendeten Kanälen verschieden stark sein können, werden die Messungen auf allen Kanälen wiederholt. Die Stärke der Störung auf einem Kanal c ergibt sich aus dem Verhältnis von erreichter und maximal möglicher Senderate MR_A.

$$S(c) = \frac{R_A(c)}{MR_A}$$

Der Wert für $S(c)$ liegt zwischen 0 und 1, wobei bei stärkerer Störung $S(c)$ kleiner ist und visa vi. Im Interferenzgraphen wird jedoch eine starke Interferenz durch ein großes Gewicht wiedergegeben und deshalb wird für die Stärke der Interferenz durch externe Quellen folgende Wert bestimmt:

$$\mathit{ExterneInterferenz}(c) = 1 - \frac{R_A(c)}{MR_A}$$

Im Interferenzgraphen wird für jeden Kanal ein zusätzlicher "Störknoten" hinzugefügt. Die Knoten des Graphen, welche jeweils ein Knoten im Netzwerk darstellen, erhalten zu diesem Störknoten eine Kante, falls sie auf dem entsprechenden Kanal eine externe Störquelle festgestellt haben, wobei das Gewicht der Kante die Stärke der Interferenz repräsentiert.

Die Abbildung 3.2 zeigt ein Beispiel für einen solchen Interferenzgraphen. Die Knoten A und C werden durch eine externe Störung beeinflusst. Die Quelle der Störung muss für beide nicht die selbe sein, was jedoch für die Kanalzuweisung und somit für den Graphen keine Rolle spielt.

3.1.3 Interferenzen beim Client

In einem Infrastruktur-Netzwerk kann bei der Kanalzuweisung neben der Interferenz bei den APs auch jene bei den Clienten berücksichtigt werden. Dazu muss diese aber bekannt sein. Die in den letzten

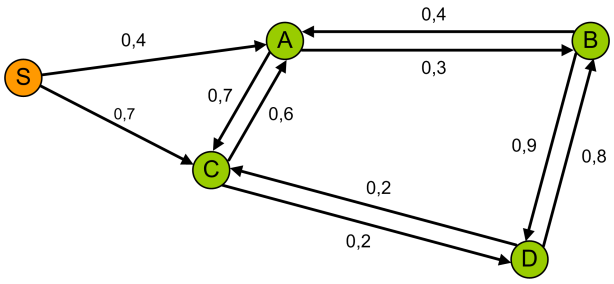

Abbildung 3.2: Beispiel für einen Interferenzgraphen mit vier Netzwerkknoten (A bis D) und einer Störquelle S. Die Knoten B und D werden nicht durch eine externe Quelle gestört.

Abschnitten vorgestellten Verfahren benötigen dazu z. T. Änderung an der Soft- bzw. Hardware der Clienten. Der 802.11k Standard definiert verschiedene Messungen, die eine Station unterstützen muss und welche ebenfalls eine Messung der Interferenz zulassen, was sich jedoch auf das Bestimmen von Signalstärken und freier Mediumzeit beschränkt (Kapitel 2). Da gängige Hard- bzw. Software den 802.11k Standard noch nicht unterstützt, wird im Rahmen der Arbeit darauf nicht weiter Bezug genommen.

3.2 Kanalseparationsmetrik

Die bei 802.11b/g verwendeten 14 Kanäle liegen im Bereich von 2,4 GHz bis 2,4835 GHz und haben einen Abstand von 5 MHz. Da die verwendete Bandbreite jeweils 22 MHz beträgt, überlappen sich die Kanäle zum Teil. Damit sich die verwendeten Kanäle nicht überlappen, müssen diese mindestens 5 Kanäle auseinander liegen. Daraus ergeben sich einige Kombinationen von Kanälen, wie z. B. 1, 6 und 11. Durch die Verwendung von überlappenden Kanälen kommt es zwischen den Knoten ebenfalls zu Interferenzen. Man spricht dabei von Nachbarkanalstörung (*adjacent-channel interference*, ACI). Um diese bei der Kanalzuweisung ebenfalls zu berücksichtigen, wird eine sogenannte Kanalseparationsmetrik verwendet.

$$Kanalseparation(i,j) = \min(|C_i - C_j|, 5)$$

Die Kanalseparation zweier Knoten ist das Minimum vom Abstand ihrer verwendeten Kanäle und dem minimalen Abstand zweier nicht überlappender Kanäle. Bei IEEE 802.11b/g liegen zwei nicht überlappende Kanäle mindestens fünf Kanäle auseinander. Ein größerer Abstand zwischen den verwendeten Kanälen führt dazu, dass sich zwei Knoten nicht mehr stören. Die Kanalseparation wird bei der Berechnung der Gesamtinterferenz zwischen zwei Knoten auf eins normiert und von eins subtrahiert, damit entsprechend dem Interferenzgraph auch hier eine stärkere Störung durch einen höheren Wert repräsentiert wird. Durch diese Umformung erhält man die Kanalinterferenz. Für die Interferenz zwischen zwei Knoten auf beliebigen Kanälen (Gesamtlinkinterferenz) wird die Interferenz zwischen beiden (Linkinterferenz), welche man dem Interferenzgraphen entnimmt, mit der Kanalinterferenz gewichtet (Listing 3.1). Der Zusammenhang zwischen Kanalseparation und Gesamtlinkinterferenz ist linear. Halbiert sich der Kanalabstand, so verdoppelt sich die Gesamtlinkinterferenz.

Listing 3.1: Interferenz unter Berücksichtigung der Kanalseparation

```
Kanalseparation(i,j) = min(|Ci - Cj|, 5);
Kanalinterfrenz(i,j) = 1 - Kanalseparation(i,j) * 1/5;
Gesamtlinkinterferenz(i,j) = Kanalinterferenz * Linkinterferenz;
```

Zubow et al. zeigte in [28], dass Adjacent-Channel Interferenz nicht nur von den verwendeten Kanälen abhängt, sondern auch vom Abstand zwischen den Knoten. Es wurde in Experimenten beobachtet, dass es auch zwischen Knoten zu Störungen kam, obwohl diese nicht überlappende Kanäle verwendeten, wenn sie sehr dicht beieinander standen. Diese Störungen traten bis zu einer Distanz von ungefähr 2 Metern auf. Die Dichte in aktuellen Infrastruktur-Netzwerken liegt aber deutlich darüber, so dass die Ergebnisse hier nicht weiter berücksichtigt werden.

Der 802.11a Standard benutzt im Gegensatz zu 802.11b/g das 5-GHz-Frequenzband. In Europa stehen insgesamt 19 Kanäle in diesem Bereich zur Verfügung, welche jeweils 20 MHz breit sind. Der Abstand zwischen ihnen beträgt 20 MHz. Die Kanäle überlappen sich bei 802.11a dem entsprechend nicht. Die Kanalseparationsmetrik lautet deshalb:

$$Kanalseparation(i,j) = \min(|C_i - C_j|, 1)$$

Die Gesamtinterferenz zwischen zwei Geräten i und j, welche die Kanäle C_i und C_j verwenden, bestimmt sich deshalb bei 802.11a wie folgt:

Listing 3.2: Interferenz unter Berücksichtigung der Kanalseparation

```
Kanalseparation(i,j) = min(|Ci - Cj|, 1);
Kanalinterfrenz(i,j) = 1 - Kanalseparation(i,j);
Gesamtlinkinterferenz(i,j) = Kanalinterferenz * Linkinterferenz;
```

3.3 Kanalzuweisung: Client- und Traffic-agnostisch

Ein Kanalzuweisungsverfahren, welches weder die Interferenz der Clienten, noch die Art und Umfang des Netzwerkverkehrs berücksichtigt, bezeichnet man als Client- und Traffic-agnostisch. Der Vorteil bei einem solchen Verfahren ist, dass beim Ermitteln des Interferenzgraphen nur die APs selbst berücksichtigt werden müssen. In Infrastruktur-Netzwerken ist dies sehr einfach zu realisieren. Auf Grundlage des gemessenen Interferenzgraphen, wird durch die Kanalzuweisung die Gesamtinterferenz im Netzwerk minimiert [23, 9]. Dies lässt sich mit Hilfe der Gesamtlinkinterferenz aus Abschnitt 3.2 als Optimierungsproblem formulieren:

$$\text{Minimiere} : Gesamtinterferenz = \sum_{i,j \in A, i \neq j} Gesamtlinkinterferenz(i,j)$$

Die Menge A ist die Menge aller APs im Netzwerk. Die Gesamtinterferenz ist die Summe der einzelnen Interferenzen zwischen den APs der Menge A. Die Interferenz zwischen zwei APs i und j (Gesamtlinkinterferenz(i,j)) ist dabei abhängig von den verwendeten Kanälen und der gemessenen Interferenz, wenn beide den selben Kanal verwenden, welche dem Interferengraphen entnommen werden kann (Listing 3.1 und 3.2). In [31] formuliert Haidar et al. das Optimierungsproblem als lineares Programm (Integer Linear Program; ILP). Im weiter Verlauf dieser Arbeit werden einige Heuristiken vorgestellt, welche ebenfalls das Ziel haben, die Gesamtinterferenz im Netzwerk zu minimieren, jedoch geringere Komplexität aufweisen.

3.4 Kanalzuweisung: Client-aware

Damit bei der Kanalzuweisung die Clienten in einem Infrastruktur-Netzwerk berücksichtigt werden können (*Client-aware*), muss die Interferenz bei ihnen bekannt sein. Dazu müssen die Clienten entsprechend angepasst werden. Um sicher zu stellen, dass jeder Client mit einem AP verbunden ist, findet die Kanalzuweisung erst nach der Assoziierung statt und der Client erhält dabei den Kanal seines APs. Dies verhindert, dass ein Client einen Kanal zugewiesen bekommt, auf welchem kein AP in seinem Umfeld operiert. Die Interferenz zwischen einem AP und seinen Clienten wird nicht mit in die Gesamtinterferenz einbezogen, da beide direkt miteinander kommunizieren müssen und es deshalb nicht als Störung aufgefasst wird. Es wird nur die Interferenz zwischen den Basic Service Sets (BSS) berücksichtigt. Zu einem solchen BSS gehört ein AP und die mit ihm verbundenen Clienten. Die Interferenz innerhalb der Basic Service Sets, z. B. zwischen den Clienten eines BSSs wird nicht berücksichtigt. Ziel der Kanalzuweisung ist wiederum die Minimierung der Gesamtinterferenz, wodurch sich folgendes Optimierungsproblem ergibt:

$$\text{Minimiere} : \mathit{Gesamtinterferenz} = \sum_{i,j \in A \cup B, BSS(i) \neq BSS(j)} \mathit{Gesamtlinkinterferenz}(i,j)$$

Dabei bezeichnet A die Menge aller APs und B die Menge aller Clienten.

3.5 Kanalzuweisung: Traffic-aware

In [23] haben E. Rozner durch Analyse von Mitschnitten des Datenverkehrs eines Netzwerkes ermittelt, dass der Umfang des Netzwerkverkehr z. T. sehr ungleichmäßig über die AP verteilt ist. Durch den Einsatz von Kanalzuweisungsverfahren, welche dies nicht berücksichtigen, kann es dazu kommen, dass APs, die stark interferieren, aber nur wenige Daten senden bzw. empfangen, verschiedene Kanäle bekommen, obwohl sie mit nur sehr wenig Einbußen den selben Kanal benutzen könnten. Andere Stationen, zwischen denen die Interferenz nicht ganz so stark ist, bekommen im Gegensatz dazu häufig den selben Kanal zugewiesen. Wenn sie jedoch mehr Daten senden und empfangen, ist die Störung meist größer als zwischen Knoten die nur wenig senden.

Die Störungen zwischen zwei APs treten dabei in zwei Fällen auf: ein AP sendet, während der andere Daten von einem Clienten empfängt oder beide APs senden Daten. Im Fall, dass beide Daten empfangen, tritt zwischen ihnen keine Störung auf. Aus dem Anteil der Zeit, in welcher die APs senden (S) und empfangen (E), kann bestimmt werden, wie groß die zeitliche Überlappung im Mittel ist. Daraus ergibt sich folgende Gewichtung:

$$W_{A,B} = S_A \times S_B + S_A \times E_B + S_B \times E_A$$

Die Gesamtlinkinterferenz zwischen zwei APs A und B wird mit $W_{A,B}$ gewichtet und daraus ein Optimierungsproblem formuliert:

$$\text{Minimiere} : \mathit{Gesamtinterferenz} = \sum_{i,j \in A, i \neq j} W_{i,j} \times \mathit{Gesamtlinkinterferenz}(i,j)$$

Ein solches Kanalzuweisungsverfahren setzt allerdings voraus, die Datenrate mit welcher die APs und die Clienten senden, genau zu kennen. Zwar können z. B. in einem Infrastruktur-Netzwerk die APs bzw. ein zentraler Kontroller den Datenverkehr analysieren und für jeden Clienten bzw. AP die gesendete

und empfangene Datenmenge näherungsweise bestimmen, jedoch ist die gesendete Datenmenge meist höher, da z. B. Fehlübertragungen durch geringe Signalstärken oder Interferenzen nicht erfasst werden. Die Datenraten können sich außerdem häufig ändern. Das ständige Anpassen der Kanalzuweisung ist jedoch nicht praktikabel, da während des Kanalwechsels keine Datenübertragung möglich ist und zudem die Gefahr besteht, dass die Clienten die Verbindung zum AP verlieren und sich neu assoziieren müssen, was zusätzliche Zeit in Anspruch nimmt.

3.6 Kanalzuweisung: Traffic- und Client-aware

Sollte sowohl die Interferenz bei den Clienten als auch der Umfang des momentanen Netzwerkverkehrs bekannt sein, lassen sich auch beide Information zur Kanalzuweisung nutzen. Dazu werden die Verfahren aus Abschnitt 3.3 und 3.4 kombiniert und zu folgendem Optimierungsproblem zusammengefasst:

$$\text{Minimiere} : \mathit{Gesamtinterferenz} = \sum_{i,j \in A, \cup B, BSS(i) \neq BSS(j)} W_{i,j} \times \mathit{Gesamtlinkinterferenz}(i,j)$$

Die Interferenz zwischen den Clienten, welche mit dem selben AP assoziiert sind, wird dabei wiederum nicht berücksichtigt (vgl. Abschnitt 3.4). In Verlauf der Arbeit wird in einem weiteren Abschnitt erklärt, wie sich mit Hilfe von Lastverteilung der Datenverkehr gleichmäßig über die APs verteilen lässt. Dabei wird nicht vom Clienten, sondern von einem zentralen Controller bzw. den APs festgelegt, mit welchem AP sich der Client assoziieren kann.

3.7 Heuristiken

Das Ermitteln der optimalen Kanalzuweisung ist wie oben bereits erwähnt NP-hart[11]. Es gibt bei einem Netzwerk mit n Knoten und bei Verwendung von c Kanälen insgesamt c^n Möglichkeiten, die Kanäle den einzelnen Knoten zuzuweisen ($O(c^n)$). Dies ist bei sehr großen Netzwerken mit vielen Knoten sehr unpraktikabel, und verhindert u. U. ein schnelles, dynamisches Reagieren auf Veränderungen im Netzwerk, wie z. B. Störungen durch fremde Netzwerke. So ergeben sich z. B. bei 100 Knoten und 5 verwendeten Kanälen 5^{100} ($\approx 10^{70}$) Möglichkeiten.

Im folgendes Abschnitt werden deshalb vier Verfahren vorgestellt, die eine geringere Komplexität aufweisen und dennoch sehr gute Ergebnisse liefern, wie spätere Simulationen zeigen werden. Es wird dabei auch auf die Vor- und Nachteile der einzelnen Verfahren eingegangen.

3.7.1 Zufällig

Die zufällige Kanalzuweisung (Random) ist keine Optimierung, soll an dieser Stelle dennoch erwähnt werden, da sie zum einen eine sehr geringe Komplexität aufweist und zum anderen später zum Vergleich herangezogen werden soll und z. T. sehr gute Ergebnisse liefert.

Bei der zufälligen Kanalzuweisung bekommt jeder Knoten einen zufälligen aus allen zur Verfügung stehenden Kanälen. Die Komplexität dieses Algorithmus ist $O(n)$, d. h. die Laufzeit wächst linear mit der Anzahl der Knoten. Auch ohne eine zentrale Kontrolle ist dies sehr leicht zu implementieren. Die Interferenz zwischen den Knoten im Netzwerk wird dabei nicht berücksichtigt, jedoch können externe Störer in dieses Verfahren mit einbezogen werden. Dazu streicht jeder Knoten die Kanäle, die vermieden werden sollen aus der Auswahlliste. Eine weitere Möglichkeit ist es, die Kanäle je nach Stärke der Störung so zu gewichten, dass Kanäle mit geringer Störung eine höhere Wahrscheinlichkeit haben, Verwendung zu finden.

Die zufällige Kanalzuweisung spiegelt sehr gut die Situation in Wohngebieten wieder, wo die Benutzer entweder den voreingestellten Kanal verwenden, der sich bei den einzelnen Herstellern z. T. unterscheidet oder den APs einen beliebigen Kanal geben, ohne dabei die anderen drahtlosen Netzwerke im Umkreis zu berücksichtigen.

3.7.2 Merge

Die Idee des Merge-Verfahren ist es, dass die Knoten bzw. die Gruppen von Knoten zweier unterschiedlicher Kanäle, die am wenigsten miteinander interferieren, den selben Kanal verwenden sollten. Knoten, welche den selben Kanal z benutzen, werden in einer Gruppe G_z zusammengefasst.

Das Verfahren im Detail: Zu Beginn bekommt jeder Knoten einen eigenen Kanal k und ist damit der jeweils einzige Knoten in der entsprechenden Gruppe G_k. In jeder der nun folgenden Iterationen werden nun paarweise zwischen den Gruppen die Interferenz bestimmt. Die zwei Gruppen G_x und G_y, deren Interferenz am geringsten ist, werden zu einer neuen Gruppe G_z zusammengefasst. Dadurch reduziert sich in jeder Iteration die Anzahl der Gruppen und damit auch die der Kanäle um eins. Die Anzahl der Iterationen i ist durch die Anzahl der Knoten n und die maximale Anzahl an Kanälen k vorgegeben. Es gilt: $i = n - k$. Nach i Iterationen werden die zu verwendenden Kanäle den k verbliebenen Gruppen zugeordnet.

Die Komplexität dieses Verfahren wird durch Aufwand zum Finden der zwei Gruppen mit der geringsten Interferenz vorgegeben. In jeder Iteration sind dabei bis zu $\binom{n}{2}$ Vergleiche nötig, da es bei n Knoten zu Beginn n Gruppen gibt und sich daraus $\binom{n}{2}$ Paare ergeben. Da die Anzahl der Iterationen linear von n abhängig ist, ergibt sich so eine Komplexität von $O(n^3)$.

Dieses Verfahren hat einige Nachteile. So muss die Anzahl der möglichen Kanäle für alle Knoten gleich sein, d. h. es besteht keine Möglichkeit zu vermeiden, dass ein einzelner Knoten einen, bei ihm stark gestörten bzw. durch fremde Geräte genutzten Kanal verwenden muss. Ein weiter Nachteil ist, dass dieses Verfahren die Interferenz zwischen benachbarten Kanälen nicht berücksichtigt. Die Nachteile haben ihre Ursache in der Tatsache, dass erst am Ende des Verfahrens, die Gruppen ihre tatsächlich verwendeten Kanäle zugeordnet bekommen. Des weiteren wird auch nicht berücksichtigt, dass die Interferenz auf verschiedenen Kanälen unterschiedliche stark sein kann.

3.7.3 Least Recently Used

Least Recently Used (LRU) ist eine Strategie aus dem Bereich der Cache-Verwaltung, bei welcher in der Vergangenheit selten benutze Daten von neuen Daten verdrängt werden. Dieses Konzept lässt sich auch auf die Kanalzuweisung übertragen.

Jeder Knoten im Netzwerk verwendet jenen Kanal, der in seiner Umgebung bzw. Nachbarschaft am wenigsten verwendet wird. Diese Nachbarschaftsbeziehung kann unter anderem über den Empfangsradius bestimmt werden. Dabei werden alle Stationen als Nachbarn gewertet, von denen Daten empfangen werden konnten. Mit Hilfe des Interferenzgraphen kann dieses Verfahren weiter verbessert werden. Dazu wird für jede Station jener Kanal bestimmt, auf welchem die Interferenz zu seinen Nachbarn am geringsten ist. Der Vorteil dabei ist, dass dabei auch Knoten in der Umgebung berücksichtigt werden, von denen der Knoten keine Daten empfangen kann, deren Signalstärke jedoch ausreichend ist, um Fehler zu verursachen.

Da die Änderung des Kanals eines Knoten eine Änderung bei seinen Nachbarn zur Folge haben kann, da sich für diese die Bedingungen geändert haben, muss dieser Algorithmus mehrere Iterationen durchlaufen. Um dabei jedoch ein Pendeln zwischen mehreren Kanalzuweisungen zu verhindern bzw. zu beenden, begrenzt man die maximale Anzahl der Iterationen oder verwendet eine Hysterese. Folgende Kriterien sind u. a. möglich und können auch kombiniert werden:

1. Fest vorgegebene maximale Anzahl von Iteration.

2. Minimale Anzahl von Kanaländerungen, die zu einer weiteren Iteration führt, d. h. sollte in der Iteration r weniger als k Knoten ihren Kanal ändern, terminiert der Algorithmus.

3. Reduzierung der Interferenz, welche die letzte Iteration erzielt wurde. Sollte diese unterhalb eines Schwellwertes liegen, folgt keine weitere Iteration (Hysterese).

In jeder Iteration muss jeder Knoten die Anzahl der Nachbarn bzw. die Summe der Interferenz zwischen ihm und den anderen bestimmt werden, was bei n Knoten bis zu n^2 Berechnungen benötigt. Da die Anzahl der Iterationen unabhängig von der Anzahl der Knoten ist, hat dieser Algorithmus eine Komplexität von $O(n^2)$.

3.7.4 Registerallokation und Simulated Annealing

Die von E. Rozner et al.[23] verwendete Kanalzuweisung setzt sich aus 2 Schritten zusammen. Im ersten Schritt wird mittels eines einfachen Verfahren eine initiale Kanalzuweisung bestimmt. In einem weiteren Schritt wird diese mit Hilfe von Simulierter Abkühlung (*Simulated annealing*, SA)[39] weiter verbessert. Die initiale Kanalzuweisung ist an einen Ansatz für die Registerallokation von Chaitin[18] angeleht:

1. Erstelle den Interferenzgraphen, wobei jeder Knoten einen Netzwerkknoten repräsentiert und Kanten die Interferenzen zwischen ihnen widerspiegeln.

2. Wähle den Knoten aus dem Graphen, der den maximalen Grad kleiner k (k = #Kanäle) hat, lege ihn auf den Stack und entferne ihn und seine Kanten aus dem Graphen. Wiederhole diesen Schritt bis kein Knoten mehr im Graphen ist, der einen Grad kleiner k hat.

3. Sollte der Graph nicht leer sein, nehme den Knoten mit dem größten Grad und seine Kanten heraus, lege ihn auf den Stack und gehe zu Schritt 2.

4. Nehme jeweils ein Knoten vom Stack, lege ihn zurück in den Graphen, weise ihm den Kanal zu, den keiner seiner aktuellen Nachbarn hat. Sollte es keinen solchen Kanal mehr geben, markiere den Knoten.

5. Wähle für alle markierten Knoten den Kanal, der am wenigsten Interferenz verursacht.

Auf Grundlage dieser initialen Kanalzuweisung wird nun mittels SA versucht, die Gesamtinterferenz weiter zu reduzieren. In jeder Iteration wird dazu der Kanal eines Knoten geändert und die Gesamtinterferenz für die resultierende Kanalzuweisung bestimmt. Sollte die Interferenz geringer geworden sein, so wird mit der nächsten Iteration fortgefahren. Bei einer Erhöhung der Gesamtinterferenz wird die neue Kanalzuweisung mit einer Wahrscheinlichkeit $e^{(f_{neu}-f_{alt})/T}$ übernommen. Dabei sind f_{neu} und f_{alt} Funktionen der aktuellen und alten Zuweisung und T die momentane "Temperatur". Die "Temperatur" wird kontinuierlich mit jeder Iteration um einen bestimmten Faktor reduziert. E. Rozner et al. verwenden als Faktor 0,999. Dieses Reduzieren führt dazu, dass zu Beginn auch mit relativ hoher Wahrscheinlichkeit eine schlechtere Kanalzuweisung übernommen wird, während nach vielen Iterationen und damit "geringer Temperatur", man schlechtere Zuweisungen eher verwirft. Nach allen Iterationen wird die beste von allen gefundenen Kanalzuweisungen übernommen.

Da SA jede beliebige Kanalzuweisung als Ausgangssituation nehmen kann, lässt es sich auch mit den anderen oben vorgestellten Algorithmen kombinieren. Der initiale Algorithmus der von E. Rozner et al. vorgeschlagen wird, geht von einer binären Interferenz aus, d. h. es wird nur unterschieden, ob Knoten interferieren oder nicht. In [23] wird zur Bestimmung des Interferenzgraphen die Methode Maximum Throughput (s. Abschnitt 3.1.1) verwendet, bei der sich kontinuierliche Werte zwischen 1 und 0 für die Stärke der Interferenz ergeben. Es wird nicht darauf eingegangen, wie der initiale Algorithmus angepasst

wurde, um mit kontinuierlichen Werten zu arbeiten bzw. wie aus den kontinuierlichen Werten der Messung ein Graph mit binärer Interferenz erstellt wurde.

In der vorliegenden Arbeit wurde mit Hilfe eines Schwellwertes eine binäre Interferenz aus den kontinuierlichen Werten der Interferenz bestimmt. Durch Experimente mit verschiedenen Werten, wurde ein Schwellwert von 0,5 als Optimum ermittelt. Kanten im Interferenzgraph, deren Gewicht kleiner als 0,5 waren, wurden für den initialen Algorithmus entfernt, alle anderen mit einem Gewicht von 1 versehen. Für das SA wurde jedoch der Interferenzgraph mit den kontinuierlichen Werten verwendet.

3.8 Verteilung der Netzwerklast

In den Abschnitten 3.4 bis 3.6 wurden Verfahren für die Kanalzuweisung vorgestellt, welche die Clienten und den Netzwerkverkehr zwischen ihnen und den APs berücksichtigen. Diese Verfahren erreichen ein besseres Ergebnis als solche, die weder den Netzwerkverkehr noch die Clienten berücksichtigen[23]. Die bisher ungeklärte Frage ist, nach welchen Gesichtspunkten sich die Clienten ihren AP, mit dem sie sich assoziieren, aussuchen und ob in großen Infrastruktur-Netzwerken dies zentral gesteuert bzw. beeinflusst werden kann und nach welchen Kriterien dabei vorgegangen werden sollte.

Kriterien der Lastverteilung

Wie in Kapitel 2.2 bereits erklärt, wählen die Clienten den AP anhand der Signalstärke der empfangenen Beacons aus. Sie assoziieren sich mit jenen, welcher die größte Signalstärke hat. Auch in [23] wird davon ausgegangen. Durch Verwendung von Kanalzuweisungsverfahren, welche die Assoziierung der Clienten und den Netzwerkverkehr berücksichtigen, kann dabei die Leistung im Netzwerk verbessert werden. Jedoch kommt es durch die Art wie die Clienten den AP wählen und bei ungünstiger Verteilung der APs häufig zu unterschiedlicher Netzwerklast bei den einzelnen APs, d. h. es gibt starke Unterschiede bei der Auslastung. Im Extremfall haben einige APs keine Clienten, während andere sehr viele haben. Besonders nachteilig wirkt sich dies in Szenarien aus, in denen die Bandbreite des Backbones zum Gateway bzw. Internet begrenzt ist. Ein Beispiel sind hier Hotspots, die z. T. aus Kostengründen nur über DSL angebunden sind. In [21] wird mit Hilfe von ganzzahliger linearer Optimierung die Last des am stärkste benutzen AP minimiert, indem die Clienten den APs so zugewiesen werden, dass die von ihnen erzeugte Netzwerklast möglichst gleichmäßig über alle APs verteilt ist.

Ein weiteres wichtiges Kriterium ist die Auslastung der Kapazität der einzelnen im drahtlosen Netzwerk verwendeten Kanäle. Da bei der Auswahl des APs durch den Clienten dies keine Berücksichtigung findet, werden z. T. freie Kanäle nicht verwendet, obwohl trotz möglicher höherer Paketfehlerrate u. U. ein besserer Durchsatz erzielt werden würden, da der einzelne Client viel häufiger Zugriff auf das Medium erhält. In [32] wird bei der Auswahl des besten AP für einen neuen Clienten deshalb die verfügbare Kapazität als Metrik benutzt. Diese ergibt sich aus dem Produkt von freier Mediumzeit bei dem entsprechenden AP und der erwarteten Übertragungsrate.

Steuerung der Assoziierung

Die Assoziierung der Clienten kann auf verschiedene Art beeinflusst werden. So hat der AP die Möglichkeit die Assoziierungsanfrage unter Angabe eines Grundes abzulehnen (vgl. Kapitel 2.2). Eine weitere Möglichkeit ist die Reduzierung der Sendeleistung für die Beacons, anhand deren Signalstärke der Client den für ihn beste AP auswählt. Der AP kann durch entsprechende Wahl der Sendeleistung den Bereich, in dem Clienten seine Beacons empfangen, vergrößern bzw. verkleinern. In [25, 13, 15] wird dieses sogenannte *Cell Breathing* verwendet, um Clienten zwischen den AP gleichmäßig zu verteilen bzw. zu verhindern, dass einzelne APs überlastet werden.

Mit Cell Breathing können auch Clienten, die schon mit einem AP assoziiert sind, dazu gebracht werden, einen neuen AP zu verwenden, indem die Sendeleistung der Beacons in Schritten so lange reduziert wird, bis einzelne Clienten einen neuen AP wählen, dessen Beacons sie mit höherer Signalstärke empfangen. Das Verfahren ist jedoch in zweifacher Hinsicht ungenau. Zum einen lässt sich damit nicht gezielt ein bestimmter Client, der z. B. sehr viel Netzwerkverkehr erzeugt, verschieben, zum anderen ist auch nicht die Anzahl an Clienten vorhersehbar, die sich mit einem anderen AP assoziieren werden. Durch die Kombination von Cell Breathing und gezieltem Ablehnen von neuen Clienten lässt bei zentraler Kontrolle des Netzwerkes die Verteilung der Netzwerklast dennoch recht genau steuern.

Nachteile

Es muss jedoch beim Verschieben bzw. Verteilen von Clienten mittels Cell Breathing einiges beachtet werden. So kann der Wechsel des APs u. U. zum Abbrechen von bestehenden Verbindungen führen. Sollte zudem der Client beim Wechsel seine IP-Adresse mittels DHCP erneuern, so kann dies zu einer längeren Unterbrechung von einigen wenigen Sekunden führen. Des weiteren ist nicht bekannt, welche Bitraten von den Clienten für die Datenübertragung zum neuen AP verwenden werden können.

3.9 Zusammenfassung

Die Kanalzuweisung ist entscheidend für den Gesamtdurchsatz in einem drahtlosen Netzwerk. In diesem Kapitel wurden Verfahren vorgestellt, die sowohl die Interferenz bei den Clienten als auch die Netzwerklast berücksichtigen. Da die Kanalzuweisung sehr komplex ist, wurden verschiedene Heuristiken vorgestellt, die eine deutlich geringere Komplexität aufweisen und deshalb für den praktischen Einsatz in dynamischen Systemen deutlich besser geeignet sind. Ein großer Unterschied zwischen den einzelnen Heuristiken liegt in ihrer Erweiterbarkeit bezüglich der Berücksichtigen von Beschränkungen, wie z. B. Vermeidung bestimmter Kanäle für bestimmte APs bzw. Clienten. Dies ist aber ein wichtiges Kriterium, um z. B. Störungen durch andere Netze vermeiden zu können. Hier sei das Verfahren LRU besonders hervorgehoben, da es zudem verteilt realisierbar ist und somit auch in Netzen Anwendung finden kann, die nicht zentral kontrolliert werden können. Die Tabelle 3.1 gibt noch einmal eine Übersicht über alle vorgestellten Heuristiken und der Möglichkeit jeweils externe Störung zu berücksichtigen und eine verteilte Umsetzung zu realisieren. Zusätzlich beinhaltet sie auch die zeitliche Komplexität der Verfahren, welche von der Anzahl der Knoten (n) und der Kanäle (c) abhängig ist.

Tabelle 3.1: Zusammenfassung der vorgestellten Verfahren für die Kanalzuweisung und ihre Eigenschaften.

Verfahren	Externe Interferenz	Verteilt	Zeitl. Komplexität
`Erschöpfende Suche`	Ja	Nein	$O(c^n)$
`Merge`	Nein	Nein	$O(n^3)$
`LRU`	Ja	Ja	$O(n^2)$
`Simulated Annealing`	Ja	Nein	$O(n^2)$
`Zufällig (Random)`	Ja	Ja	$O(n)$

Kapitel 4

Verteilte Antennen

4.1 Motivation

Moderne Hardware, welche den Standard 802.11a/g unterstützt, bietet Datenraten von bis zu 54 Mbit/s. Jedoch liegen die tatsächlich erreichten Durchsätze auf der Anwendungsschicht weit darunter und schwanken zudem stark. Ein Hauptgrund für den geringeren Durchsatz sind Paketfehler, d. h. dass Pakete gar nicht oder nicht korrekt empfangen wurden. Die Ursachen dafür sind Pfadverlust, Interferenz und Fading. Ersteres führt dazu, dass ein Signal mit zunehmendem Abstand von der Quelle (Sender) schwächer wird. Als Interferenzen werden Überlagerungen von mehreren Signalen bezeichnet. In drahtlosen Netzwerken treten diese auf, wenn verschiedene Sender gleichzeitig Daten übertragen und sich die Signale beim Empfänger überlagern. Dieser kann die Signale u. U. nicht mehr dekodieren und es kommt zum Übertragungsfehler. Zum Fading zählt man Einflüsse wie die Mehrwegausbreitung (Multipath-Fading) und den Dopplereffekt. Ersteres bezeichnet die Tatsache, dass Signale durch Reflexion verschiedene Wege vom Sender zum Empfänger laufen. Die Signale treffen so mehrfach und phasenverschoben bei Empfänger ein. Durch die Phasenverschiebung kann es zu destruktiver und konstruktiver Interferenz (Dämpfung bzw. Verstärkung) kommen. Durch Mobilität des Senders und des Empfängers bzw. Bewegung in der Umgebung, unterliegt die Signalstärke beim Empfänger zeitlichen Schwankungen, wie Abbildung 4.1 verdeutlicht.

Der IEEE 802.11 Standard kennt verschiedene Mechanismen, um Fehler bei der Übertragung zu verringern, zu erkennen und zu korrigieren. So wird zur Fehlererkennung jedes Paket mit einer CRC-Prüfsumme (Checksumme) versehen, mit welcher der Empfänger die Korrektheit überprüfen kann. Erfolgreich empfangene, d. h. fehlerfreie Pakete werden vom Empfänger durch das Senden eines Acknowledgement (ACK) bestätigt. Der Sender wiederholt beim Ausbleiben der Bestätigung die Übertragung (*automatic repeat request* (ARQ))[16, 108]. Durch Forward Error Correction (FEC) von IEEE 802.11a/g erzeugt der Sender mittels zusätzlicher Bits eine je nach Bitrate unterschiedliche starke Redundanz, die eine Korrektur von Fehlern auf der Seite des Empfängers ermöglicht. Die Bits des Datenpaketes werden nach dem Einfügen der redundanten Bits verwürfelt (*Scrambler*), d.h. in ihrer Reihenfolge umgeordnet. Dadurch wird sichergestellt, dass eine zeitlich kurze Störung, z. B. durch Interferenz mit einem Bluetooth-Gerät, nicht die gesamte Redundanz beeinflusst.

Eine weitere Möglichkeit zur Reduzierung von Übertragungsfehlern ist die Ausnutzung der räumlichen Diversität (*Spatial Diversity*) durch die Verwendung von mehreren (kooperativen) Empfängern. Dabei wird die Tatsache ausgenutzt, dass die Schwankungen im Kanal nicht nur zeitlich, sondern auch räumlich wenig korreliert sind. Die Abbildung 4.1 zeigt exemplarisch die Schwankungen der Kanalqualität zwischen einem Sender und 3 potentiellen Empfängern (AP 1, AP 2 und AP 3). Bei der räumlichen Diversität unterscheidet man Mikro- und Makro-Diversität.

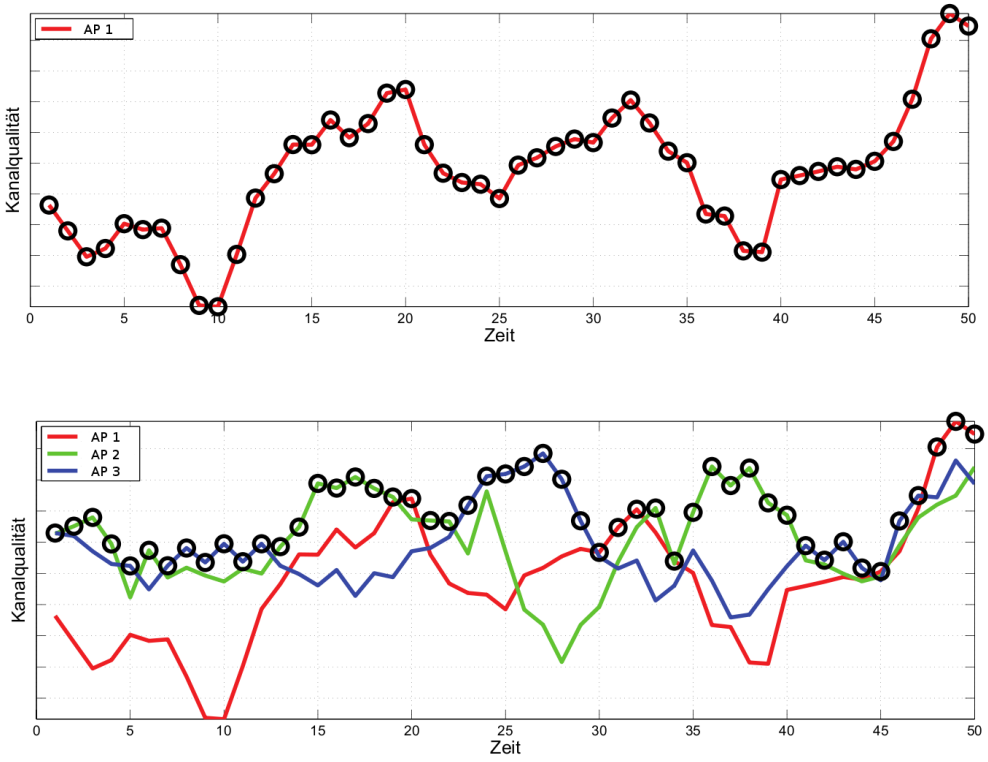

Abbildung 4.1: Die Kanalqualität schwankt zeitlich. Ursache dafür sind Pfadverlust, sowie Fading und Interferenz.

Von Mikro-Diversität spricht man, wenn die Empfangsantennen einen Abstand in der Größenordnung der Wellenlänge des Signals haben. Beim Multipath-Fading liegen die Bereiche, in denen sich ein Signal, welches durch Reflexion über mehrere Wege zum Empfänger gelangen, konstruktiv und destruktiv überlagert sehr dicht beieinander. Durch mehrere, dicht angeordnete Empfangsantennen können die Übertragungsfehler reduziert werden, da die Signale bezüglich Multipath-Fading unkorreliert sind. Moderne Chips, wie z. B. von Atheros, bieten die Möglichkeit mehrere Empfangsantennen zu verwenden. Der Chip erkennt beim Empfang, genauer anhand der Präambel, bei welcher Antenne die Signalstärke am höchsten ist und verwendet diese, um den Rest des Frames zu empfangen (selection combining).

Sind die Antennen ein höheres Vielfaches der Wellenlänge λ und weiter voneinander entfernt, so spricht man von Makro-Diversität. Hierbei werden zudem nicht nur mehrere Antennen, sondern unterschiedliche Stationen bzw. Radios, wie z. B. mehrere Basisstationen in UMTS-Netzen, verwendet. Durch die größerer Distanz zwischen den einzelnen Empfängern, können zusätzlich Übertragungsfehler aufgrund Interferenz und Abschattung ausgeglichen werden. So ist eine durch eine externe Quelle verursachte Störung in einem drahtlosen Netzwerk, wie z. B. einem Mikrowellenherd, räumlich begrenzt und es ist somit wahrscheinlich, dass nicht alle Empfänger gestört werden. Es wird hierbei also davon profitiert, dass Paketverluste sowohl orts- als auch pfadabhängig (Multipath-Fading) sind[10].

In großen Infrastruktur-Netzwerken sind mehrere APs über ein schnelles, drahtgebundenes Netzwerk miteinander und meist einem Gateway verbunden. Die APs, welche räumlich verteilt sind, können in solchen Netzwerken verteilte Antennen (VA) bilden und somit die Datenübertragung von den Clienten

zu ihnen verbessern.Der Einsatz von mehreren Empfänger muss jedoch mit anderen Mechanismen zur Fehlerkontrolle, wie z. B. dem ARQ in Einklang gebracht werden. So muss der Sender von mindestens einem Empfänger eine Bestätigung für ein gesendetes Paket bekommen. Es sind dazu Änderungen am Sender oder Empfänger, z. B. der MAC-Schicht nötig.

In diesem Abschnitt werden mehrere Möglichkeiten zur Bildung von verteilten Antennen und entsprechende Protokolle vorgestellt. Die vorzunehmenden Änderungen unterscheiden sich dabei darin, bei wem diese vorgenommen werden müssen (Sender bzw. Empfänger) und ob sie auf MAC- oder einer höherer Schicht zu machen sind.

4.2 Verteiltes Empfangen

Der IEEE 802.11 Standard definiert 2 Möglichkeiten zur Übertragung an eine Gruppe von Empfängern. Eine Broadcast-Übertragung wird von allen Empfängern verarbeitet, die sie empfangen. Eine Multicast-Übertragung hingegen ist an eine Gruppe von Empfängern gerichtet. In beiden Fällen erhält der Sender jedoch keine Rückmeldung, wer das Paket empfangen hat und wer nicht. Eine erfolgreiche Unicast-Übertragung, welche der Sender an genau einen Empfänger sendet, wird jedoch, wenn sie fehlerfrei war, bestätigt. Der Sender erhält somit eine Rückmeldung und kann gegebenenfalls die Übertragung wiederholen.

Verteilte Antennen sollen beides umsetzen. Zum einen sollen mehrere Empfänger das Paket empfangen und gegebenenfalls weiterleiten, zum anderen soll der Sender eine Bestätigung von mindestens einem der Empfänger erhalten, wenn die Übertragung fehlerfrei war. Verteilte Antennen bieten zudem die Möglichkeit, mehrere defekte Kopien eines Paketes u. U. zu einem korrekten zu kombinieren. Hierbei kann erst nach der Rekonstruktion des Paketes festgestellt werden, ob es korrekt empfangen wurde und somit bestätigt werden kann.

Ein wichtiger Punkt bei verteilten Antennen sind die nötigen Änderung bei Sender. Die Adressierung der möglichen Empfänger kann zum einen durch den Sender passieren oder aber indirekt, d. h. die zusätzlichen Empfänger agieren so, dass der Client die verteilte Antenne nicht berücksichtigen muss. Im folgenden werden 4 mögliche Umsetzungen von verteilten Antennen vorgestellt und erläutert.

4.2.1 Slotted Acknowledgement

Zubow et al. beschreibt in [5] ein Protokoll für verteilte Antennen. Hierbei adressiert der Sender das Paket an mehrere Empfänger, die eine sogenannte Kanditatenmenge bilden. Jeder dieser Empfänger muss bei Erhalt des Paketes dieses bestätigen. Damit es dabei nicht zu Kollision zwischen den Bestätigungen der Empfänger kommt, senden diese ihre Bestätigungen zeitlich versetzt. Jeder bekommt einen sogenannten Zeitschlitz (Time-Slot). Dieses Verfahren zur Bestätigung nennt man deshalb *Slotted Acknowledgement*. Die Reihenfolge bzw. die Priorität der einzelnen Kandidaten wird dabei vom Sender durch die Reihenfolge der Empfängeradressen im Datenpaket festgelegt, wobei der höchst priorisierte Kandidaten zuerst seine Bestätigung senden muss.

Jeder Kandidat, der eine Bestätigung von einem höher priorisierten empfängt, notiert diese Information in seinem Acknowledgement. Sollte der Sender des Datenpaketes z. B. das Acknowledgement von Kandidat A nicht erhalten, so kann er durch Kandidat B dennoch erfahren, dass A das Paket erhalten hat. Da bei diesem Verfahren jeder Kandidat eine Bestätigung sendet, ist diese Protokoll sehr robust. Die Kandidaten können durch das Slotted Acknowledgement feststellen, wer aus der Kanditatenmenge das Datenpaket erhalten hat. Der höchste Kandidat, der das Paket erhalten hat, leitet dies an den Gateway weiter.

Da ein Kandidat, der das Datenpaket nicht korrekt empfangen hat, keine Bestätigung sendet, entsteht während seines Zeitschlitzes eine Lücke. Um zu verhindern, dass dadurch ein fremder Knoten in dieser Zeit

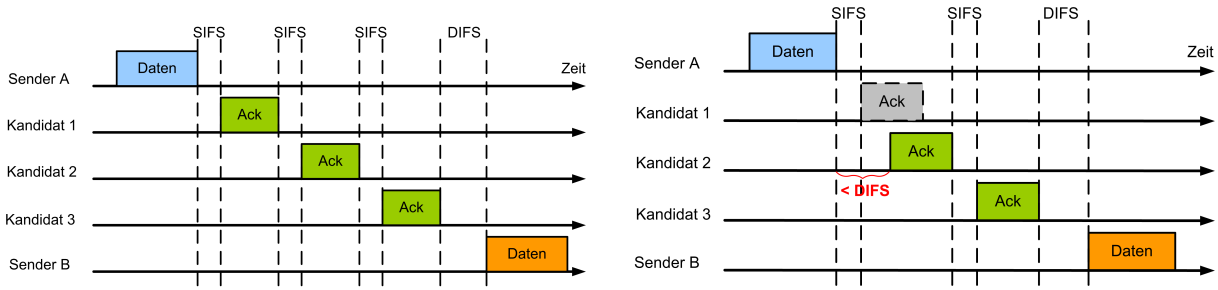

Abbildung 4.2: Slotted Acknowledgement: Die einzelnen Empfänger bestätigen den Empfang nacheinander (links). Sollte eine Bestätigung ausbleiben, so zieht der nachfolgende Kandidat seine Übertragung vor, um keinen zu großen Abstand entstehen zu lassen (rechts).

eine Übertragung beginnt, weil er das Medium als frei erkennt, sendet der nachfolgende Kandidat seine Bestätigung, sobald er feststellt, dass der zeitlich direkt vor ihm sendende Kandidat nichts überträgt. Er zieht sein Acknowledgement vor und schließt dadurch die Lücke bzw. macht sie kleiner. Die Abbildung 4.2 zeigt zum einem den perfekten Ablauf des Protokolls (links) als auch das Vorziehen des Acknowledgement (Kandidat 2). Durch das Fehlen des Acknowledgement von Kandidat 1 beginnen alle weiteren Empfänger ihre Übertragungen früher.

4.2.2 Cognitive Acknowledgement

Das im letzten Abschnitt vorgestellte Slotted Acknowledgement basiert auf Änderungen an der MAC-Schicht beim Sender und den Empfängern. Das Cognitive Acknowledgement, welches im Rahmen der Arbeit entstanden ist, benötigt keine Veränderungen am Clienten und eignet sich so für den Einsatz in großen Infrastruktur-Netzwerken, bei welchen die Clienten nicht verändert werden sollen. Provider solcher Netze können durch den Austausch ihrer Hardware, also der Access Points, dieses Protokoll für verteilte Antennen verwenden. Das Cognitive Acknowledgement basiert auf dem Vorziehen des Sendezeitpunktes der Bestätigung wie beim Slotted Acknowledgement.

Funktionsweise

Wie schon beim Slotted Acknowledgement bilden mehrere Empfänger (APs) eine verteilte Antenne. Und auch hier sind diese geordnet und erhalten eine Priorität. Jedoch bestimmt nicht der Sender des Paketes die Empfänger bzw. deren Reihenfolge, sondern die Empfänger bzw. ein zentraler Controller. Der Sender adressiert sein Pakete nach dem 802.11 Standard an einen Empfänger. Bei Infrastruktur-Netzwerken ist dies der AP, mit dem er sich assoziiert hat. Der Controller weißt den APs der VA jeweils eine Priorität zu, wobei der AP, mit dem sich der Client assoziiert hat, die höchste erhält. Von den APs, die eine verteilte Antenne bilden, sendet, von denen, die das Paket vom Sender erhalten haben, jener mit der höchsten Priorität die Bestätigung (Acknowledgement, Ack). Es wird also höchstens eine Bestätigung gesendet. Ein Beispiel zeigt Abbildung 4.3: AP_1, AP_2 und AP_3 gehören zu einer verteilten Antenne, wobei AP_1 die höchste Priorität hat. Wird das Paket von allen empfangen, wie es die linke Abbildung zeigt, so bestätigt AP_1 das Paket. Im zweiten Fall, der in der rechten Abbildung zu sehen ist, wird das Paket nur von AP_2 und AP_3 empfangen. Da AP_2 die höchste Priorität von diesen beiden hat, sendet nur er die Bestätigung.

Entscheidend bei diesem Verfahren ist, dass jeweils nur ein AP die Bestätigung schickt, da es sonst zu Kollisionen kommen kann und der Sender des Datenpaketes die Bestätigung nicht korrekt empfangen könnte. Dies wird dadurch sichergestellt, indem ein AP eine Zeit T wartet und dann überprüft, ob ein

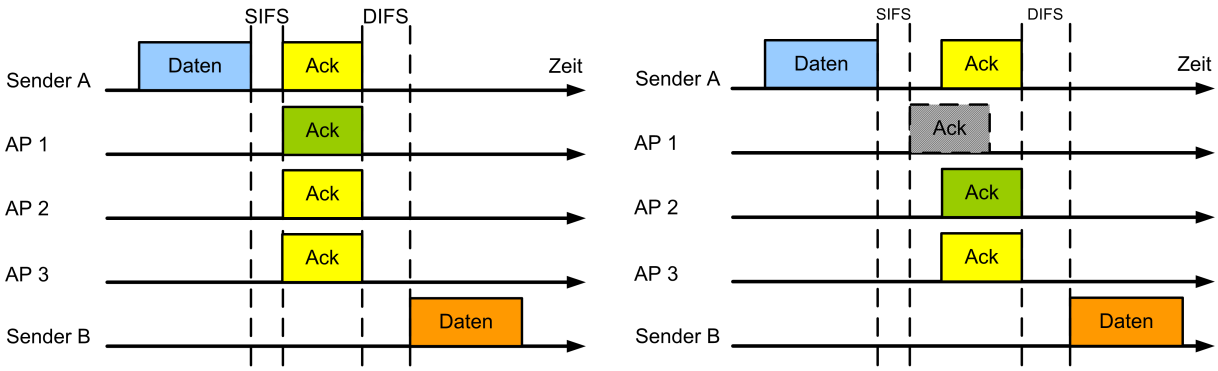

Abbildung 4.3: Der höchst priorisierte AP, der das Datenpaket empfängt, bestätigt es. Der nachfolgende AP stellt ein mögliches Fehlen der Bestätigung fest und übernimmt dann das Senden (rechts).

höher priorisierter eine Bestätigung versendet. Diese Wartezeit ist dabei abhängig von seiner Priorität, wobei APs mit höherer Priorität früher senden dürfen. Die Abbildung 4.4 verdeutlicht noch einmal den Ablauf.

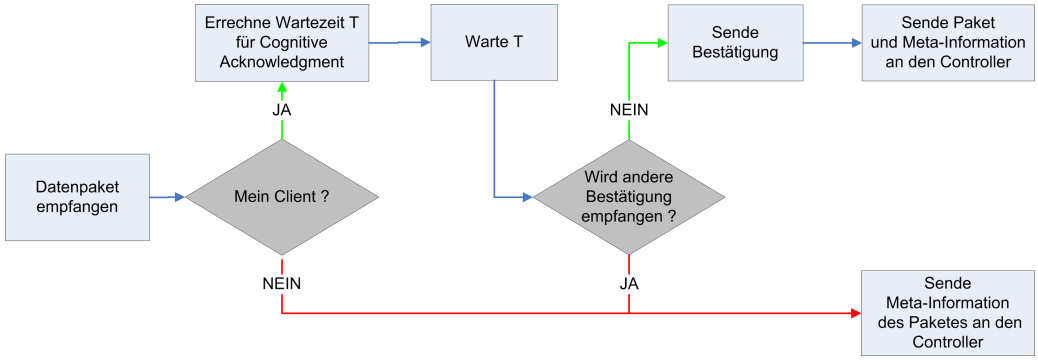

Abbildung 4.4: Ablauf des Cognitive Acknowledgements. Ein AP einer verteilten Antennen wartet eine von seiner Priorität abhängige Zeit T und prüft danach das Medium. Gegebenenfalls sendet er eine Bestätigung.

Für die Bestimmung der Wartezeit muss berücksichtigt werden, dass sowohl das Erkennen einer Übertragung eines anderen APs als auch das Umschalten des Radios von Empfangen auf Senden (Rx/Tx-Turnaround) eine gewisse Zeitdauer benötigt. Die Signallaufzeit kann ebenfalls nicht unberücksichtigt bleiben, auch wenn sich das Signal mit Lichtgeschwindigkeit ausbreitet. Zusätzlich muss der höchst priorisierte AP der verteilten Antenne nach dem 802.11-Standard die Zeit SIFS warten, bevor er die Bestätigung verschickt. Um diese Zeit muss auch die Wartezeit der nachfolgenden APs verlängert werden. Die Wartezeit T des Empfängers mit der Priorität n berechnet sich wie folgt:

$$T \quad = \quad SIFS + (n-1) \cdot ((Signallaufzeit\ und\ Signalerkennung) + RxTxTurnaround)$$

Die Wartezeit T des höchst priorisierten AP (Priorität 1) beträgt danach SIFS, was dem Standard entspricht.

Einschränkung der Antennengröße

Die maximale Anzahl von APs, die eine VA bilden können, ist beschränkt. Zwar lassen sich beliebig viele AP so platzieren, dass dieses Protokoll funktioniert, jedoch ist die Zeit, die bis zum Aussenden eines Acknowledgement-Paketes vergehen darf beschränkt. Die theoretische maximale Größe ist zum einen durch die Zeit beschränkt, die der Client auf die Bestätigung wartet. Der Grund dafür ist, dass der Sender des Paketes von einer fehlerhaften Übertragung ausgeht, wenn die Bestätigung nicht innerhalb einer festgelegten Zeit von ihm empfangen wird. Mit diesem Problem beschäftigen sich besonders Verfahren für sogenannte *Long-Distance-Links*, bei denen die Kommunikationspartner bis zu über hundert Kilometern voneinander entfernt sind. Die Signallaufzeit sind dabei z. T. so lang, dass die Bestätigung nicht rechtzeitig den Empfänger erreicht und dieser deshalb eine erneuten Übertragung beginnt. Verschiedene Treiber wie z.B. Madwifi[30] bieten deshalb die Möglichkeit, bei entsprechender Hardware die Wartezeit zu verlängern. Diese Zeit muss also bei großen VAs mit vielen APs beim Clienten verlängert werden, damit er länger auf die Bestätigung wartet und somit auch die Bestätigung vom AP mit der niedrigsten Priorität empfangen kann, bevor er von einem Übertragungsfehler ausgeht.

Die andere Einschränkung hat ihre Ursache im Zugriffsverfahren von IEEE 802.11. Eine sendewillige Station darf mit ihrer Übertragung beginnen, wenn für die Dauer von DIFS kein Mediumzugriff durch eine andere Station erkannt wurde. Der AP, der also innerhalb der verteilten Antenne als letztes eine Bestätigung sendet, wenn dies keine vor ihm getan hat, muss also spätestens nach DIFS nach dem Ende des Datenpaketes mit dem Senden des Acknowledgements beginnen. Da der erste AP für die Dauer von SIFS warten muss bevor er die Bestätigung sendet und alle Nachfolger ihrerseits mindestens die Zeit abwarten müssen, die der jeweilige Vorgänger braucht, um vom Empfangen auf Senden umzuschalten (Rx/Tx-Turnaround), ergibt sich daraus die maximale Anzahl n von APs in einer verteilten Antenne. Damit der n-te AP seine Übertragung beginnt, bevor ein anderer das Medium für die Zeitspanne DIFS als frei erkennt und übertragen darf, muss gelten:

$$DIFS \quad > \quad SIFS + (n-1) \cdot (CCA + RxTxTurnaround)$$

Der 802.11g-Standard legt SIFS mit $16\,\mu s$ und DIFS mit $34\,\mu s$ fest. Bei einer Umschaltdauer von Senden auf Empfangen von $5\,\mu s$ und $4\,\mu s$ für die Erkennung, ob das Medium belegt ist, ergibt sich dabei eine maximale Anzahl von 3 Empfängern innerhalb der verteilten Antenne (Abbildung 4.5 und Tabelle 4.1). Es ist anzumerken, dass die Zeit für die Erkennung der Mediumbelegung (*Clear Channel Assessment*, CCA) eine Mikrosekunde für die Laufzeit des Signals mit einrechnet, in der das Signal circa 300 m zurücklegen kann. Die Berechnung geht von perfekt funktionierender Hardware aus. Es kann also davon ausgegangen werden, dass höchstens 3 APs eine verteilte Antenne mit dem hier vorgestellten Verfahren bilden können.

Tabelle 4.1: Zeiten des 802.11g Standards.

Parameter	Zeit
`SIFS`	$16\,\mu s$
`DIFS`	$34\,\mu s$
`Slot Time`	$9\,\mu s$
`Rx/Tx-Turnaround`	$5\,\mu s$
`CCA`	$4\,\mu s$

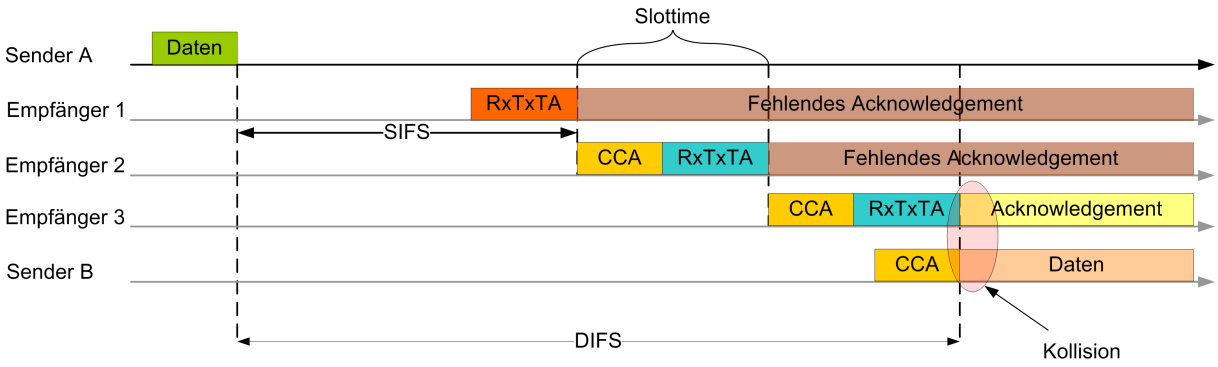

Abbildung 4.5: Cognitive Acknowledgement mit 3 APs bei 802.11g. Durch die lange Slot Time könnte jedoch der dritte AP bereits mit einem anderen Sender kollidieren, wenn dieser keinen Backoff mehr machen muss.

Parametrisierung

Eine Möglichkeit, die Anzahl der APs in einer Verteilten Antenne zu erhöhen, ergibt sich durch die Verkleinerung der Slot Time. Diese setzt sich aus der Zeit für den Wechsel von Empfangen auf Senden und der Erkennung der Belegung des Mediums zusammen. Letzteres kann nicht weiter reduziert werden. Die Slot Time kann also nur durch Reduzierung der Umschaltzeit verkleinert werden, was durch bessere Hardware realisiert werden kann. Die Abbildung 4.6 zeigt das Verfahren mit einer Slot Time von $7\,\mu s$, wobei die Dauer des Umschalten (Rx/Tx-Turnaround) nur noch $3\,\mu s$ beträgt. Eine weitere Möglichkeit die maximal mögliche Größe der verteilten Antenne zu erhöhen, ist die Zeit DIFS zu verlängern und ihre Dauer dabei entgegen dem Standard unabhängig von SIFS und der Slot Time festzulegen. Dies muss jedoch bei allen Geräten innerhalb des drahtlosen Netzwerkes geschehen, und benötigt so nicht nur eine Änderung bei den Clienten, sondern auch der IEEE 802.11 Geräte die nicht zum Netzwerk gehören, aber in Empfangsreichweite sind. Diese Idee wird deshalb im Rahmen dieser Arbeit nicht weiter verfolgt.

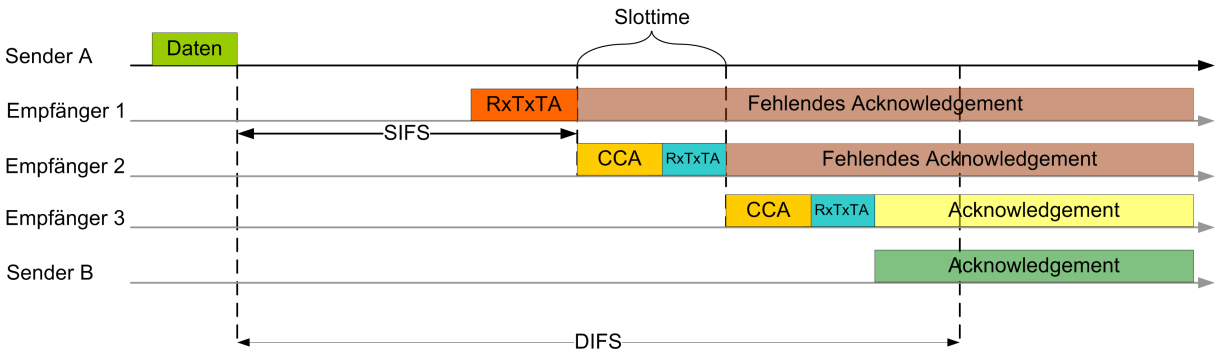

Abbildung 4.6: Cognitive Acknowledgement mit 3 APs. Durch Verkürzen der Umschaltzeit zwischen Empfangen und Senden kann eine Kollision des dritten APs mit einen anderen Sender verhindert werden.

Koordination zwischen den APs

Beim Cognitive Acknowledgement müssen die APs nicht wie beim Slotted Acknowledgement die Pakete anderer APs der VA empfangen können, sondern es ist ausreichend, wenn sie diese Übertragungen wahrnehmen können. Dies geschieht anhand der gemessenen Signalstärke bzw. des Rauschpegels. Sollte beim Messen ein festgelegter Schwellwert überschritten werden, so geht der AP von einer Übertragung durch einen anderen aus. Der Schwellwert kann dabei fest sein oder dynamisch ermittelt werden. Letzteres hat den Vorteil, dass parallele Übertragungen berücksichtigt werden können. Der AP misst dazu direkt nach Erhalt des Datenpaketes den Rauschpegel. Parallele Übertragung führen hierbei zu einem höheren Wert. Der Schwellwert wird nun daraus bestimmt. Er liegt einen bestimmten Betrag oberhalb des gemessenen Rauschens.

Erkennung von potentiellen verteilten Antennen

Die APs, welche eine verteilte Antenne bilden, müssen die Übertragung eines anderen anhand eines Ansteigen der Signalstärke registrieren. Der in Abschnitt 3.1.1 ermittelte Interferenzgraph kann verwendet werden, um APs zu erkennen, bei denen dieses Verfahren mit großer Wahrscheinlichkeit funktioniert. Nochmal zur Erinnerung: Ein hohes Kantengewicht zwischen 2 Knoten im Graph, welche die APs repräsentieren, bedeutet, dass die Übertragung, die ein AP macht, einen anderen AP beeinflusst. Die APs erkennen anhand einer hohen Signalstärke die parallele Übertragung (das Medium ist nicht frei) und warten für ihre Übertragung auf ein freies Medium, was zu einer geringer Anzahl ausgesendeter Pakete pro Zeit führt. Diese Reduzierung ausgesendeter Pakete deutet also auf Interferenz hin. Ein hohes Kantengewicht zeigt dementsprechend an, dass ein AP die Übertragung des anderen erkennt, auch wenn er diese Übertragung selbst nicht empfangen kann, sondern lediglich wahrnehmen kann.

4.2.3 Bestätigung mit Sendediversität

In [29] zeigt Kurth et. al. anhand von Experimenten, dass Sendediversität auch mit Standard-Hardware, d. h. ohne die Verwendung von Space-time Codes[8] möglich ist. Durch mehrere räumlich getrennte Sender wurde ein verteiltes MISO gebildet. In einem ersten Experiment wurde dabei zunächst ermittelt, wie genau die Interframe Spaces von der verwendeten Hardware (Atheros-Chipsatz) eingehalten werden. Die Abweichung war dabei nicht größer als $1\,\mu s$. In einem weiteren Versuch wurden bei 2 Empfängern die gleiche MAC-Adresse eingestellt. Ein weiteres Gerät sendet danach Pakete an diese Adresse. Durch Vergleiche der Statistiken über gesendete und empfangene Pakete des Sender, der Empfänger und eines weiterer passiven Empfängers, konnte gezeigt werden, dass sich die Acknowledgements beider Empfänger häufig konstruktiv überlagerten.

In einem Infrastruktur-Netzwerk lässt sich dies für verteilte Antennen nutzen. Die APs einer verteilten Antenne bekommen die gleiche MAC-Adresse. Pakete, welche an diese adressiert sind, werden von allen APs zeitgleich bestätigt. Ist ein AP in mehreren VAs involviert, so besitzt er mehrere MAC-Adressen.

Der Vorteil dieses Verfahrens ist, dass keine Kommunikation zwischen den APs nötig ist, sie also weit voneinander entfernt sein können. Dies bietet mehr Flexibilität, da die Auswahl der APs für eine verteilte Antenne weniger Beschränkungen hat.

Ein Nachteil ist, dass die Empfänger können nicht sofort erkennen, welcher weitere Empfänger das Paket eventuell korrekt erhalten hat. Hierfür ist zusätzliche Kommunikation über das drahtlose Medium bzw. einem drahtgebundenen Backbone nötig. Deshalb muss entweder jeder Empfänger die Daten weiterleiten oder eine zusätzliche Kommunikation zwischen den APs stattfinden.

4.2.4 Block Acknowledgement mit 802.11e

IEEE 802.11e bietet mit dem Block Acknowledgement eine weitere Möglichkeit, verteilte Antennen transparent für den Client zu implementieren. Beim Block Acknowledgement werden vom Sender bis zu 64 Pakete verschickt, ohne dass der Empfänger diese bestätigt. Erst nach dem letzten Paket schickt der Sender an den Empfänger ein Block-Acknowledgement-Request und erfragt somit beim Empfänger die Bestätigungen für die Pakete. Der Standard 802.11e definiert 2 Möglichkeiten, wie diese Bestätigung erfolgen kann.

Bei der sofortigen Bestätigung (*Immediate Block-Ack*) bestätigt der Empfänger den Block-Acknowledgement-Request mit einem Block-Ack, welches eine Bitmap für die maximal 64 Pakete enthält, um diese selektiv zu bestätigen.

Im Falle der verzögerten Bestätigung (*Delayed Block-Ack*) sendet der Empfänger eine klassische Bestätigung, wenn er den Block-Acknowledgement-Request erhält. Das Block-Ack sendet er bei der nächsten Möglichkeit. Bei der verzögerten Bestätigung wird, anders als bei der sofortigen Bestätigung, das Block-Ack wiederum vom Sender der Pakete bestätigt.

Durch die Verzögerung zwischen Erhalt der Pakete und dem Senden der Bestätigung, lässt sich das Block-Ack als Protokoll für verteilte Antennen verwenden. Clienten, die IEEE 802.11e unterstützen, müssen dafür nicht angepasst werden. Die APs der verteilten Antenne teilen dem AP, mit dem sich der Client assoziiert hat, über eine schnelles drahtgebundenes Netzwerk mit, welche Pakete sie von dem Clienten empfangen haben. Der AP bestätigt mit dem Block-Ack neben den Paketen, die er empfangen hat auch die der anderen APs.

Bei der sofortigen Bestätigung können je nach Geschwindigkeit des Backbones jedoch nicht alle Pakete, welche die APs der VA empfangen haben, bestätigt werden. Die Zeit zwischen dem letzten Paket des Clienten und dem Senden des Block-Acks ist zu kurz, damit andere APs dem AP des Clienten rechtzeitig über den Empfang dieses Paketes informieren können. Bei sehr hohen Latenzen zwischen den APs und sehr hohen Datenraten zwischen dem Clienten und den APs können evtl. mehrere Pakete am Ende eines solchen Blocks betroffen sein.

4.2.5 Multi-Radio Diversität

In [10] stellen Miu et. al das Multi-Radio Diversity (MRD) System vor. Dabei wird bei den APs und Clienten zwischen der MAC- und der Netzwerk-Schicht eine zusätzliche Sicherungsschicht eingefügt, welche für die erneute Versendung von nicht bestätigten Paketen zuständig ist. Die Hardware muss bei diesem Protokoll nicht verändert werden, lediglich das ARQ der MAC-Schicht wird ausgeschaltet, d. h. verlorene Pakete werden von der MAC-Schicht nicht erneut übertragen. Das ARQ wird stattdessen in der zusätzlichen Sicherungsschicht realisiert. Diese enthält eine Warteschlange für Pakete. Vom Empfänger bestätigte Pakete und Pakete, die auch nach mehren Versuchen nicht erfolgreich übertragen wurden, werden aus dieser herausgenommen.

Diese zusätzliche Schicht bietet die Möglichkeit zur Bildung von verteilten Antennen. Die APs senden empfangene Pakete an einen zentralen Controller, der den AP des Clienten über den Empfang der Pakete informiert. Die Sicherungsschicht des AP bestätigt dem Clienten dieses Paket.

Da die APs auch fehlerhafte Pakete, d. h. Pakete, deren CRC-Prüfsumme nicht korrekt ist, an den Controller schicken, besteht die Möglichkeit, dass dieser die fehlerhaften Versionen eines Paketes zu einem korrekten rekombinieren und auch dieses bestätigt wurde.

Der Nachteil ist jedoch, dass die Clienten angepasst werden müssen. Ihr Netzwerkstack wird wie bereits erwähnt um diese zusätzliche Sicherungsschicht erweitert.

4.3 Auswahl der verteilten Antennen

Die letzten 3 vorgestellten Verfahren Block-Acknowledgement, MRD und Bestätigung mit Sendediversität unterliegen bezüglich der maximalen Anzahl von APs innerhalb einer VA keiner Beschränkung, d. h. hier können im Extremfall alle APs eine VA bilden. Für die beiden oben beschriebenen Verfahren *Slotted Acknowledgement* und *Cognitive Acknowledgement* ist die Anzahl der APs in einer verteilten Antenne hingegen beschränkt. Bei ersterem ist das Limit jedoch nicht durch das Protokoll festgelegt. Es ergibt sich vielmehr durch den zusätzlichen Bandbreitenbedarf des Protokolls ein Trade-off zwischen dem Gewinn durch zusätzliche APs in der VA und die dafür zusätzlich benötige Bandbreite für das Protokoll.

Ziel bei der Auswahl der APs für eine VA ist die Minimierung der Übertragungsfehler bzw. die Maximierung der Wahrscheinlichkeit für eine erfolgreiche Übertragung (packet success rate; PSR) vom Clienten zu den APs. Diese lässt sich aus der PSR der einzelnen APs bzw. der Übertragungsstatistik bestimmen.

Für das Slotted Acknowledgement muss zudem die PSR zwischen den APs bekannt sein, welche ebenfalls anhand der Übertragungsstatistiken ermittelt werden kann. Über die Bestätigungen der einzelnen APs erfolgt beim Slotted Acknowledgement auch die Auswahl des APs, der das Paket des Clienten weiterleitet. Anhand der einzelnen PSR zwischen den APs und dem Clienten kann errechnet werden, wie hoch die PSR für die VA ist, welche von den APs gebildet wird[43].

Die Übertragungswahrscheinlichkeit zwischen den APs spielt beim Cognitive Acknowledgement hingegen keine Rolle. Hier müssen die APs lediglich die Übertragung eines anderen wahrnehmen. Um dies bei der Auswahl der APs für eine VA sicherzustellen, wird der Interferenzgraph benutzt (Abschnitt 3.1.1).

Ein hohes Kantengewicht im Interferenzgraph zeigt also, dass ein AP den jeweils anderen wahrnehmen kann. Durch Simulationen wurde ein Kantengewicht von 0,85 als Wert für eine sicheres Funktionieren des Protokolls ermittelt. APs, deren Kanten untereinander also dieses oder ein größeres Gewicht besitzen, können eine VA bilden.

Um die Übertragungswahrscheinlichkeit der VA für einen Client zu bestimmen, werden die einzelnen PSRs zwischen dem Clienten und den APs benötigt. Diese werden als unabhängig voneinander betrachtet. Die Übertragungswahrscheinlichkeit PSR_{VA} einer VA, die aus den APs $AP_1,\ldots,AP_n$ mit der jeweiligen Übertragungswahrscheinlichkeit $PSR_1,\ldots,PSR_n$ besteht, lässt sich wie folgt bestimmen:

$$PSR_{VA} \quad = \quad 1 - \prod_{i=1}^{n} (1 - PSR_i)$$

Für die Berechnung der PSR einer VA wird nur die Übertragungswahrscheinlichkeit von Clienten zu den APs, nicht jedoch die Rückrichtung betrachtet, da zum einen die Übertragungswahrscheinlichkeit vom AP zum Clienten nicht bekannt sind und es zum anderen die Rechnung extrem vereinfacht und die Ungenauigkeit im Verhältnis dazu vernachlässigbar ist.

In [12] zeigten Zubow et. al, dass die PSRs zwischen einem Sender und mehreren Empfänger nicht immer unabhängig voneinander sind. Ein Beispiel dafür sind Störquellen, welche mehrere Empfänger gleichzeitig beeinflussen. Eine starke Korrelation zwischen den Paketfehlern wurde jedoch nur bei geringen Abständen von bis zu 2 m festgestellt. Da die Abstände zwischen den APs in Infrastruktur-Netzwerken größer sind, wurde dies nicht berücksichtigt.

4.4 Paketaggregation

In Infrastruktur-Netzwerken sind die APs nicht direkt mit dem Internet verbunden, sondern senden die Pakete zunächst an einen gemeinsamen Gateway, der diese zum eigentlichen Ziel weiterleitet. Da bei einer verteilten Antenne alle APs, die eine solche bilden, die von ihnen empfangenen Pakete des

Clienten weiterleiten, kann es zu Duplikaten, d. h. zu mehrfachen Kopien des selben Paketes kommen. Ein Vorteil dabei ist, dass mehrere fehlerhaften Kopien eines Paketes, welche die APs empfangen haben, zu einem korrekten Paket rekombiniert werden können und man dadurch, wie Miu et. al in [10] zeigt, die Paketfehlerrate weiter reduzieren kann. Ein Nachteil dieses vielfachen Weiterleiten der selben Pakete durch mehrere APs ist jedoch der erhöhte Bandbreitenbedarf. Die beiden Vor- und Nachteile werden in den nächsten Abschnitten genauer untersucht. Dabei wird auf die vorgestellten Verfahren für VAs und ihre Besonderheiten eingegangen.

4.4.1 CRC-Fehler

Mit forward error correction (FEC) und automatic repeat request (ARQ) sieht der IEEE 802.11 Standard zwei Verfahren vor, Übertragungsfehler, die bei der drahtlosen Kommunikation u. a. durch Interferenzen oder zu schwachen Signalen auftreten, zu erkennen und zu korrigieren. Des weiteren gibt es verschiedene Ansätze mehrere fehlerhafte Versionen eines Paketes zu einem korrekten zu rekombinieren. In [22] stellt Dubois-Ferrière et. al einen sehr einfachen Ansatz vor. Statt defekte Pakete zu verwerfen, werden diese gespeichert, um mit weiteren fehlerhaften Kopien ein korrektes zu erhalten.

In [10] wird dieses Verfahren für verteilte Antennen erweitert. Hierbei leiten die APs, welche eine verteilte Antenne bilden, ihre empfangenen Pakete an einen Controller weiter, der die fehlerhaften Kopien wenn möglich zu einem korrekten Paket kombiniert. Bei erfolgreicher Korrektur wird dieses Paket bestätigt und eine Neuübertragung verhindert. Da jedoch die Rekonstruktion eines Paketes durch fehlerhafte Kopien komplex und zeitaufwändig ist, wird beim MRD[10] eine zusätzliche Sicherungsschicht zwischen MAC- und Netzwerkschicht eingefügt, die das ARQ auf höherer Schicht übernimmt. Dadurch kann die Zeitspanne zwischen Empfang eines Paketes und der Bestätigung ausreichend lang gemacht werden, um die Korrektur von Fehlern zu ermöglichen. Das in Abschnitt 4.2.4 beschriebene Block-Ack von IEEE 802.11 bietet durch seine Umsetzung des ARQ ebenfalls die Möglichkeit CRC-Fehler auf der Seite der Empfängern zu korrigieren und dabei mehrere Empfänger in einer verteilten Antenne zu verwenden.

Für die Korrektur von CRC-Fehler beim Vorliegen mehrerer fehlerhafter Kopien eines Paketes gibt es verschiedene Ansätze. Der einfachste Ansatz realisiert eine Mehrheitsentscheidung. Ein Bit an einer bestimmten Position erhält den Wert, den die meisten Kopien an dieser Stelle haben. Sollten 0 und 1 die gleiche Häufigkeit aufweisen, so wird mit beiden Varianten die CRC-Summe berechnet. Dieses Verfahren ist besonders bei wenigen Kopien sehr aufwändig. In [22] wird deshalb eine blockbasierte Kombinierung vorgeschlagen. Die empfangenen k Kopien eines Paketes, werden dazu jeweils in n Blöcke zerlegt. Die Blöcke werden dann miteinander kombiniert und jeweils die CRC-Summe bestimmt. Dieses blockbasierte Kombinieren der Pakete hat eine Komplexität von $O(k^n)$.

4.4.2 Bandbreite im Backend

Die APs einer verteilten Antenne leiten die empfangenen Pakete an einen Controller weiter. Um die vorliegende Netzwerksituation besser analysieren zu können, können die APs zusätzliche Information wie empfangene Signalstärke usw. mit dem Paket übertragen. Dies führt jedoch insgesamt dazu, dass mehr Bandbreite im Backbone verbraucht wird, da mehrere Kopien des selben Paketes von mehreren APs weitergeleitet werden. Bei sehr vielen APs und hoher Netzwerklast kann so auch ein schnelles Backbone, wie z. B. Gigabit-Ethernet an seine Grenzen stoßen.

Eine Reduzierung der benötigen Bandbreite im Backbone kann dadurch erreicht werden, dass die APs die empfangen Pakete zunächst speichern und dem Controller lediglich die Meta-Informationen zu dem Paket übermitteln. Die Meta-Informationen müssen dabei ausreichend sein, um das Paket eindeutig zu identifizieren. Die MAC-Adresse des Empfängers und des Absenders zusammen mit der Sequenznummer des Paketes stellt dies zum Beispiel sicher. Sollte der Controller zudem eine CRC-Korrektur vornehmen können, so muss zudem aus der Zustand des Paketes, d. h. ob es fehlerfrei ist oder nicht, übermittelt

werden. Der Controller kann dann das Paket selektiv bei den einzelnen APs anfordern. Dieser Ansatz führt jedoch zu einer erhöhten Latenz, was sich besonders auf TCP/IP-Anwendungen negativ auswirkt. Sie kann reduziert werden, indem der AP mit dem sich der Client assoziiert hat, das empfangene Paket immer sofort weiterleitet. Dadurch wird die Latenz nur dann erhöht, wenn dieser es nicht empfangen hat.

Das Slotted Acknowledgement und das Cognotive Acknowledgement bietet eine weitere Verbesserungsmöglichkeit. Beide Protokolle ermöglichen es den APs durch die gesendeten Bestätigungen zu ermitteln, wer das Paket empfangen hat. Die Empfänger sind bei beiden Protokollen durch eine Priorität sortiert. Es leitet jeweils der Empfänger das Paket weiter, welcher die höchste Priorität hat.

Begrenzte Bandbreite im Backend

Eine besondere Herausforderung ist die Realisierung von verteilten Antennen, wenn die entsprechenden APs an der drahtlosen Schnittstelle mehr Bandbreite zur Verfügung stellen können als zum Controller. Ein Beispiel dafür sind Hotspots, bei denen die APs über DSL-Leitungen mit dem Netzwerk des Anbieters verbunden sind. Hierbei liegt die Bandbreite, die 802.11 zur Verfügung stellt weit über dem, was gängige DSL-Anschlüsse bieten. In einem solchen Fall muss die Netzwerklast möglichst über die einzelnen APs verteilt werden.

Wie bereits beschrieben, können die APs die Pakete zunächst zwischenspeichern und den Controller nur über die empfangene Pakete informieren ohne sie komplett zu übertragen. Der Controller kann dann die Pakete selektiv von den einzelnen APs anfordern. Die Auswahl des APs, der das empfangene Paket weiterleiten soll, kann dabei so gewählt werden, dass die benötigte Bandbreite über alle APs gleichmäßig verteilt ist. In einem Beispielszenario, welches das verdeutlichen soll, sind alle APs einer VA mit der selben Bandbreite mit dem Controller verbunden. Der Controller fordert das empfangene Paket jeweils von dem AP an, dessen letzte Weiterleitung zeitlich am längsten zurückliegt (Balancing). Der Nachteil der erhöhten Latenz durch das Anfordern der Weiterleitung der Pakete ist bei der Anbindung der APs über DSL-Leitungen besonders stark. Es muss hierbei also zwischen hoher Latenz und benötigter Bandbreite abgewogen werden, wobei dabei die verfügbare Bandbreite entscheidend ist.

Das Cognitive Acknowledgement und das Slotted Acknowledgement bieten eine andere Möglichkeit. Wie oben bereits erläutert, kann hier die Priorität bestimmen, wer das Paket an den Controller weiterleitet. Durch Veränderung dieser Priorität, kann dabei Einfluss genommen werden, welcher AP das Paket vorrangig weiterleitet. Somit kann ohne zusätzliche Latenz die Netzwerklast im Backbone, d. h. auf die einzelnen DSL-Verbindungen, verteilt werden.

4.5 Zusammenfassung

In diesem Kapitel wurden verschiedene Verfahren zur Realisierung von verteilten Antennen erläutert. Dabei wurde darauf eingegangen, welche Komponenten des Netzwerkes zur Umsetzung verändert werden müssen und welche weiteren Möglichkeiten das jeweilige Verfahren bieten. Dazu gehört z. B. die Korrektur fehlerhafter Pakete durch mehrere empfangene Kopien. Der Bandbreitenbedarf zu einem zentralen Controller, welcher von allen vorgestellten Verfahren benötigt wird, wurde ebenfalls diskutiert. Die Tabelle 4.2 zeigt eine Zusammenfassung.

Für Infrastruktur-Netzwerke, bei denen die APs eine verteilte Antenne bilden sollen, eignen sich je nach Anforderung nicht alle der vorgestellten Verfahren. Das Slotted Acknowledgement und MRD benötigen Protokolländerungen beim Clienten, was bei der Vielfältigkeit der heutzutage benutzen Geräte aufwändig ist. Sowohl das Cognitive Acknowledgement als auch das Slotted Acknowledgement ermöglichen eine Reduzierung und Verteilung der Netzwerklast ohne die Latenz bei der Paketweiterleitung von den APs zum Controller zu erhöhen. Besonders bei Backbone mit geringer Bandbreite, wie z. B. DSL-Verbindungen, eignen sie sich deshalb besonders. Die Korrektur von CRC-Fehler kann, wie es in [10] gezeigt wurde, den Vorteil von verteilten Antennen gegenüber einzelnen APs weiter erhöhen. Lediglich

Tabelle 4.2: Zusammenfassung der vorgestellten Verfahren und ihre Eigenschaften.

Verfahren	Client-Änderung	Zusätzl. Bandbreitenbedarf	CRC-Korrektur
`Slotted Ack.`	Ja	gering	Nein
`Cognitive Ack.`	Nein	gering	Nein
`MRD`	Ja	hoch	Ja
`Block Ack.`	Nein	hoch	Ja
`Sendediversität`	Nein	hoch	Nein

MRD und mit kleinen Einschränkungen auch das Block Acknowledgement von IEEE 802.11e ermöglichen dies.

Das Ziel der Arbeit ist es u. a. die verteilten Antennen so zu realisieren, dass keine Änderungen bei den Clienten nötig sind. Da der Bandbreitenverbauch im Backbone ebenfalls ein wichtiges Kriterium ist, wird im weiteren Verlauf der Arbeit das Cognitive Acknowledgement verwendet.

Kapitel 5

Implementierung

In den beiden vorherigen Kapiteln wurden Verfahren für die Kanalzuweisung und Protokolle für verteilte Antennen vorgestellt. Ziel dieser Arbeit ist es zu untersuchen, inwieweit sich beide kombinieren lassen. Die Kombination wird durch gegensetzliche Ziele beider Verfahren erschwert. So versuchen Algorithmen für die Kanalzuweisung die Interferenzen zwischen den drahtlosen Geräten durch Verwendung möglichst vieler Kanäle zu minimieren, wodurch jedoch eine Kommunikation zwischen zwei APs in einen Infrastruktur-Netzwerk verhindert werden kann, wenn diese unterschiedliche Kanläle verwenden. Bei den Protokollen für verteile Antennen wie das Slotted Acknowledgement und das Cognitive Acknowledgement findet jedoch eine Koordination zwischen den einzelnen APs über das drahtlose Medium statt, wodurch sie den selben Kanal verwenden müssen.

Da ein weiteres Ziel der Arbeit war, die Clienten in einem Infrastruktur-Netzwerk nicht verändern zu müssen, wurde für die verteilten Antennen das Cognitive Acknowledgement als MAC-Sicherung gewählt, da es, wie in Abschnitt 4.2.2 beschrieben nur eine Softwareänderung (MAC-Protokoll) bei den APs benötigt.

5.1 Netzwerksimulator

JiST (**J**ava **i**n **S**imulation **T**ime,[14]) ist ein in Java geschriebener diskreter ereignisgesteuerter Simulator. Der Bytecode der Java-Anwendungen wird zur Laufzeit von einem Bytecode-Rewriter modifiziert und dann in Simulationszeit ausgeführt. Der Quellcode wird dabei nicht verändert, d. h. für die Anwendungen ist die Simulation völlig transparent. Dies vereinfacht die Entwicklung deutlich, da nicht wie bei anderen Simulatoren, wie z. B. ns-2[33], eine zusätzliche Sprache für die Simulationsbeschreibung o. ä. erlernt werden muss.

SWANS (**S**calable **W**ireless **A**d-hoc **N**etwork **S**imulation) erweitert JiST um die Möglichkeit drahtlose Netzwerke zu simulieren. Die Architektur von SWANS orientiert sich dabei am ISO-OSI-Referenzmodell (Abbildung 5.1). Diese Strukturierung ermöglicht ein einfaches Austauschen von einzelnen Komponenten, wie z. B. der MAC-Schicht. Da SWANS wie auch JiST in Java geschrieben ist und dadurch Konzepte wie Vererbung zur Verfügung stehen, lassen sich vorhandene Komponenten des Protokolstack leicht erweitern. Für SWANS sind bereits verschiedenen Protokolle implementiert, u. a. das IEEE 802.11-MAC-Protokoll, Routingprotokolle wie DSR und AODV und das UDP- und TCP-Protokoll. Des weiteren gibt es in SWANS bereits einige Pfadverlustmodelle.

Der Berlin RoofNet Simulator (BRN.Sim) basiert auf JiST/SWANS. Neben zusätzlichen Radiomodellen wurden unter anderem auch IEEE 802.11e und verschiedene Bitraten-Algorithmen für IEEE 802.11 implementiert. Des weiteren wurde eine graphische Benutzeroberfläche hinzugefügt, welche die Bedienung

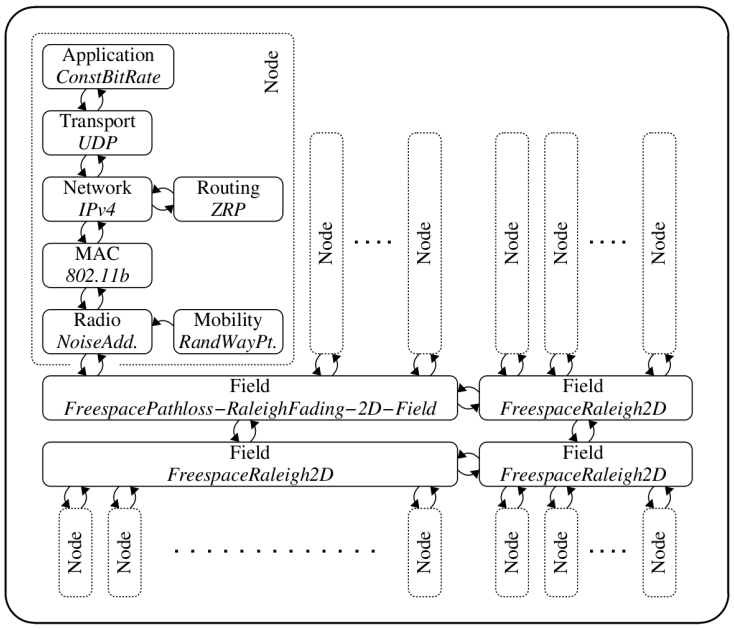

Abbildung 5.1: Architektur von SWANS.

des Simulators und das Auswerten der Ergebnisse erheblich vereinfacht. Ein weiteres wichtiges Werkzeug ist *DistSim*, ein System für die Verteilung von Simulationen. Damit ist es möglich, eine Vielzahl von Simulationen mit unterschiedlichen Parametern auf mehreren Rechner parallel laufen zu lassen, wodurch die Evaluation, z. B. von neuen Protokollen, beschleunigt wird.

5.2 Controller

Der Controller ist die zentrale Komponente des Netzwerkes. Alle APs sind mit ihm verbunden und leiten die empfangenen Pakete an ihn weiter. Er erstellt Statistiken, wie z. B. Paketfehlerrate zwischen den Clienten und den APs. Des weiteren nimmt der Controller die Kanalzuweisung vor und bestimmt mit welchem AP sich neue Clienten assoziieren dürfen. Die Abbildung 5.2 zeigt die einzelnen Elemente des Controllers und ihre Abhängigkeiten untereinander.

Die am Controller angemeldeten APs und die Clienten werden in einer zentralen Datenbank gespeichert. Neben dem momentan verwendeten Kanal ist dort auch die aktuelle Sende- und Empfangsrate jedes Knoten im Netzwerk gespeichert. Die Datenbank enthält aber auch die Information über erkannte Störquelle, wie z. B. fremde Netze. Des weiteren steuert der Controller auch die Messung für den Interferenzgraphen und wertet die Ergebnisse aus. Mit Hilfe der Übertragungsstatistik und dem Interferenzgraphen nimmt der Controller die Kanalzuweisung vor und bestimmt mögliche Antennen. Bei der Zuweisung der Antennen wird dabei auch die Lastverteilung im Netzwerk berücksichtigt.

5.2.1 Interferenzgraph

Der Interferenzgraph wird mit dem in Kapitel 3.1.1 beschriebenen Maximum-Troughput-Verfahren bestimmt, bei welchen jeder AP sowohl alleine als auch paarweise mit jedem anderen AP die maximale Senderate einer Broadcastübertragung ermittelt. Die Anzahl F der nötigen Messungen wächst dabei

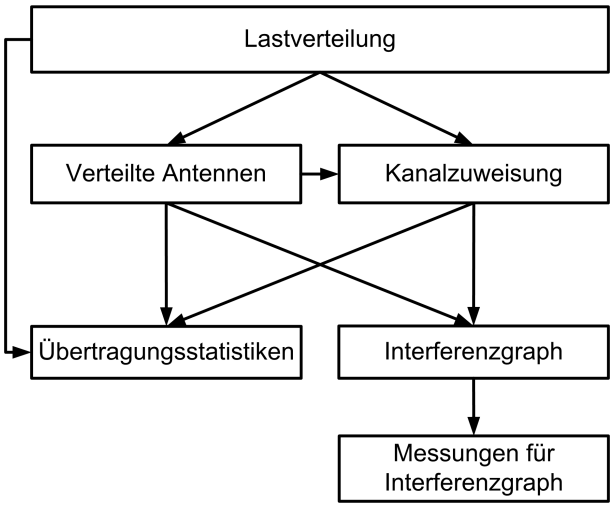

Abbildung 5.2: Aufbau des Controllers

durch das paarweise Messen quadratisch mit der Anzahl der Knoten:

$$F = n + \frac{n \cdot (n-1)}{2}$$

Da die Interferenzen auf den verschiedenen Kanälen unterschiedlich stark sein können, müssen die Messungen auf allen Kanälen wiederholt werden. Die Messungen selbst werden vom Controller selbst gesteuert. Er erstellt einen Ablaufplan für die Messungen und starten diese auf den einzelnen APs. Dazu sendet er ihnen kurze Nachrichten mit den benötigten Informationen, wie z. B. die Dauer der Messung und die zu verwendende Bitrate. Die Ergebnisse über die erzielten Sende- und Empfangsraten werden von den APs an den Controller gesendet, der daraus den Interferenzgraphen bestimmt.

5.2.2 Übertragungsstatistiken

Sowohl für die Kanalzuweisung als auch für die Bildung von verteilten Antennen werden Statistiken über die empfangenen und gesendeten Pakete der einzelnen APs und Clienten im Netzwerk benötigt. Dazu gehört u. a. auch die Paketfehlerrate. Die APs übermitteln deshalb verschiedene Informationen über die empfangenen Pakete an der Controller, der diese auswertet. Dazu gehören u. a.:

1. Absender- und Zieladresse (MAC)
2. MAC-Sequenznummer (IEEE 802.11)
3. Empfangene Signalstärke (RSSI)
4. Zustand (korrekt, fehlerhaft,...)
5. Paketgröße
6. Verwendete Bitrate

Der Controller bestimmt daraus u. a. die Sende- und Empfangsrate der APs bzw. Clienten. Des weiteren lässt sich durch diese Information die Auslastung der Kanäle bestimmen[32].

5.3 Kanalzuweisung

In den Abschnitten 3.3 bis 3.6 wurden 4 Verfahren für die Kanalzuweisung vorgestellt. Sie unterscheiden sich darin, ob sie den aktuellen Netzwerkverkehr und die Interferenz bei den Clienten berücksichtigen oder nicht:

- **Client- und Traffic Aware**: Sowohl die Interferenz bei den Clienten als auch der Netzwerkverkehr wird bei der Kanalzuweisung berücksichtigt.
- **Clientagnostic und Traffic Aware**: Der Netzwerkverkehr wird berücksichtigt.
- **Client Aware und Trafficagnostic**: Die Interferenz bei den Clienten wird berücksichtigt.
- **Client- und Trafficagnostic**: Bei der Kanalzuweisung wird nur die Interferenz zwischen den APs berücksichtigt.

Alle 4 Verfahren wurden als Optimierungsproblem formuliert, dessen Lösung NP-hart ist. Da dies deshalb nicht praktikabel sind, wurden verschiedene Heuristiken vorgestellt, welche eine geringe Komplexität aufweisen (Kapitel 3.7):

1. Random
2. Merge
3. Simulated Annealing
4. LRU

Diese Heuristiken wurden implementiert, wobei dabei sowohl der Netzwerkverkehr als auch die Clienten unberücksichtigt blieben (Client- und Trafficagnostic). Für die Bestimmung der Kanalzuweisung benötigen die Heuristiken sowohl den Interferenzgraphen als auch eine Liste aller Knoten im Netz (Clienten und APs). Letzteres enthält zu jedem Knoten auch die Sende- und Empfangsraten, welcher anhand der Übertragungsstatistik ermittelt wurden. Dadurch wäre auch eine Implementierung der Heuristik möglich, welche den Netzwerkverkehr berücksichtigt. Durch eine Erweiterung des Interferenzgraphen, um die Clienten im Netzwerk, könnte dies bei der Kanalzuweisung berücksichtigt werden (Client Aware). Der Interferenzgraph enthält zusätzlich Informationen über externe Störquellen, welche ebenfalls von den Heuristiken berücksichtigt werden.

Der Kanalwechsel bei den APs erfolgt allerdings nicht unmittelbar nach der Kanalzuweisung, sondern die neuen Kanäle der APs bzw. der Clienten werden zunächst nur vom Controller vermerkt. Die Bildung von verteilten Antennen kann die Kanalzuweisung noch einmal ändern. Erst nach der Festlegung der verteilten Antennen wird die Kanaländerung von den Knoten übernommen.

5.4 Verteilte Antennen

Die Festlegung der verteilten Antennen erfolgt, wie Abbildung 5.2 zeigt, auf Grundlage der Übertragungsstatistik und des Interferenzgraphen. Dazu werden im Interferenzgraphen alle von APs gebildeten Cliquen gesucht. Im Interferenzgraphen werden jedoch nur jene Kanten berücksichtigt, deren Gewicht einen gewissen Wert überschreiten. Durch Simulation (Abschnitt 6.2) wurde ein Wert von 0,85 als Richtwert ermittelt. Bei kleineren Werten kam es häufig zu VAs, bei denen das Cognitive Acknowledgement nur unzureichend funktionierte. Die APs einer Clique müssen zudem den selben Kanal haben. Die so gefundenen Cliquen sind die potentiellen VAs. Für jeden Clienten wird mit Hilfe der Übertragungsstatistik die

Übertragungswahrscheinlichkeiten (Packet success rate; PSR) für jede dieser VAs bestimmt. Dabei werden die einzelnen Übertragungswahrscheinlichkeiten als unabhägig angesehen (siehe Kapitel 4.3). Dadurch ergibt sich z. B. für die beiden APs A und B mit der PSR von PSR_A und PSR_B folgende Gesamt-PSR PSR_{AB}:

$$PSR_{AB} = 1 - ((1 - PSR_A) \cdot (1 - PSR_B))$$

Die endgültige Zuweisung von verteilten Antennen zu den Clienten wird von den Strategien für die Assoziierung bestimmt, die sich hauptsächlich darin unterscheiden, ob die Assoziierung vom Controller oder vom Clienten gesteuert wird. Es wurden 2 Strategien für die Assoziierung umgesetzt:

1. AP mit der höchsten Signalstärke
2. Beste verteilte Antenne

Bei dem ersten Verfahren assoziiert sich der Client mit dem AP mit der höchsten empfangenen Signalstärke. Dies ist die gängigste Methode. Der Controller sucht nun alle verteilten Antennen heraus, welche den vom Clienten gewählten AP als höchst priorisierten enthalten. Daraus wiederum weißt er dem Clienten jene mit der höchsten Gesamt-PSR zu.

Diese muss jedoch nicht die bestmögliche verteilte Antenne sein. Durch die Möglichkeit des APs, die Assoziierung eines Clienten ablehnen zu können (Kapitel 2.3), kann ein zentraler Controller gezielt die Assoziierung beeinflussen, indem er nur den von ihm festgelegten AP eine Assoziierung durch den Client gestattet. Dadurch ist es möglich dem Clienten die beste verteilte Antenne, d. h. jene mit der höchsten PSR, zuzuweisen. Dies realisiert das zweite Verfahren für die Assoziierung.

Nachdem für jeden Clienten eine verteilte Antenne ermittelt wurden, wird überprüft, ob einzelne APs noch keinen Clienten haben. Diese werden anderen verteilten Antennen auf anderen Kanälen hinzugefügt, wenn dadurch eine Verringerung der Fehlübertragungen zu erwarten ist. Hierdurch wird die Kanalzuweisung noch einmal geändert.

5.5 MAC-Schicht

Im Kapitel 4.2 wurden verschiedene Möglichkeiten aufgezeigt, auf welche Art und Weise eine Kooperation auf Empfängerseite möglich ist. Im Rahmen dieser Arbeit wurde das in Kapitel 4.2.2 vorgestellte Cognitive Acknowledgement implementiert.

Der AP bestätigt nicht nur die an ihn gerichteten Pakete seiner eigenen Clienten, sondern auch Pakete von Clienten für die er mit anderen APs eine verteilte Antenne bildet. Er erhält dazu vom Controller eine Liste, bestehend aus Tupeln von MAC-Adressen von Clienten und den Prioritäten innerhalb der entsprechenden VA. Der AP untersucht die Absenderadresse von Paketen und sucht den entsprechenden Eintrag aus der Liste heraus. Anhand der Priorität bestimmt der AP die Wartedauer, nach welcher er überprüft, ob ein andere AP das Datenpaket bereits bestätigt (Listing 5.1).

Listing 5.1: Berechnung der Wartezeit für das verteilte Acknowledgement

```
long getAckWaitTime(int position) {
  long waitTime = getSifs()
                  + (position-1)*getSlotTime()
                  + (getSlotTime()-getRxTxTurnaround());//CCA
  return waitTime;
}
```

Die Entscheidung, ob das Medium frei ist bzw. ein anderer AP eine Bestätigung sendet, wird in Abhängigkeit von der empfangenen Signalstärke getroffen. Für die Simulation wurden 4 verschiedene Ansätze implementiert und verglichen. Die Bestätigung für ein Datenpaket wird dabei entweder:

1. immer gesendet ("Immer").
2. nur gesendet, wenn das Radio nichts empfängt, d. h. die Signalstärke liegt unterhalb des Schwellwertes für das Empfangen von Daten ("Frei").
3. gesendet, wenn das Medium frei ist, d. h. die Signalstärke liegt unterhalb des Schwellwertes für das Sensing ("Nicht Empfangen").
4. nur gesendet, wenn die Signalstärke unterhalb eines vom gemessenen Rauschen abhängigen Schwellwertes liegt ("Nicht Wahrnehmen").

Das erste der 4 Verfahren benutzt nicht die Funktion zum Berechnen der Wartezeit, sondern alle APs der verteilten Antenne senden nach SIFS gleichzeitig eine Bestätigung für das Datenpaket. Da dieses Verfahren gänzlich auf die Erkennung der Bestätigung anderer APs verzichtet, sind die Resultate ähnlich denen, wenn bei den anderen 3 Verfahren die Erkennung auf Grund von zu großen Entfernungen zwischen den APs versagt. Der Simulator realisiert den Capture-Effekt, d. h. beim gleichzeitigen Senden der Bestätigungen wird, wenn der Unterschied der Signalstärken der empfangenen Signale ausreichend groß ist, das stärkste Signal empfangen. Bei zu geringen Unterschieden kommt es zur Kollision und somit zum Verlust. Dieses Verfahren ("Immer") wurde für den Vergleich mit den anderen implementiert, da es unter bestimmten Voraussetzung ebenfalls ein Gewinn der verteilten Antenne gegenüber einem einzelnen AP hinsichtlich der Paketfehlerrate bringt. Im Anhang A wird dies näher erläutert und an Beispielen erklärt.

Bei den anderen 3 MAC-Optionen wird eine Übertragung anhand der gemessenen Signalstärke erkannt, jedoch werden dabei unterschiedliche Schwellwerte verwendet. Liegt die gemessene Signalstärke oberhalb des jeweiligen Schwellwertes, wird davon ausgegangen, dass ein anderer AP eine Bestätigung sendet. Für das Verfahren "Frei" liegt der Schwellwert für die Signalstärke bei -95 dB. Bei diesem und höheren Werten wechselt das Radio in den Empfangsmodus.

Der Grenzwert von -96 dB wird von dem Verfahren "Nicht Empfangen" benutzt, da bei dieser und höherer Signalstärke das Radio in den Modus "Sensing" wechselt. Daten können dabei nicht dekodiert werden, jedoch erkennt das Radio die hohe Signalstärke als Übertragung und geht von einem belegtem Medium aus.

Die Grenzwerte der eben beschriebenen Verfahren "Nicht Empfangen" und "Frei" sind statisch, d. h. auch bei unterschiedlich starkem Rauschen gleich. Dies führt zu Problemen bei parallelen Übertragungen, die nicht empfangen, jedoch durch eine höheres Rauschen wahrgenommen werden. Die beiden Verfahren "Nicht Empfangen" und "Frei" erkennen auch solche fälschlicherweise als Bestätigung und senden ihrerseits keine Bestätigung. Deshalb wird für das Verfahren "Nicht Wahrnehmen" ein dynamischer Schwellwert verwendet. Dazu wird nachdem das Datenpaket des Clienten empfangen wurde, die anliegende Signalstärke bestimmt. Dies ist der Referenzwert für die Erkennung. Sollte zu diesem Zeitpunkt eine weiter Übertragungen stattfinden, welche der AP nicht empfangen, aber dennoch wahrnehmen kann, so wird dies zu einer höheren gemessenen Signalstärke führen. Das Senden einer Bestätigung durch einen höher priorisierten AP, führt zu einem weiteren Anstieg der Signalstärke. Der Faktor, um welchen die Signalstärke ansteigen muss, damit ein AP von einer Übertragung durch einen anderen AP der VA ausgeht, ist ein Parameter des Cognitiven Acknowledgement.

Durch Simulationen wurde ein Faktor von 1,5 als zuverlässiger Wert ermittelt. Sollte die Signalstärke zwischen ersten Messen kurz nach Empfang des Paketes des Clienten (P_0) und dem Messen zur Erkennung der Bestätigung eines anderen APs, um mindestens das 1,5-fache steigen, so erkennt das Cognitive Acknowledgement die Bestätigung. Der Faktor von 1,5 entspricht 1,76 dB:

$$\begin{aligned} Schwellwert &\leqq Gemessenes\ Rauschen + 10 \cdot log_{10}\left(\frac{1,5 \cdot P_0}{P_0}\right) dB \\ &\lesssim Gemessenes\ Rauschen + 1,76\, dB \end{aligned}$$

5.6 Packetaggregation

Durch den Einsatz von verteilten Antennen kann es zu Duplikaten kommen, wenn mehrere APs das gleiche Paket empfangen und es an den Controller weiterleiten. Dieser muss deshalb mehrfach erhaltene Pakete erkennen und herausfiltern. Jedes Paket bekommt dazu eine eindeutige ID. Diese kann z. B. aus der Absenderadresse und der Sequenznummer des Paketes oder einem Hashwert bestehen. Die Eindeutigkeit muss dabei nur über einen kurzen Zeitraum sichergestellt sein, in welchem Duplikate auftreten können.

Im verwendeten Simulator wurde jedes Paket durch die Nummer des Paketflusses und der Paketnummer innerhalb des Flusses eindeutig identifiziert.

Die im Kapitel 4.4.1 erwähnte Möglichkeit aus mehren fehlerhaften Kopien ein korrektes Paket zu erzeugen, wurde nicht umgesetzt, da die Bitfehlermodelle des Simulator nicht verwendet wurden und somit keine fehlerhaften Pakete empfangen wurden. Diese wurden zuvor vom MAC verworfen.

5.7 Simulationsparameter

Im Simulator sollen Kanalzuweisung und verteilte Antennen einzeln und in Kombination evaluiert werden. Eine Simulation lässt sich dazu hauptsächlich über 4 Parameter steuern:

1. Anzahl der Kanäle
2. Kanalzuweisungsverfahren (Heuristik)
3. Maximale Größe der verteilten Antennen
4. MAC-Option (Cognitive Acknowledgement)

Wird bei einer Simulation nur ein Kanal verwendet, so findet keine Kanalzuweisung statt und alle APs verwenden den selben Kanal. Falls mehr als ein Kanal verwendet wird, so wird die gewählte Heuristik für die Kanalzuweisung verwendet. Über die Größe der verteilten Antenne wird die maximal Anzahl von APs festgelegt, die eine verteilte Antenne bilden können. Bei nur einem AP in einer VA, d. h. die Größe ist auf eins festgelegt, werden keine verteilten Antennen verwendet. Für die verteilten Antennen wird immer das Cognitive Acknowledgement als MAC-Sicherung verwendet. Über die MAC-Option lässt sich dabei festlegen, welches Verfahren für die Erkennung der Bestätigung innerhalb einer VA verwendet wird (Abschnitt 5.5).

5.8 Simulationsaufbau

Die beschriebenen Komponenten wurden im Netzwerksimulator implementiert. Eine Simulation ist in drei teile gegliedert:

1. Analyse
2. Konfiguration

3. Messung

Die Abbildung 5.3 zeigt den Ablauf, der die ersten beiden Punkte (Analyse, Konfiguration) umfasst. In den folgenden Abschnitten werden die einzelnen Schritte genauer erläutert.

5.8.1 Analyse

Für die Kanalzuweisung und das Bilden der verteilten Antennen muss sowohl der Interferenzgraph als auch die Paketfehlerraten von den Clienten zu den APs bekannt sein. Deshalb werden zunächst die Messungen der Interferenzen (Abschnitt 5.2.1) durchgeführt und daraus der Interferenzgraph bestimmt (Abschnitt 3.1.1). Eine einzelne Messung dauert jeweils $2\,s$.

Da die Messungen für den Interferenzgraphen sehr zeitaufwendig ist, und z. B. im Simulator beim Vergleich mehrerer Heuristiken für die Kanalzuweisung die gleichen Knotenplatzierungen sowie Radiomodelle verwendet werden, wird diese Messung bei großen Netzen jeweils einmalig durchgeführt und bei den nachfolgenden Simulationen dieser gespeicherte Interferenzgraph verwendet (Interferenzgraph-Caching). Dadurch kann die Simulationszeit deutlich verkürzt werden.

Nachdem der Interferenzgraph bestimmt ist, senden die Clienten für $10\,s$ mit einer konstanten und geringen Rate Broadcastpakete. Dadurch wird mit Hilfe der Übertragungsstatistik (Abschnitt 5.2.2) die Paketfehlerrate zwischen den Clienten und AP bestimmt.

5.8.2 Konfiguration

Im Anschluss an die Analyse erfolgt die Konfiguration, welche aus 3 Teilen besteht:

1. Kanalzuweisung
2. Bildung und Zuweisung der verteilten Antennen
3. Verbesserung der verteilten Antennen durch Kanalwechsel bei unbenutzten APs

Für die Konfiguration wird der Interferenzgraph und die Paketstatistik aus der Analyse benötigt. Zunächst wird die Kanalzuweisung vorgenommen, wobei dabei die maximale Anzahl der Kanäle und die zu verwendende Heuristik über entsprechende Parameter (Abschnitt 5.7) gewählt werden. Bei nur einem Kanal entfällt entsprechend die Kanalzuweisung, d. h. alle AP bekommen den selben Kanal. Dadurch können die verteilten Antennen isoliert evaluiert werden.

Nach der Kanalzuweisung werden für die Clienten alle potentiellen verteilten Antennen bestimmt. Die maximale Größe der VA wird über einen Parameter festgelegt. Welche verteilte Antenne dem Clienten zugewiesen wird, hängt von der Assoziierung ab. Die Wahl des APs kann dabei vom Clienten oder dem Controller gemacht werden. Ersteres entspricht der gängigen Praxis. Der Client sucht sich anhand der Signalstärke der Beacons den besten AP, d. h. jenen mit der höchsten empfangenen Signalstärke, heraus. In diesem Fall wird dem Clienten die beste verteilte Antenne zugewiesen, welche den von ihm gewählten AP enthält. Eine weitere Möglichkeit besteht, dass der Controller den AP für den Clienten bestimmt. In diesem Fall wählt er die verteilte Antenne mit der geringsten Paketfehlerrate aus. Der Client wird dann gezwungen sich mit dem höchst priorisierten AP der VA zu assoziieren, indem alle anderen eine Assoziierung des Clienten ablehnen.

Im letzten Schritt werden nun unbenutzte APs gesucht. Diese werden von keiner verteilten Antenne benutzt und können so ihren Kanal wechseln ohne die bisherige Konfiguration zu beeinflussen. Der Controller ermittelt neue verteilte Antennen, bei denen diese unbenutzten APs keinen festen Kanal haben, d.h. sie dürfen jeden Kanal verwenden, der zur Verfügung steht. Sollten sich dabei für einzelne Clienten andere VAs mit einer geringeren Paketfehlerrate ergeben, so bekommen sie diese zugewiesen. Dabei muss jedoch beachtet werden, dass der von Clienten gewählte AP wiederum in dieser VA enthalten ist.

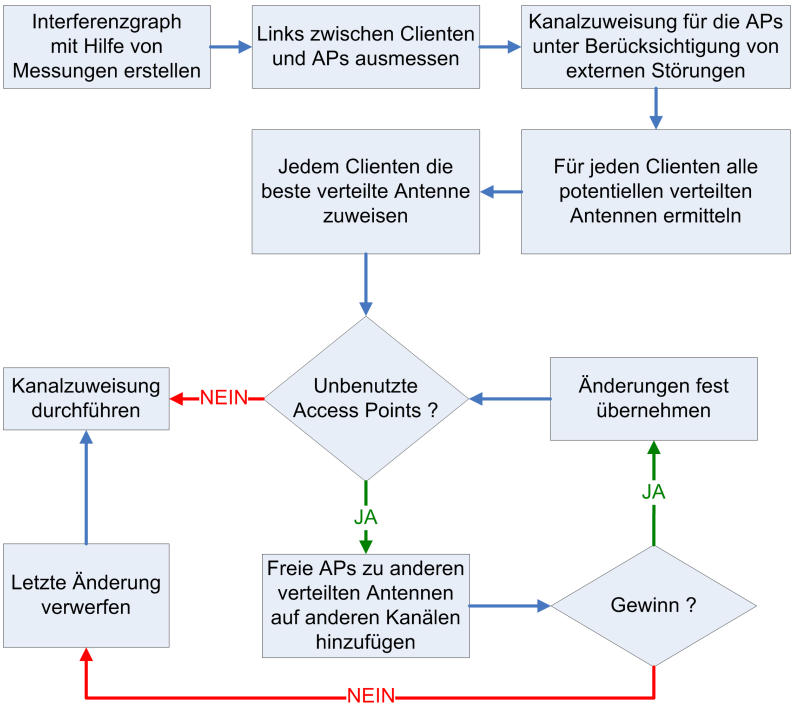

Abbildung 5.3: Die Kanalzuweisung erfolgt vor dem Ermitteln möglicher verteilter Antennen und der Zuweisung von Clienten zu den Access Points. Die Kanäle einzelner, unbenutzter APs können geändert werden, damit diese anderen VAs zugeordnet werden können, wenn dadurch eine bessere Gesamtleistung zu erwarten ist.

Bilden z. B. in einem Netzwerk die APs AP_1 und AP_2 auf dem Kanal k_1 eine verteilte Antenne für den Clienten C und ist AP_3, welcher den Kanal k_2 verwendet, unbenutzt, so kann dieser den Kanal wechseln. Hat die verteilte Antenne aus AP_1 und AP_3 eine geringere Fehlerrate als jene aus AP_1 und AP_2, so wird sie dem Clienten C zugewiesen. Der AP AP_3 verwendet dann den Kanal k_1.

5.8.3 Messung

Die Bewertung der einzelnen Heuristiken für die Kanalzuweisung, den verteilten Antennen bzw. der Kombination der beiden Verfahren erfolgt anhand des erzielten Durchsatzes und der Latenzen. Dazu werden UDP-Paketflüsse mit unterschiedlichen Datenraten vom Clienten zu den APs (Uplink) aufgesetzt und der erzielte Durchsatz der einzelnen Clienten ermittelt. Die Messung wird unmittelbar nach der Konfiguration gestartet und dauert 10 s. Zusätzlich zum Durchsatz wird die Zuverlässigkeit des Cognitive Acknowledgement ermittelt. Dazu wird für jeden AP gespeichert, welche Pakete er von welchen Clienten empfangen hat und ob er die Bestätigung eines anderen APs wahrgenommen bzw. selber eine Bestätigung gesendet hat. Diese Information ermöglicht es zu erkennen, ob und unter welchen Voraussetzung das Cognitive Acknowledgement funktioniert. Es lässt sich dadurch auch bewerten, ob die Festlegung der verteilten Antennen anhand der Paketstatistik und des Interferenzgraphen zuverlässige Ergebnisse liefert.

5.9 Erweiterungen in JiST/SWANS

Im Rahmen der Arbeit wurde der Simulator um Funktionalitäten erweitert. Zum einen sollte die Platzierung der Knoten auch anhand von realen geographischen Koordinaten vorgenommen werden können. Zum anderen musste, da die APs in einem Infrastruktur-Netzwerk ihre Position nicht ändern und damit stationär sind, wohingegen die Clienten mobil sind, das Feldmodell dahingehen erweitert werden, dies zu modellieren. Beide Erweiterungen werden im folgenden Abschnitt beschrieben.

5.9.1 Platzierung anhand geographischer Koordinaten

Bei Simulationen von drahtlosen Netzen werden die Knoten meist zufällig anhand einer Verteilung, wie z. B. Poission, platziert. Für diese Arbeit standen die Standorte (Koordinaten) von DSL-Anschlüssen zur Verfügung (Abb. 5.4). Da heutzutage die Kunden von DSL-Providern meist einen Access Point zu ihrem DSL-Anschluss bekommen, kann man davon ausgehen, dass an vielen dieser Standorte ein AP steht.

Für einen DSL-Provider bietet sich somit die Möglichkeit eine flächendeckende öffentliche Infrastruktur anzubieten. Dazu nutzt er einen Teil der DSL-Verbindung um darüber den Datenverkehr von anderen Benutzern ins Netzwerk des Providers zu transportieren[40]. Im Backend kann sich ein zentraler Controller befinden, der auf Grundlage der übertragenen Information die Kanalzuweisung vornimmt.

Abbildung 5.4: Für die Platzierung der APs lagen die Positionen von DSL-Anschlüssen vor. Es wurde dabei angenommen, dass an jedem Anschluss ein DSL-Router steht, welcher gleichzeitig mit einem WiFi-AP ausgestattet ist. Diese Abbildung zeigt eine Illustration.

5.9.2 Feldmodell

Im Simulator kann Mobilität durch Änderung der einzelnen Knotenposition auf dem Feld realisiert werden, ferner ist es möglich Schwankungen der Signalstärke infolge von Mobilität durch Shadow-Fading nachzubilden, welches ein Teil des Modells für den Pfadverlust ist. Shadowing ist ein gaussverteilter Zufallsprozeß mit einem Mittelwert und einer Standardabweichung (in dB), die von der Umgebung abhängig ist und die Stärke der Abschattung repräsentiert. Durch eine hohe Standardabweichung werden große Abschattungen modelliert, z. B. Betonwände. Kleinere Werte, werden für die Modellierung geringerer Abschattung (z. B. dünne Wände) verwendet. Das vorhandene Modell in JiST/SWANS macht dabei keinen Unterschied zwischen den einzelnen Knoten des Feldes. Die entspricht u. U. nicht der Realität, wo

APs an festen Orten installiert sind und lediglich die Clienten Mobilität aufweisen. Das Feldmodell wurde deshalb dahingehen angepasst, die Knoten in 2 Gruppen zu teilen. Die Werte für die Standardabweichung des Shadowing können bei diesem erweiterten Modell, sowohl für das Kanalmodell innerhalb der einzelnen Gruppen als auch für jenes zwischen ihnen, einzeln festgelegt werden. Zwischen den Access Points wurde die Standardabweichung auf 0dB gesetzt, d. h. zwischen ihnen gab es keine sich ändernde Abschattung, zwischen den einzelnen Clienten bzw. zwischen den Clienten und den APs wurden größer Werte für die Standardabweichung verwendet, da es durch die Mobilität der Clienten zu einer Veränderung der Abschattungen kommt.

Kapitel 6

Evaluation

Die 3 folgenden Szenarien werden in diesem Abschnitt mit Hilfe von Simulationen evaluiert:

1. Kanalzuweisung
2. Verteilte Antennen
3. Kombination von Kanalzuweisung und verteilten Antennen

Ziel der Simulationen war es zu ermitteln, ob und wie sich beide Ansätze kombinieren lassen. Dazu wurden beide Ansätze zunächst getrennt untersucht. Da für die Kanalzuweisung mehrere Algorithmen implementiert wurden, sollte durch Simulationen von verschiedenen Szenarien, jener ermittelt, der die besten Ergebnisse hinsichtlich des mittleren Durchsatzes im Netzwerk zeigte. Dieser wurde dann auch für alle weiteren Simulationen, bei denen mehr als ein Kanal verwendet und somit eine Kanalzuweisung benötigt wurde, verwendet. Das MAC-Protokoll für verteilte Antennen wurde in verschiedenen Szenarien untersucht, um zunächst zu ermitteln, welcher der Ansätze für die Erkennung einer gesendeten Bestätigung innerhalb der verteilten Antenne die besten Ergebnisse liefert. Dabei war nicht nur der Durchsatz entscheidend, sondern vor allem wie zuverlässig der jeweils verwendete Ansatz funktionierte, d. h. wie häufig fälschlicherweise eine Bestätigung erkannt und wie oft eine solche nicht wahrgenommen wurde.

Zum Abschluss wurden beide Verfahren, Kanalzuweisung und verteilte Antennen, kombiniert. Es sollte untersucht werden, ob und unter welchen Voraussetzung von beiden gleichzeitig profitiert werden kann. Auf Grundlage der Ergebnisse der Simulationen lässt sich ein dynamisches System entwerfen, welches abhängig von der momentanen Anforderung an das Netzwerk, beide Verfahren bestmöglich kombiniert.

Die Simulationen wurden für jedes Szenario 50 mal wiederholt, um fundierte Ergebnisse zu erhalten. Als Konfidenz wird der Standardfehler angeben. Der Durchsatz wurde sowohl von den APs zu den Clienten (Download) als auch in der anderen Richtig (Upload) gemessen. Da die verteilten Antennen von den APs gebildet werden und somit nur der Durchsatz vom Client zu den APs verbessert wird, bezieht sich der Begriff “Durchsatz” in diesem Kapitel ausschließlich auf Paketflüsse von den Clienten zu den APs.

6.1 Kanalzuweisung

Zunächst wurden die vier in Kapitel 3.7 vorgestellten Heuristiken:

1. Random
2. Merge

3. LRU

4. Simulated Annealing

in verschiedenen Szenarien verglichen. Die optimale Kanalzuweisung durch erschöpfende Suche konnte im Rahmen dieser Arbeit aufgrund der hohen Komplexität des Verfahren nicht untersucht und für einen Vergleich herangezogen werden. Jedoch ist dieses in der Praxis, besonders in dynamischen Systemen, ohnehin nicht möglich bzw. praktikabel. Der für die Kanalzuweisung benötigte Interferenzgraph wurden mit Hilfe des Maximum-Throughput-Verfahren (Abschnitt 3.1.1) ermittelt. Dabei wurde jedoch nur die Interferenz zwischen den APs ermittelt, weil die Clienten unverändert bleiben sollten. Da sie aus diesem Grund auch nicht Teil des Interferenzgraphen waren, wurden sie bei der Kanalzuweisung nicht berücksichtigt. Die Kanalzuweisung war also Client-agnostisch. In den einzelnen Simulationen wurden jeweils 10 APs verwendet. Die Feldgröße und die Anzahl der Clienten und der Kanäle wurden variiert, wobei letzteres auf 3 beschränkt war.

Tabelle 6.1: Simulationsparameter für die Evaluation der Kanalzuweisungsverfahren.

Parameter	Wert
`Bitrate`	6 Mbit/s (OFDM)
`UDP-Datenrate`	Maximale Datenrate, 0,9 Mbit/s
`Pfadverlustmodell`	Shadowing
`Dämpfungskoeffizient`	3,5
`Shadowing (Stdev)`	6 dB, 8 dB
`Koherenzzeit (Shadowing)`	0 ms
`Seitenlänge des quadratischen Feldes`	200 m, 300 m, 400 m
`#Access Points`	10
`#Clienten`	1, 2, 5, 10, 20, 30
`Min. Abstand der Clienten zum AP`	20 m
`Max. Abstand der Clienten zum AP`	120 m

Die 10 APs wurde auf 2 Arten in dem quadratischen Feld platziert. In einem Teil der Simulationen wurden ihre Positionen zufällig bestimmt. Des weiteren standen im Rahmen der Arbeit die Koordinaten von DSL-Anschlüssen zur Verfügen. Diese wurden ebenfalls für die Platzierung der APs verwendet. Die Positionen der Clienten wurden immer zufällig bestimmt, jedoch musste zu jedem AP ein Mindestabstand und zu mindestens einem auch ein Maximalabstand eingehalten werden. Letzteres stellt sicher, dass der Client die Möglichkeit hat zu mindestens einem AP eine Verbindung herzustellen. Der Mindestabstand wiederum findet sich auch in den meisten realen Szenarien wieder, bei welchem die APs z. B. meist etwas höher gelegen an Häuserwänden angebracht werden oder wie bei den Hotspot der Betreibers FON bei den Kunden in der Wohnung stehen. Der Mindestabstand wurde dabei so gewählt, dass bei dem verwendeten Pfadverlustmodell, die Paketfehlerrate unter 10 % liegt. Die Clienten wählen den AP, dessen Signalstärke am größten ist, und assoziieren sich mit diesem. In der Tabelle 6.1 sind alle wichtigen Parameter für die Simulation aufgelistet.

Ergebnisse

Die beiden Diagramme aus Abbildung 6.1 zeigen die Ergebnisse für den mittleren Durchsatz pro Client bei verschiedenen Feldgrößen und 5 (links) bzw. 20 Clienten (rechts), wobei jeder Client mit maximal möglicher Datenrate gesendet hat. Den Erwartungen entsprechend, steigt der mittlere Durchsatz mit der Anzahl der Kanäle, da durch die Verwendung von zusätzlichen Kanälen die Kapazität im Netzwerk

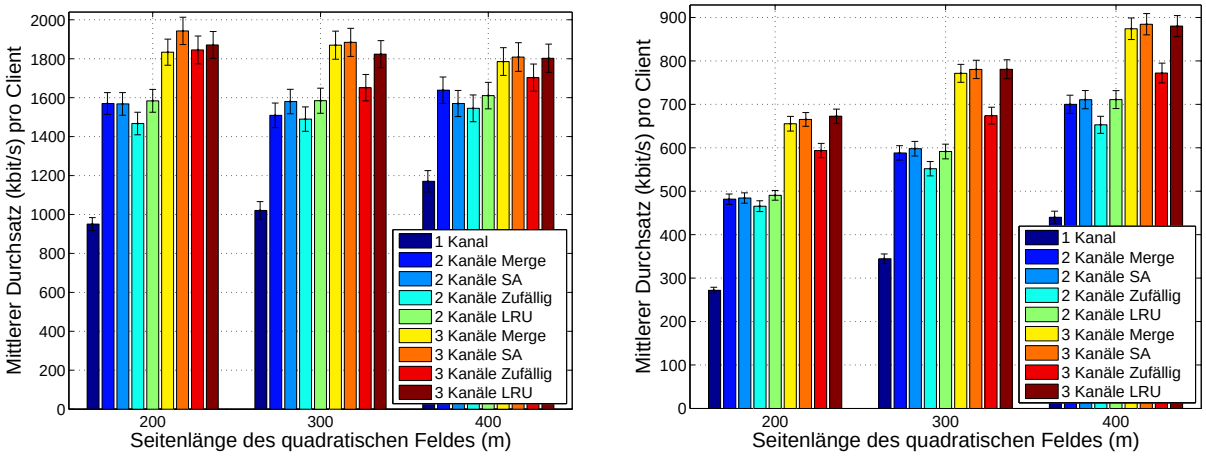

Abbildung 6.1: Mittlerer Durchsatz (± Standardfehler) bei verschiedenen Feldgrößen und Kanalzuweisungsverfahren. In der linken Abbildung wurden 5, in der rechten 20 Clienten im Feld platziert. Jeder Clienten sendete mit maximaler Datenrate.

gesteigert wird. Es zeigt jedoch auch, dass die Kanalzuweisung ebenfalls eine entscheidende Rolle spielt. Verfahren wie LRU verbessern den mittleren Durchsatz pro Client um 13 % gegenüber der zufälligen Kanalwahl. Vergleich man beide Abbildung, so wird deutlich, dass eine effiziente Kanalzuweisung um so entscheidender ist, je mehr Clienten im Netzwerk sind. Der Grund dafür ist die Interferenz die, mit wachsender Anzahl von Clienten zunimmt. Bessere Kanalzuweisungsverfahren wie LRU reduzieren diese und verringern somit Paketverluste durch Kollisionen. Des weiteren wird durch die geringere Interferenz die Parallelität im Netzwerk erhöht, d. h. es können mehr Übertragungen gleichzeitig gemacht werden, wodurch wiederum der Durchsatz erhöht wird.

Die mittleren Durchsätze pro Client unterscheiden sich bei den 3 verwendeten Heuristiken Merge, LRU und Simulated Annealing kaum. Der Unterschied beträgt weniger als 5 %.

In der rechten Abbildung erkennt man, dass der mittlere Durchsatz pro Client zunimmt, je größer das Feld ist. Die Ursache ist der größere mittlere Abstand zwischen den APs bzw. Clienten. Zwar resultiert eine größere Distanz zwischen Clienten und AP auch in einer geringeren Signalstärken (Pfadverlust), jedoch führt die größere mittlere Entfernung zwischen den Clienten auch dazu, dass diese sich gegenseitig weniger stören und somit auf dem selben Kanal gleichzeitig Daten übertragen können (Spatial Reuse).

Die Abbildung 6.2 zeigt die Ergebnisse einer weiteren Simulation, bei der die APs und Clienten wiederum zufällig auf dem Feld verteilt wurden. Die Clienten verwendeten jedoch eine feste Datenrate von 0,9 Mbit/s. Die Summe der Datenraten von fünf Clienten (rechtes Diagramm) beträgt 4,5 Mbit/s. Sie liegt damit unter der möglichen minimalen Bitrate von 802.11g (6 Mbit/s), welche verwendet wurde. Durch Paketfehler und den dadurch nötigen Neuübertragungen ist die Datenrate auf MAC-Schicht jedoch höher. Dies wird deutlich, wenn man den mittleren Durchsatz bei einem und 2 verwendeten Kanälen vergleicht. Er kann durch den zusätzlichen Kanal um bis zu 9 % gesteigert werden. Durch die Verwendung eines dritten Kanals kann in diesem Szenario der Durchsatz nicht weiter gesteigert werden. Bei 20 Clienten hingegen führt jeder zusätzliche Kanal zu einer Verbesserung des Durchsatzes. Auch hier zeigt sich der Unterschied zwischen zufälliger Kanalwahl und einem effizienten Verfahren deutlich. Der mittlere Durchsatz liegt bei Verwendung von LRU um bis zu 12 % höher. Der Unterschied zwischen den Heuristiken ist in diesem Szenario geringer als beim Senden mit der maximaler Datenrate. Er beträgt nur bis zu 3 %.

Die Ergebnisse zeigen, dass bei geringer Netzwerklast, d. h. wenig Clienten und geringen Datenraten,

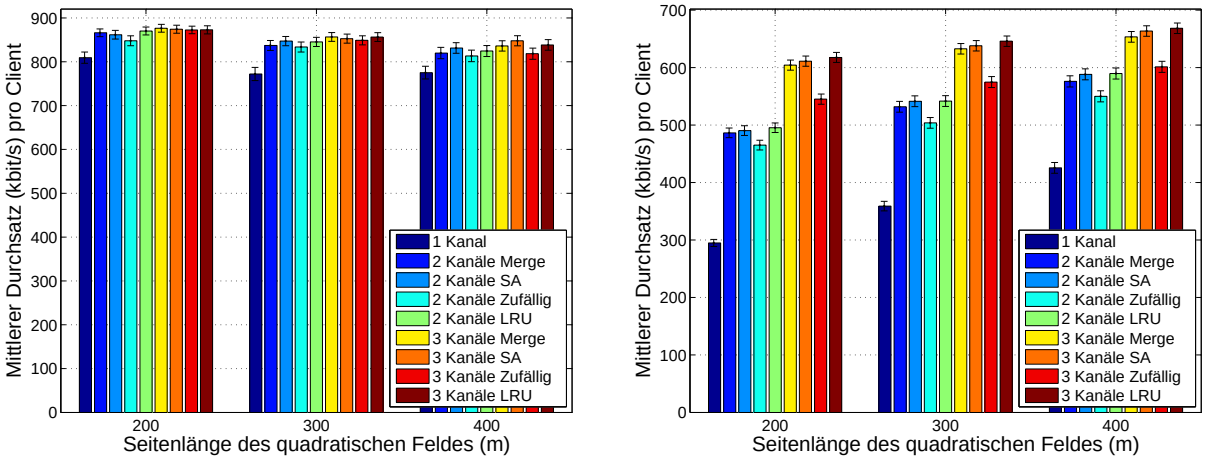

Abbildung 6.2: Mittlerer Durchsatz (± Standardfehler) bei verschiedenen Feldgrößen und Kanalzuweisungsverfahren. In der rechten Abbildung wurden 5, in der linken 20 Clienten im Feld platziert. Die Datenrate der Clienten wurde auf 0,9 Mbit/s begrenzt.

der Gewinn aus zusätzlichen Kanälen gering ist. Man benötigt also hohe Netzwerklast und insbesondere viele Clienten, um von mehreren Kanälen zu profitieren. Dann ist auch die Kanalzuweisung von entscheidender Bedeutung. Die Unterschiede zwischen den vorgestellten Heuristiken waren gering, vergleicht man den mittleren Durchsatz. Die Unterschiede liegen eher in der Komplexität. Das Verfahren LRU hat dabei neben der einfachen Implementierung den Vorteil, dass es verteilt realisierbar ist.

6.2 Verteilte Antennen

Verteilte Antennen können in drahtlosen Netzwerken durch Kooperation mehrerer Empfänger die Paketfehlerrate reduzieren und somit den Durchsatz erhöhen. Im Abschnitt 4 wurden mehrere Möglichkeiten für kooperatives Empfangen vorgestellt. Im Rahmen dieser Arbeit sollte ein Verfahren zum Einsatz kommen, bei welchem die Clienten nicht verändert werden müssen. Im Netzwerksimulator wurde das Cognitive Acknowledgement implementiert, welches im Abschnitt 4.2.2 vorgestellt wurde. Da beim IEEE 802.11 Protokoll jedes korrekt empfangene Paket vom Empfänger bestätigt werden muss, ist es auch bei einer verteilten Antenne nötigt, dass mindestens einer der Empfänger diese Bestätigung sendet. Die potentiellen Empfänger, die eine verteilte Antenne bilden, erhalten deshalb beim Cognitive Acknowledgement unterschiedliche Prioritäten, welche festlegt, wann sie eine Bestätigung nach dem Erhalt eines Paketes senden dürfen. Damit jedoch nur eine Bestätigung gesendet wird, darf ein AP diese nur dann senden, wenn sie kein anderer Empfänger mit einer höheren Priorität sendet. Die Erkennung einer Übertragung einer Bestätigung durch einen Empfänger mit höherer Priorität ist also ein wichtiger Bestandteil des Protokolls. Die Erkennung wird von der gemessenen Signalstärke abhängig gemacht. Liegt diese über einem Schwellwert, so wird angenommen, dass ein Empfänger mit höherer Priorität die Bestätigung sendet. Im Rahmen der Arbeit wurden dabei zunächst 3 verschiedene Optionen zur Erkennung verglichen, welche sich in der Höhe und in der Bestimmung des Schwellwertes unterscheiden.

In weiteren Simulationen wurden die verteilten Antennen in verschiedenen Szenarien evaluiert. Dabei wurde neben dem erreichten Durchsatz auch die Dauer der einzelnen Übertragungen (Latenz) gemessen. Bei allen Szenarien wurde nur ein Kanal verwendet, um einen Einfluss durch die Kanalzuweisung

auszuschließen.

Protokoll für verteilte Antennen

Die Abbildung 6.3 zeigt den Aufbau der Simulation mit einem Clienten und zwei APs. Die Abstände d_1, d_2 und d_3 wurden dabei variiert. Die Entfernung d_3 zwischen den APs ist dabei ausschlaggebend für das korrekte Funktionieren des Cognitive Acknowledgement, da zu große Entfernungen dazu führen, dass das Senden der Bestätigung eines APs nicht von dem anderen erkannt werden kann. Das Resultat wäre, dass mehrere Bestätigungen gleichzeitig gesendet werden und es somit zu Kollisionen beim Empfänger kommen könnte. Der Abstände d_1 und d_2 zwischen dem Clienten und den beiden APs haben Einfluss auf die Signalstärke der gesendeten Pakete (Pfadverlust) und somit auf die Paketfehlerrate. Bei größeren Abständen steigt die Paketfehlerrate.

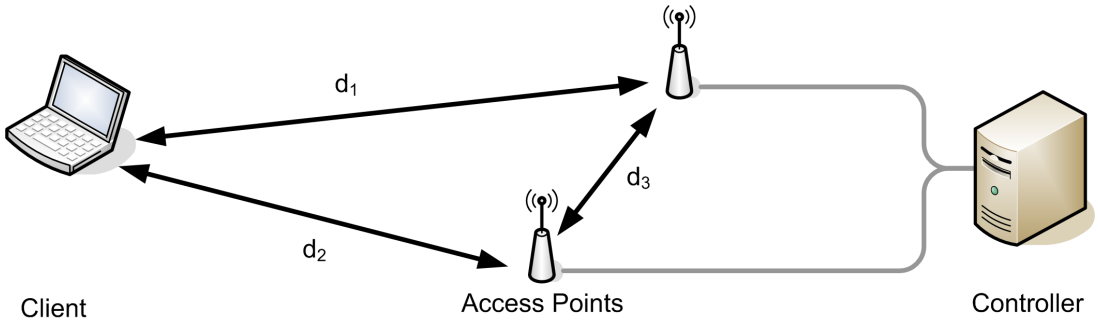

Abbildung 6.3: Der Abstand zwischen dem Clienten und den APs wurde variiert, um so den Einfluss auf das Protokoll zu evaluieren. Es wurde dabei der Durchsatzgewinn bei Verwendung von verteilten Antennen ermittelt.

Das Cognitive Acknowledgement für verteilte Antennen basiert darauf, dass die APs erkennen, ob ein höher priorisierter AP eine Bestätigung sendet. Dafür wurden drei Ansätze implementiert (Abschnitt 5.5) und in einer ersten Simulation verglichen:

- `Frei`: Eine Bestätigung wird gesendet, wenn das Medium nicht belegt ist.
- `Wahrnehmen`: Der Rauschpegel muss unterhalb eines festgelegten Wertes liegen, damit eine Bestätigung gesendet wird.
- `Nichts Empfangen`: Wenn das Radio keine Daten empfängt, wird eine Bestätigung gesendet.

Für jede Platzierung wurde ein Paketfluss mit maximaler Datenrate vom Clienten zu den APs aufgesetzt. Der Client war dabei mit dem AP assoziiert, deren Signalstärke am höchste war. Jede Messung wurde dabei mit und ohne Einsatz von verteilten Antennen durchgeführt, wobei für den letzteren Fall alle Verfahren zur Erkennung der Bestätigung einzeln zum Einsatz kamen. Die Größe der verteilten Antenne wurde auf 2 APs festgelegt, d. h. es wurde vorher nicht überprüft, ob ein Gewinn durch den Einsatz des zweiten Empfängers zu erwarten ist und ob die Erkennung der Bestätigung bei dem jeweiligen Abstand funktionieren kann. So konnten die Auswirkung von Fehlentscheidungen erfasst und gleichzeitig ermittelt werden, welches der drei Verfahren am zuverlässigsten funktioniert und somit in den meisten Szenarien verwendet werden kann. Die Tabelle 6.2 zeigt die wichtigsten Parameter und ihre Werte, die im Simulator verwendet wurden.

Tabelle 6.2: Simulationsparameter für die Evaluation des Protokolls für das Cognitive Acknowledgement.

Parameter	Wert
`Bitrate`	6 Mbit/s
`UDP-Datenrate`	Maximale Datenrate
`Pfadmodell`	Shadowing
`Dämpfungskoeffizient`	3,5
`Shadowing (Standardabweichung)`	8 dB
`Koherenzzeit (Shadowing)`	0 ms
`Abstand zwischen den APs (`d_3`)`	40 m - 140 m
`Abstand zwischen dem Clienten und den APs (`d_1`,`d_2`)`	25 m - 175 m

Ergebnisse

Das Diagramm 6.4 zeigt für die 3 MAC-Optionen wie oft beide APs gleichzeitig gesendet haben, d.h das Senden der Bestätigung nicht erkannt wurde und es zu Kollisionen beim Sender kommt. Der Abstand zwischen den APs und dem Clienten (d_1,d_2) betrug dabei 100 m und zwischen den APs wurde er zwischen 100 m und 140 m variiert. Das Verfahren, welches bei Empfang von Daten keine Bestätigung sendet ("Nicht Empfangen"), erkennt ab einem Abstand von 120 m zwischen den APs nicht mehr alle Bestätigungen des höher priorisierten APs. Bei 140 m nimmt dies noch einmal deutlich zu und es kommt vermehrt zu Kollisionen.

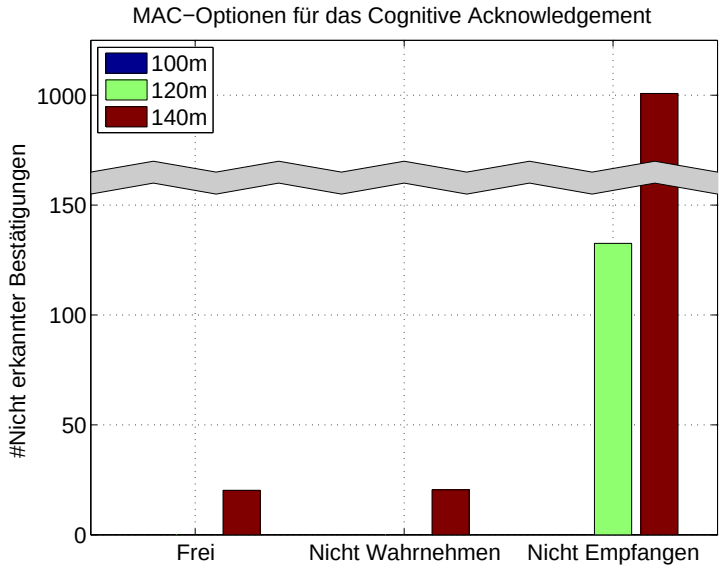

Abbildung 6.4: Dieser Vergleich der verschiedene MAC-Optionen für das verteilte Bestätigung zeigt die Anzahl der nicht erkannten Bestätigungen bei verschiedenen Abständen zwischen den APs.

Die beiden anderen MAC-Optionen unterscheiden sich hier kaum. Erst bei einem Abstand von 140 m erkennt der zweite AP nicht alle der gesendeten Bestätigungen des anderen APs und sendet fälschlicherweise eine Bestätigung, wodurch es zu Kollisionen beim Empfänger kommt.

Auf Grundlage dieser Ergebnisse konnte nun durch weitere Simulationen, bei welchen der Abstand

zwischen den APs in kleineren Schritten variiert wurde, ermittelt werden, wie mit Hilfe des Interferenzgraphen abgeschätzt werden kann, ob bei zwei gegebenen APs des Netzwerkes das Cognitive Acknowledgement funktioniert, d. h. ob das Senden einer Bestätigung des ersten APs durch den zweiten AP erkannt werden kann. Die Idee dabei ist, dass das Messen der Interferenz ebenfalls darauf basiert eine andere, dabei jedoch störende Übertragung zu erkennen. Ein AP kann bei Störung durch einen anderen AP nicht mehr so häufig auf das Medium zugreifen, d. h. seine maximale Datenrate wird reduziert und dies spiegelt sich in einem hohen Wert im Interferenzgraphen wieder (siehe Abschnitt 3.1.1).

Bei den einzelnen Simulationen wurde für die verschiedenen Abständen die Stärke der Interferenz zwischen den APs (Interferenzgraph) und die Anteil nicht erkannter Bestätigungen ermittelt. Es zeigte sich, dass ein Wert für die Interferenz größer als 0,85 im Interferenzgraph ausreicht, um das Funktionieren der beiden Verfahren "Frei" und "Nicht Wahrnehmen" sicherzustellen.

Im nächsten Abschnitt wird durch weitere Simulationen anderer Szenarien evaluiert, welches der beiden MAC-Optionen "Frei" und "Nicht Wahrnehmen" robuster gegenüber parallelen Übertragungen ist. Erst dadurch kann das zuverlässigste der 3 Verfahren bestimmt werden.

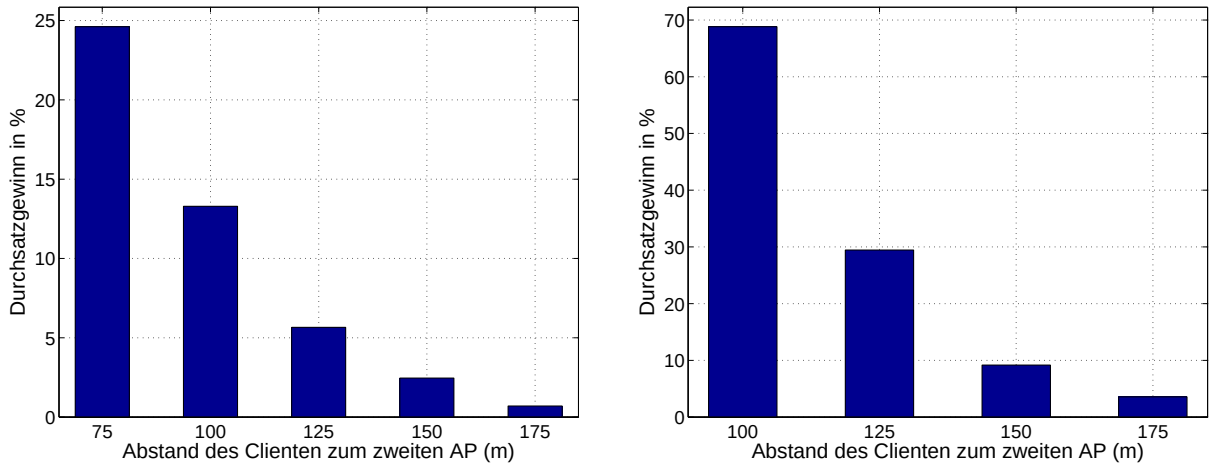

Abbildung 6.5: Mittlerer Durchsatzgewinn einer verteilten Antennen gegenüber eines einzelnen APs. AP 1 hat 75 m (links) bzw. 100 m (rechts) Abstand zum Clienten und der Abstand zwischen den APs beträgt 150 m.

Die Abbildung 6.5 zeigt Durchsatzsatzgewinn einer Datenübertragung vom Clienten zum AP beim Einsatz einer verteilten Antenne mit zwei APs. Für das Congnitive Acknowledgement wurde dabei die MAC-Optionen "Nicht Wahrnehmen" benutzt. Der dichtere und auch höher priorisierte AP der verteilten Antenne hat einen Abstand von 75 m (links) bzw. 100 m (rechts). Der erzielte Durchsatz ohne einen zweiten Empfänger wurde als Vergleich herangezogen, wobei sich der Client dabei mit dem dichteren AP assoziiert hat.

Der Abstand des zweiten APs wurde dabei zwischen dem des ersten AP und 175 m variiert. Die verteilte Antenne führte gegenüber einem einzelnen AP zu deutlich mehr Durchsatz (bis zu 68 %). Bei kleineren Abständen des höher priorisierten APs war dieser Vorteil geringer, da hier die Paketfehlerrate zu diesem einzelnen AP bereits gering ist. Für ein großes Netzwerk bedeutet dies, dass mit höherer Dichte des Netzes und damit auch geringerem Abstand zwischen den Clienten und den APs der Gewinn durch die verteilte Antennen sinkt. Zusammenfassend kann man sagen, dass besonders schlechte Links von verteilten Antennen profitieren. Ein Vergleich zwischen den beiden Abbildungen macht dies deutlich.

6.2.1 Einfluss von Interferenz

In dem Szenario aus dem vorherigen Abschnitt war die Ursache für Paketverlust eine geringe Signalstärke infolge größerer Abstände zwischen dem Clienten und den APs. Da auch Interferenz einen starken Einfluss auf die Paketfehlerrate hat, wurden in der folgenden Simulation die Anzahl der Clienten erhöht. Der Aufbau entspricht dabei einem Straßenszenario, bei welchem auf einer Seite die APs in gleichmäßigem Abstand angeordnet und die Clienten auf der anderen Seite zufällig platziert wurden (siehe Abbildung 6.6). Dies bildet stark vereinfacht eine Straße nach, wobei die APs in den Häusern platziert werden, während sich die Clienten auf der Straße befinden. Die Länge der Straße und somit der Abstand zwischen den APs wurde bei den einzelnen Simulationen ebenso variiert wie auch der Abstand der Clienten zu den APs. Diese und weitere Parameter der Simulation sind in der Tabelle 6.3 zusammengefasst.

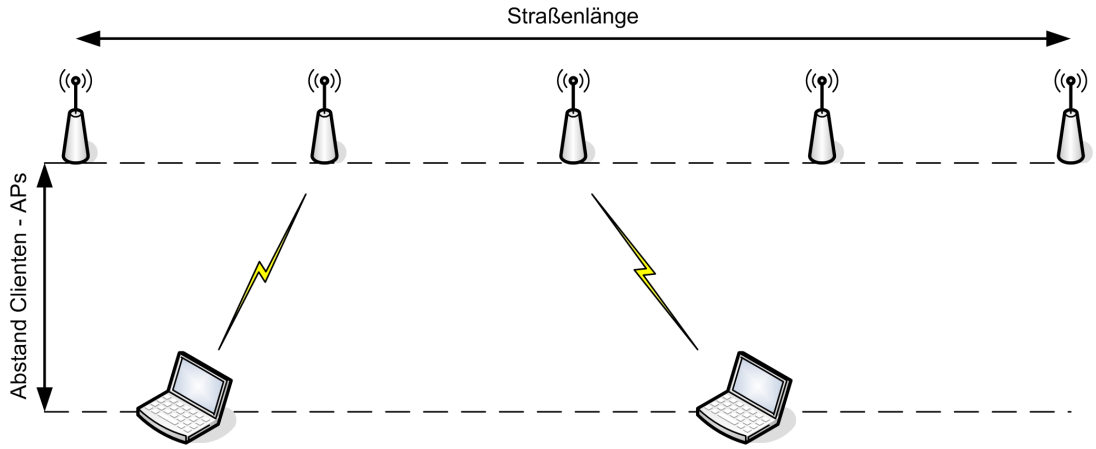

Abbildung 6.6: Straßenszenario: Gleichmäßig verteilte APs und zufällig platzierte Clienten. Der Abstand zwischen den APs sowie den Clienten und den APs wurde variiert.

Tabelle 6.3: Simulationsparameter für Simulation des Straßenszenarios.

Parameter	Wert
`Shadowing (Standardabweichung)`	8 dB
`#Access Points`	5
`#Clienten`	1, 2, 5, 10, 20
`Straßenlänge`	150 m - 750 m
`Abstand zw. Clienten & APs`	50 m - 160 m

Ein weiteres Ziel dieser Simulation ist der Vergleich zwischen den beiden MAC-Optionen “Frei” und “Nicht Wahrnehmen” des Congnitive Acknowledgements für die Erkennung der Bestätigung innerhalb einer verteilten Antenne. Besonders bei großen Netzen kommt es zu vielen parallelen Übertragungen auf dem selben Kanal. Das Erkennen der Bestätigung muss auch in solchen Situationen funktionieren, was jedoch auch bedeutet, dass parallele Übertragungen nicht als Bestätigung erkannt werden dürfen.

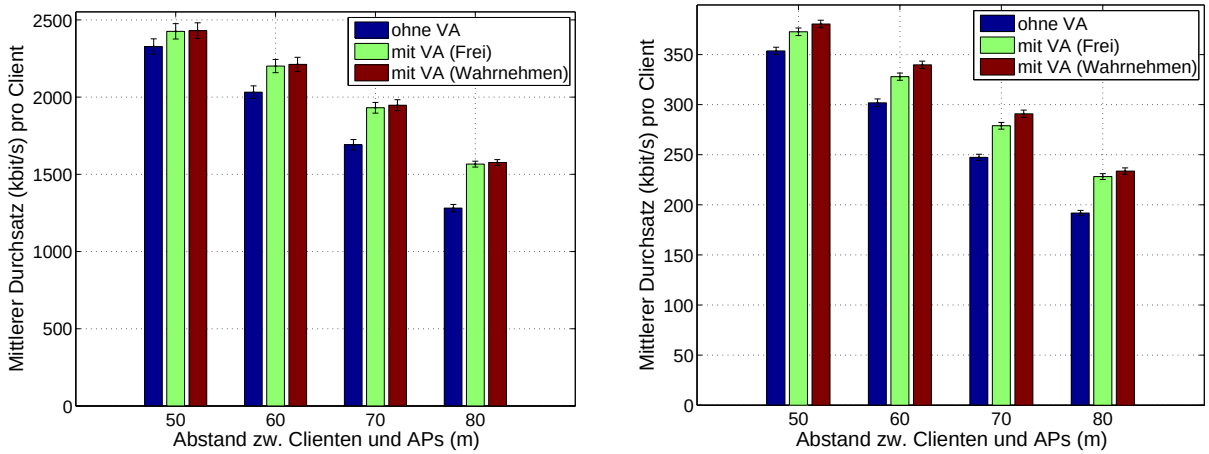

Abbildung 6.7: Mittlerer Durchsatz mit und ohne verteilten Antennen bei 250 m Straßenlänge und 2 (links) bzw. 20 Clienten (rechts).

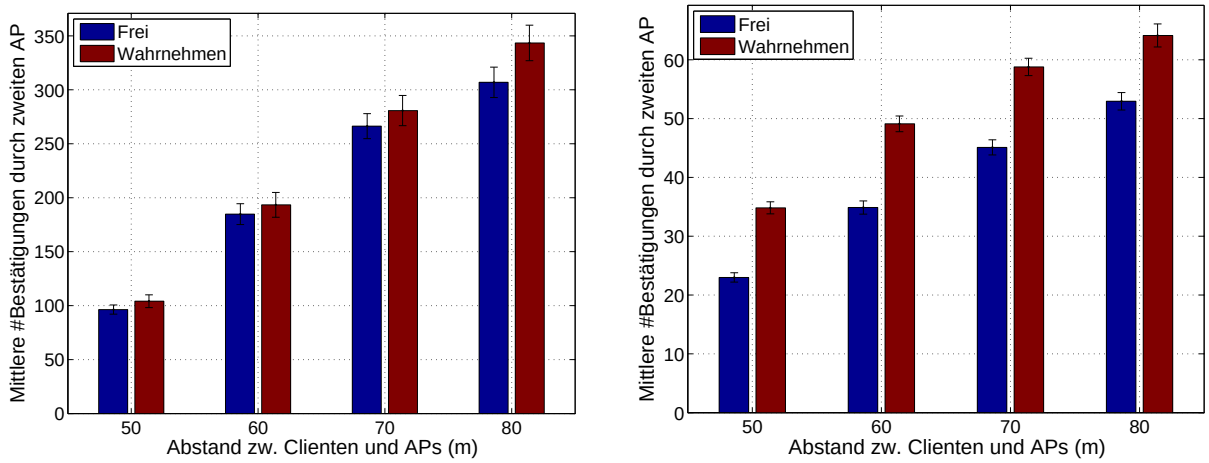

Abbildung 6.8: Mittlere Anzahl der durch den zweiten AP bestätigten Pakete pro Paketfluss bei jeweils zwei Clienten (links) bzw. 20 Clienten (rechts) und verschiedenen Abständen zwischen ihnen und den APs.

In der Abbildung 6.7 erkennt man, dass auch in diesen Simulationen der mittlere Durchsatz durch die verteilten Antennen erhöht werden konnte. Es zeigt sich aber besonders bei vielen Clienten ein Unterschied zwischen den beiden MAC-Verfahren für die Kooperation der APs innerhalb der verteilten Antennen. Der mittlere Durchsatz bei Einsatz der MAC-Option "Frei" liegt um bis zu 3,5 % unter jenem, der mit der MAC-Option "Nicht Wahrnehmen" erreicht wird.

Die Ursache ist in Abbildung 6.8 zu erkennen. Diese zeigt die mittlere Anzahl von Bestätigungen, die durch die APs gesendet wurden, welche innerhalb einer verteilten Antenne eine niedrigere Priorität besitzen. Es zeigt sich, dass bei dem Verfahren "Frei" ein AP mit niedriger Priorität seltener eine Bestätigung

sendet. Wenn das Medium belegt ist, d. h. die Signalstärke überschreitet einen festgelegten Grenzwert, wird bei diesem Verfahren angenommen, dass es sich dabei um die Übertragung einer Bestätigung durch einen höher priorisierten AP handelt.

Jedoch erkennt das Verfahren auch parallele Übertragungen anderer Clienten und APs als Bestätigung eines höher priorisierten APs. Das Verfahren "Nicht Wahrnehmen" hingegen bestimmt den Grenzwert für die Signalstärke, der für die Erkennung der Bestätigung herangezogen wird dynamisch. Direkt nachdem Empfang des Paketes vom Clienten wird der Rauschpegel gemessen. Aus diesem ergibt sich der Grenzwert für die Erkennung (siehe Abschnitt 5.5). Eine parallele Übertragung wird dadurch deshalb direkt nach Empfang des Datenpaketes erkannt und berücksichtigt.

Die niedriger priorisierten APs senden bei dem MAC-Verfahren "Nicht Wahrnehmen" viel häufiger eine Bestätigung und können somit Neuübertragungen verhindern. Das Verfahren 'Frei" hingegen erkennt häufig parallele Übertragung als eine Bestätigung und verhindert somit einen möglichen Gewinn durch die zusätzlichen Empfänger der verteilten Antenne.

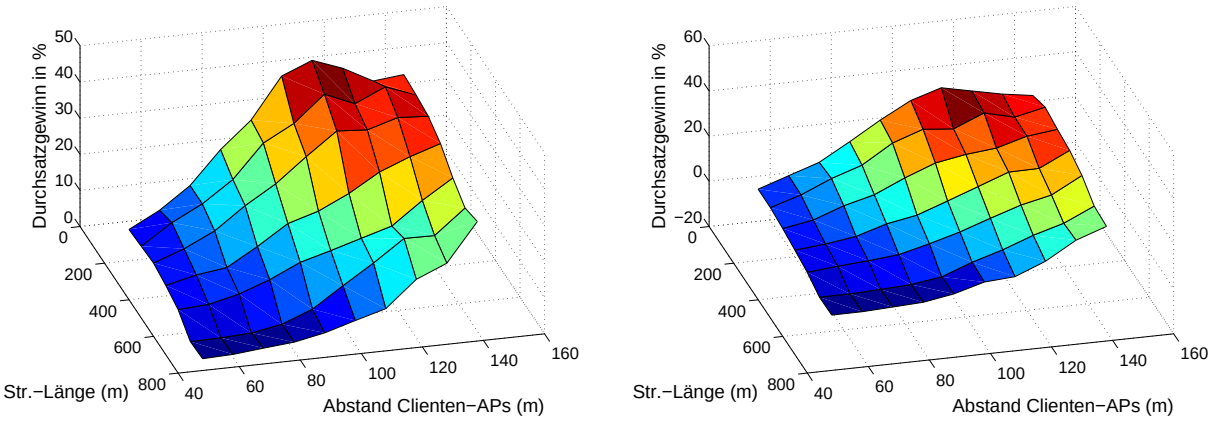

Abbildung 6.9: Die Abbildung zeigt den prozentualen Gewinn durch verteilte Antennen im Straßenszenario mit je 5 APs und 5 Clienten (links) bzw. 10 Clienten (rechts). Für die Erkennung einer Bestätigung innerhalb der verteilten Antenne wurde die MAC-Option "Wahrnehmen" verwendet.

Die Abbildung 6.9 zeigt den mittleren Durchsatzgewinn durch verteilte Antennen im vorgestellten Szenario in Abhängigkeit vom Abstand der Clienten zu den APs und der Länge der Straße, von welcher wiederum die Abstände zwischen den APs abhängig sind. Der Vorteil durch verteilte Antennen ist besonders bei kleineren Abständen zwischen den APs (kurze Straßenlänge) und größerer Entfernung der Clienten deutlich zu sehen. Er liegt bei bis zu 39 %. Dies war zu erwarten, da durch einen geringen Abstand zwischen den APs sicher gestellt ist, dass das Cognitive Acknowledgement zuverlässig funktioniert. Durch einen größeren Abstand zwischen den Clienten und den APs ist die Signalstärke geringer und es kommt zu höheren Paketfehlerraten. In diesen Fällen kann von zusätzlichen Empfängern der verteilten Antenne profitiert und der Durchsatz gesteigert werden. Mit wachsendem Abstand zwischen den APs geht der Gewinn durch die verteilten Antennen zurück. Dies hat zwei Gründe. Zum einen funktioniert das Congnitive Acknowledgement nicht mehr zuverlässig, wodurch mehrere APs einer verteilten Antenne die Bestätigung für ein Datenpaket senden und dadurch Kollisionen verursachen. Des weiteren führt ein größerer Abstand zwischen den APs dazu, dass sich die Abstände der APs einer verteilten Antenne und dem Clienten häufig stark unterscheiden bzw. asymmetrisch sind, d. h. dass der Abstand zum zweiten AP der verteilten Antenne deutlich größer ist als zum ersten. Somit unterscheiden sich auch die Paketfehlerraten der einzelnen APs deutlicher. Die zusätzlichen APs in der verteilten Antenne können in solchen

Fällen die Paketfehlerrate gegenüber dem einzelnen AP nur geringfügig senken.

6.2.2 Zufällige Netzwerke

In weiteren Simulationen wurden die APs und die Clienten in einem quadratischen Feld mit unterschiedlichen Seitenlängen zufällig platziert. Die Clienten hatten wie bei der Evaluation der Kanalzuweisung (Abschnitt 6.1) einen Mindestabstand zu allen und einen Maximalabstand zu mindestens einem AP. Die Anzahl der Clienten und die Datenrate wurden variiert, um verschiedene Netzwerklasten zu erzeugen. Die maximale Größe der verteilten Antenne wurde bei den Simulationen ebenfalls variiert. Eine verteilte Antenne der Größe eins beinhaltet nur den AP mit dem sich der Client assoziiert hat, wobei die Clienten dabei den AP mit der höchsten Signalstärke wählten.

Bei größeren VAs fügte der Controller entsprechend weitere APs hinzu, wenn dadurch eine Reduzierung der Paketfehlerrate zu erwarten war. Die Tabelle 6.2 fasst weitere wichtigen Parameter zusammen.

Tabelle 6.4: Parameter für die Simulation mit zufälliger Platzierung.

Parameter	Wert
`#Access Points`	10
`#Clienten`	1, 2, 5, 10, 20, 30
`UDP-Datenrate`	0,5 - 1,5 Mbit/s und max. Datenrate
`Seitenlänge des Feldes`	200, 300, 400
`Min. Abstand der Clienten zum AP`	20 m
`Max. Abstand der Clienten zum AP`	120 m
`Shadowing (Stdev)`	8 dB
`#APs in einer verteilten Antenne`	1, 2, 3

Die Abbildung 6.10 zeigt die mittleren Durchsätze der Clienten bei verschiedenen Feldgrößen. Durch verteilte Antennen, welche in diesen Simulationen aus maximal 2 APs bestehen, kann dieser um bis zu 9 % gesteigert werden. Vergleich man diese Ergebnisse mit jene aus den ersten beiden Szenarien (siehe Abschnitt 6.2 und 6.2.1), so ist der Gewinn deutlich geringer. Der Grund ist der große Unterschied zwischen den Abständen vom Clienten zu den APs. Schon der zweite AP innerhalb der VA hat eine deutlich höhere Paketfehlerrate als der erste AP, mit welchem sich der Client assoziiert hat. Deshalb kann durch ihn die Paketfehlerrate nur wenig reduziert werden. Besonders bei größeren Feldern waren die Abstände zwischen den APs so groß, dass das Cognitive Acknowledgement nicht zuverlässig funktioniert hätte. Dies wurde durch den Controller anhand des Interferenzgraphen erkannt und so wurde die Bildung verteilter Antennen mit 2 APs nicht immer vorgenommen.

Die Abbildung 6.11 zeigt den kumulierten Anteil der Flüsse und den entsprechenden Durchsatz. Das linke Diagramm zeigt die Ergebnisse der Simulationen, bei welchen die Clienten mit maximaler Datenrate gesendet haben, das rechte jene, bei welchen mit konstanter Rate von 0,9 Mbit/s gesendet wurde. Es zeigt sich, dass besonders schlechte Links von verteilten Antennen profitieren. So ist in den rechten Diagramm zu erkennen, dass einem einzelnen AP pro Client 50 % der Flüsse einen Durchsatz von über 500 kbit/s haben, während es bei Verwendung von verteilten Antennen über 60 % sind.

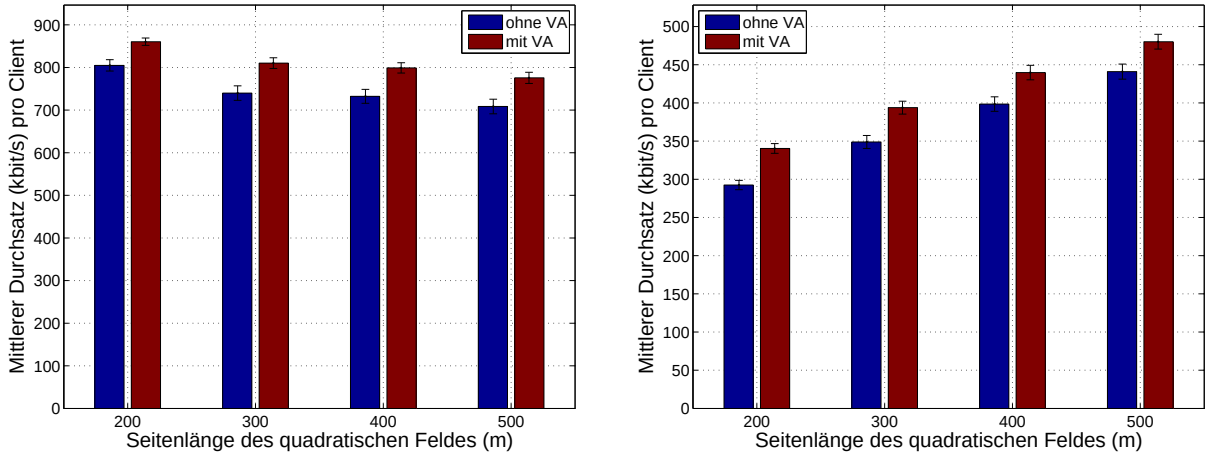

Abbildung 6.10: Mittlerer erreichter Durchsatz bei 5 (rechts) und 20 Clienten (links). Es wurde mit einer konstanten Datenrate von 0,9 MBit/s gesendet. Die verteilten Antennen umfassten maximal 2 APs.

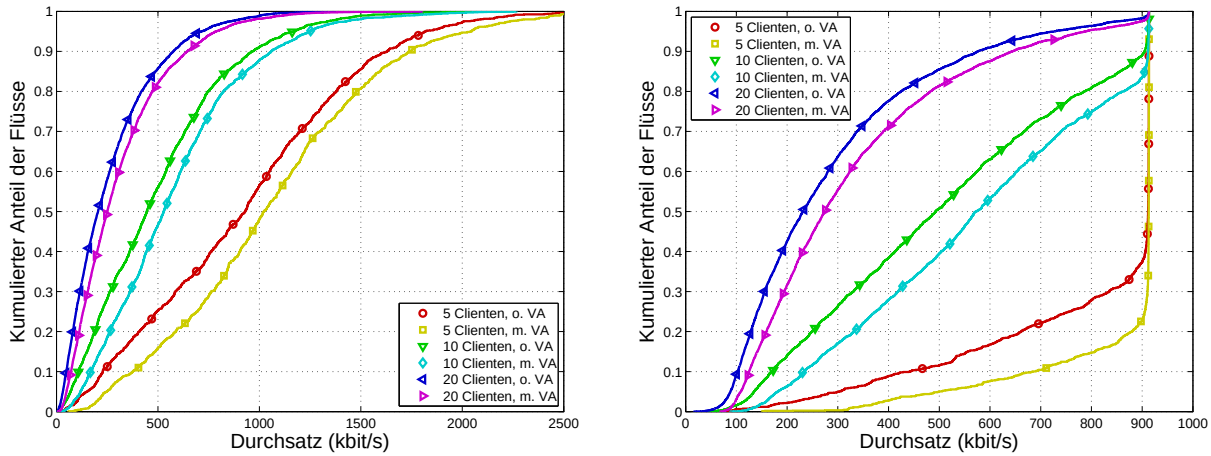

Abbildung 6.11: Kumulierter Anteil der Flüsse und der Durchsatz. Es wurde dabei die maximale (links) und eine konstante Datenrate von 0,9 Mbit/s (recht) verwendet. Das quadratische Feld hatte eine Seitenlänge von 200 m.

Aufgrund der reduzierten Paketfehlerrate durch den Einsatz von VAs wird die Anzahl der Neuübertragungen und somit die Dauer einer erfolgreichen Paketübertragung gesenkt, wie es die Abbildung 6.12 zeigt. So kann in den Szenarien mit 5 Clienten im Netzwerk der Anteil der Übertragungen, welche weniger als 10 ms auf der MAC-Schicht benötigen (MAC-Latenz) durch die verteilten Antennen von 61 % auf 81 % gesteigert werden. Besonders bei vielen Clienten im Netzwerk ist das entscheidend, da der einzelne Client durch die vermehrte Konkurrenz seltener Zugriff auf das Medium erhält und die Dauer bis zur Neuübertragung bei vielen Clienten ansteigt. Besonders Anwendungen wie VoIP, die kurze Latenzen benötigen, können deshalb von verteilten Antennen profitieren.

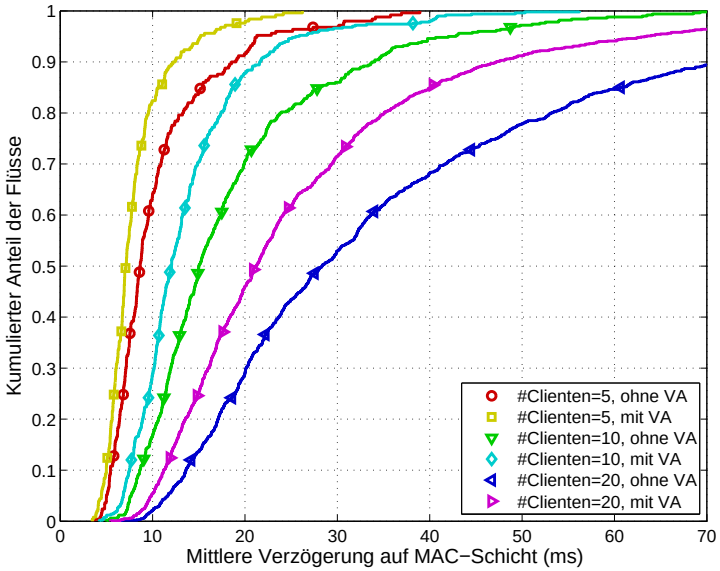

Abbildung 6.12: Kumulierte Übertragungsverzögerung auf MAC-Schicht ohne und mit verteilten Antennen. Die Größe der VA war auf maximal 2 APs beschränkt. Das quadratische Feld hatte eine Seitenlänge von 200 m.

6.3 Kanalzuweisung und verteilte Antennen

In den beiden vorherigen Abschnitten wurden Kanalzuweisung und verteilte Antennen isoliert untersucht. Es wurde dabei gezeigt, dass durch beide Verfahren der Durchsatz im Netzwerk erhöht werden kann. In diesem Abschnitt werden beide durch den in Abschnitt 5.8 dargelegten Algorithmus kombiniert. Es wird dabei zunächst die Kanalzuweisung vorgenommen und dann werden die verteilte Antennen für die Clienten gebildet. Unbenutzten APs werden danach andere Kanäle zugewiesen, wenn sie dadurch in anderen verteilten Antennen die Paketfehlerrate weiter reduzieren können.

Tabelle 6.5: Parameter für die Evaluation der Kombination von Kanalzuweisung und verteilten Antennen.

Parameter	Wert
`#Access Points`	10
`#Clienten`	1, 2, 5, 10, 20, 30
`UDP-Datenrate`	0,5 - 1,5 Mbit/s und max. Datenrate
`Seitenlänge des Feldes (m)`	200, 300, 400
`Min. Abstand der Clienten zum AP`	20 m
`Max. Abstand der Clienten zum AP`	120 m
`Shadowing (Stdev)`	8 dB
`#APs in einer verteilten Antenne`	1, 2
`#Kanäle`	1, 2, 3

Es werden in diesen Simulationen maximal 3 Kanäle im gesamten Netzwerk und maximal 2 APs in einer verteilten Antenne verwendet. Die APs und Clienten wurden zunächst zufällig auf einem quadratischen Feld mit verschiedenen Seitenlängen verteilt. Im Anschluss wurden die APs auch anhand realer

Positionen (DSL-Anschlüsse) platziert. Die Clienten wurden wiederum zufällig platziert. In beiden Fällen, zufällige und reale Platzierung, haben die Clienten wiederum zu allen APs einen Mindestabstand und zu mindestens einem AP einen Maximalabstand. Diese beiden Abstände und weitere wichtige Werte sind in der Tabelle 6.5 zusammengefasst.

Ergebnisse

Die Abbildung 6.13 zeigt Ergebnisse der Simulationen bei welchen 20 Clienten mit einer konstanten Datenrate von 1,4 Mbit/s sendeten. Es wird deutlich, dass durch die Verwendung von mehreren Kanälen der Durchsatz deutlich mehr gesteigert werden kann als durch den Einsatz von verteilten Antennen. Bei einem Kanal und ohne verteilte Antennen haben 11 % der Clienten einen höheren Durchsatz als 400 kbit/s, mit verteilten Antennen sind es 16 %. Durch einen zusätzlichen Kanal haben 34 % der Clienten einen höheren Durchsatz als 400 kbit/s. Auch bei 2 Kanälen kann dieser Anteil durch die verteilten Antennen noch auf 39 % gesteigert werden. Bei 3 verwendeten Kanälen liegt der Anteil bei 50 %, wobei hier die verteilten Antennen keinen weiteren Gewinn bringen.

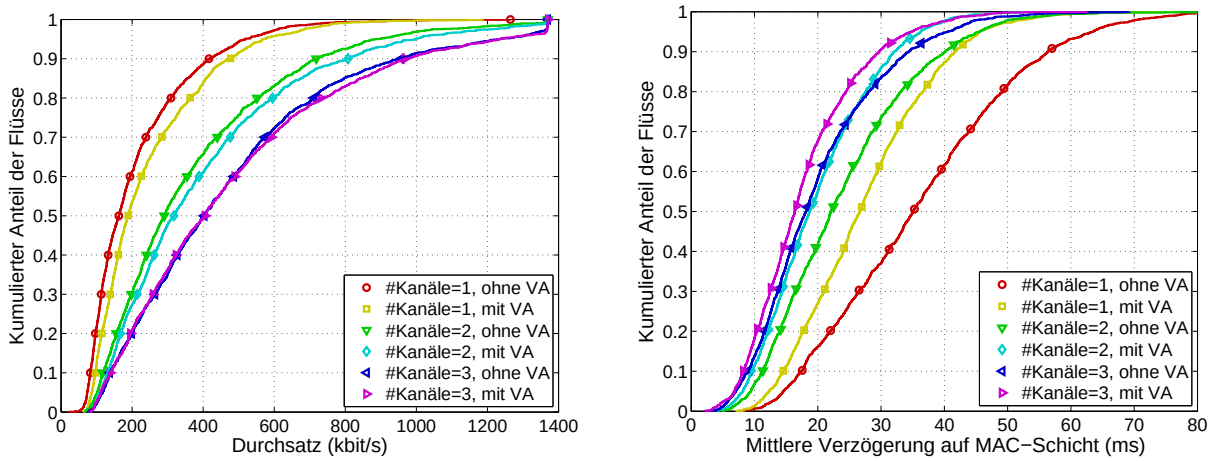

Abbildung 6.13: Die Abbildung zeigt den erreichten Durchsatz (rechts) und die Verzögerung der Übertragung auf MAC-Schicht. Die 30 Clienten und 10 APs wurden zufällig in einem quadratischen Feld mit einer Seitenlänge von 200 m platziert und sendeten mit einer konstanten Datenrate von 1,4 Mbit/s.

Das rechte Diagramm der Abbildung 6.13 zeigt die mittlere Verzögerung der Pakete auf der MAC-Schicht. Sowohl die verteilten Antennen als auch die Verwendung mehrere Kanäle reduzieren die Verzögerung. Dies jedoch aus unterschiedlichen Gründen. Eine höhere Anzahl von Kanälen führt dazu, dass jeder einzelne Netzwerkteilnehmer häufiger auf das Medium zugreifen kann, da so pro Kanal weniger Knoten um das Medium konkurrieren. Des weiteren wird die Interferenz reduziert, d. h. es gibt weniger Störungen zwischen den Clienten und somit weniger Paketfehler infolge von Kollisionen. Die verteilten Antennen reduzieren die Paketfehlerrate durch Einsatz mehrerer Empfänger. Es wird deutlich, dass der Einsatz mehrere Kanäle in diesem Szenario jedoch deutlich mehr Einfluss auf die Verzögerung hat. Während z. B. die Verwendung von 2 Kanälen statt einem dazu führt, dass 50 % der Übertragungen anstelle von 35 ms weniger als 22 ms benötigen, kann dies durch die verteilten Antennen nur auf 27 ms reduziert werden. Beide Diagramme zeigen also, dass es in einem solchen Szenario und bei solchen Netzwerklasten keinen Sinn macht, die Anzahl der verwendeten Kanäle zugunsten besserer verteilter Antennen zu reduzieren.

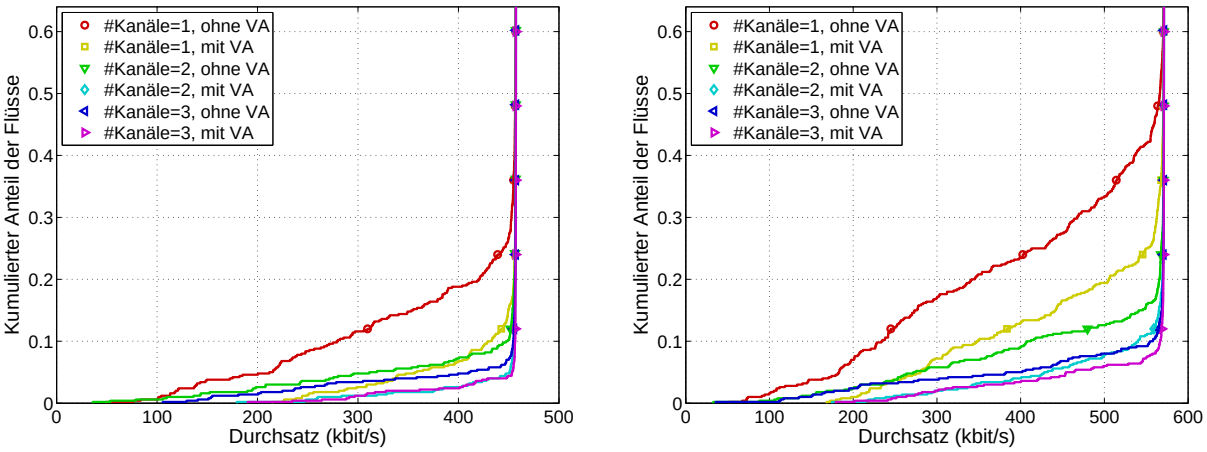

Abbildung 6.14: Die 10 zufällig platzierten Clienten sendeten mit einer Datenrate von 450 kbit/s (links) bzw. 570 kbit/s (rechts). Die Seitenlänge des quadratischen Feldes beträgt 300 m.

Die Abbildung 6.14 zeigt Ergebnisse von Simulationen mit 10 Clienten. Die Datenraten waren dabei konstant und betrugen 450 kbit/s (links) und 570 kbit/s (rechts), deshalb war die Netzwerklast hier deutlich geringer als im vorherigen Szenario. Es zeigt sich auch hier, dass die verteilten Antennen den Durchsatz erhöhen, jedoch nicht in einem solchen Umfang wie die Verwendung zusätzlicher Kanäle. Im linken Diagramm der Abbildung 6.14 ist zu erkennen, dass durch die Verwendung von verteilten Antennen die Ergebnisse für 2 und 3 verwendete Kanäle ähnlich sind. Daran wird deutlich, dass es auch hier keinen Sinn macht, weniger Kanäle zugunsten möglicher verteilter Antennen zu nutzen. Bei nur geringfügig höherer Datenrate (rechts) ist der Vorteil durch einen zusätzlichen Kanal (3 statt 2) größer als durch potentiell bessere VAs. Vergleicht man die Simulationen mit 3 Kanälen und ohne VAs mit jenen mit 2 Kanäle und VAs, so fällt auf, dass besonders schwache Links von verteilten Antennen profitieren. Der Anteil der Flüsse mit einem Durchsatz von mehr als 300 kbit/s ist bei weniger als 2 Kanälen und VAs größer als bei 3 Kanälen und ohne VAs (98 % statt 96 %). Betrachten man den jeweiligen Anteil der Flüsse mit einem Durchsatz von mehr als 540 kbit/s ist dies umgekehrt. Hier liegt der Anteil bei 3 Kanälen und ohne VA mit 91 % höher als bei 2 Kanäle und der Verwendung von VAs (98 %).

In weiteren Simulationen wurden die APs anhand der Positionen von DSL-Anschlüssen platziert (Abschnitt 5.9.1). Die Abbildungen 6.15 und 6.16 zeigen die Durchsätze bei verschiedenen Netzlasten. Es wurden sowohl 20 (rechts) als auch 10 Clienten (links) platziert. Die Clienten sendeten jeweils mit einer Datenrate von 450 kbit/s (Abbildung 6.15) und 900 kbit/s (Abbildung 6.16).

Es wird deutlich, dass bei niedriger Netzwerklast durch die Verwendung von VAs besonders profitiert werden kann. Bei 10 Clienten und einer Datenrate von 450 kbit/s (Abb. 6.15, links) kann der Anteil der Flüsse mit einem höheren Durchsatz als 400 kbit/s durch die VAs bei 2 Kanälen von 68 % auf 77 % gesteigert werden. Damit liegt letzteres sogar oberhalb dessen was mit 3 Kanälen und ohne VA erzielt wurde (72 %). Die verteilten Antennen können auch bei 3 Kanälen den Durchsatz weiter steigern. Der Anteil der Flüsse mit einem Durchsatz von 400 kbit/s und mehr kann auf 80 % gesteigert werden. Der Durchsatz in einem Netzwerk kann also nicht dadurch weiter gesteigert werden, dass die Anzahl der Kanäle zugunsten von verteilten Antennen reduziert wird. Jedoch können VA den den Durchsatz zusätzlich steigern.

Bei höherer Netzwerklast reduziert sich der Gewinn durch die VAs, wie den Ergebnissen für die

Simulationen mit 10 Clienten und 900 kbit/s (Abb. 6.16, links) und jenen mit 20 Clienten und einer Datenrate von 450 kbit/s (Abbildung 6.15, rechts) zu entnehmen ist. Im letzteren Fall steigt bei einem Kanal der Anteil der Flüsse mit mehr 400 kbit/s von 52 % auf 54 %, wenn verteilte Antennen mit dem Cognitive Acknowledgement verwendet werden.

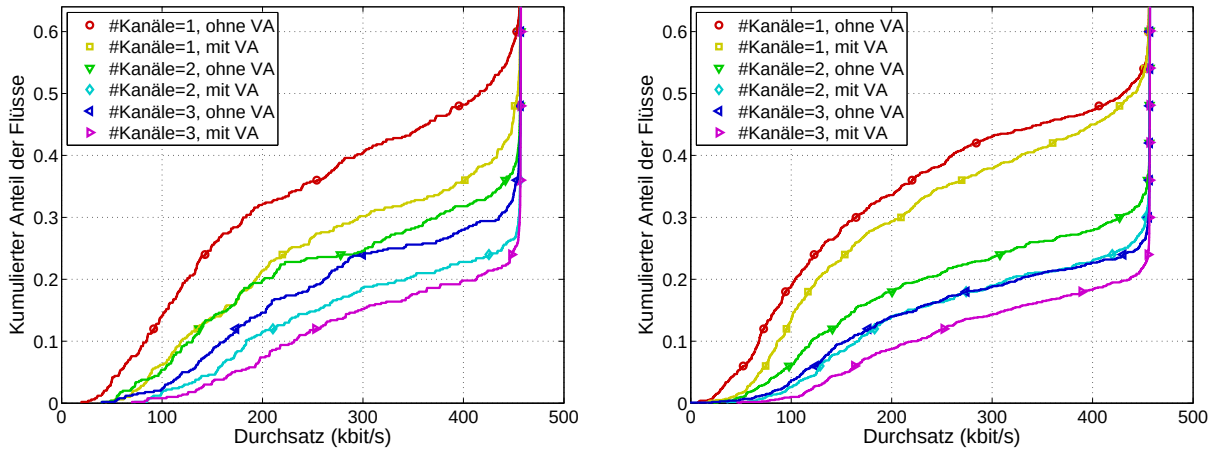

Abbildung 6.15: Reale Platzierung: Kumulierter Durchsatz im Szenario mit 10 (links) bzw. 20 Clienten (rechts) und einer Datenrate von jeweils 450 kbit/s.

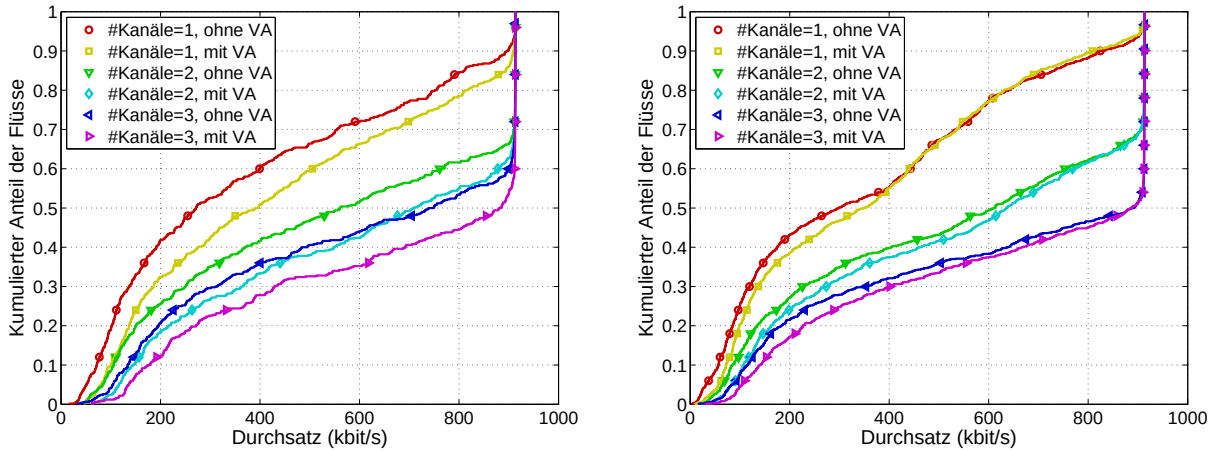

Abbildung 6.16: Reale Platzierung: Reale Platzierung: Kumulierter Durchsatz im Szenario mit 10 bzw. 20 (rechts) Clienten und einer Datenrate von jeweils 900 kbit/s. Besonders schwache Verbindungen profitieren von verteilten Antennen.

Bei einer weiteren Erhöhung der Netzwerklast (Abb. 6.16, rechts) ist eine Verbesserung des Durchsatzes durch VA nur noch bei Flüssen mit geringerem Durchsatz festzustellen. In dem Szenario mit 3 Kanälen und 20 Clienten, welche jeweils mit einer Datenrate von 900 kbit/s sendeten (Abb. 6.16, rechts),

wird der Anteil der Flüsse mit einem Durchsatz von über 200 kbit/s von 78 % auf 83 % durch verteilte Antennen gesteigert. Der Anteil der Flüsse mit einem Durchsatz von mehr als 600 kbit/s kann hingegen nur noch von 61 % auf 62 % gesteigert werden.

Zusätzliche Kanäle hingegen steigern bei solcher Netzlast den Durchsatz enorm. Allein durch die Verwendung von 3 statt 2 Kanälen wird der Anteil von Flüssen mit mehr als 800 kbit/s von 37 % auf 53 % gesteigert. Es ist anzunehmen, dass die Verwendung weiterer Kanäle die Durchsätze weiter steigern würde.

6.3.1 Auswertung und Diskussion

Die Evaluation der Verfahren für die Kanalzuweisungen haben gezeigt, dass die Verwendung mehrerer Kanäle in Verbindung mit einer effizienten Kanalzuweisung den Durchsatz im Netzwerk steigert. Die Kapazität wird dadurch deutlich erhöht und Interferenzen werden minimiert. Die Heuristiken LRU, Merge und Simulated Annealing unterschieden sich bei den Ergebnissen kaum. Die erzielten Durchsätze bei zufälliger Kanalzuweisung (Random) lagen jedoch bis zu 13 % unterhalb jener, die bei der Kanalzuweisung durch die andere 3 Heuristiken erreicht wurden. Unterschiede zeigen sich jedoch in den zusätzlichen Möglichkeiten der Heuristiken. Sowohl LRU als auch Simulated Annealing können externe Störquellen berücksichtigen, d. h. durch andere Technologien belegt Kanäle können von einzelnen APs vermieden werden. LRU bieten zudem die Möglichkeit einer verteilten Realisierung.

Für die Realisierung der verteilten Antennen wurde das in Abschnitt 4.2.2 beschriebene Cognitive Acknowledgement verwendet. Die Simulationen zeigten, dass besonders schwache Links mit hohen Paketfehlerraten von verteilten Antennen profitieren. Durch mehrere Empfänger konnte die Paketefehler, welche durch geringe Signalstärke und Interferenzen verursacht wurden, reduziert werden. Es zeigte sich, dass der Gewinn zudem maßgeblich vom Abstand zwischen den APs einer VA abhängt, da das Cognitive Acknowledgement voraussetzt, dass eine AP die Pakete der anderen APs innerhalb der VA wahrnehmen kann.

Die Kombination des Kanalzuweisungverfahren LRU und der verteilten Antennen mit dem Congnitiven Acknowledgement zeigte, dass die Kanalzuweisung wesentlicher für hohen Durchsatz im drahtlosen Netzwerk ist. Zwar konnten die VAs den Durchsatz ebenfalls weiter steigern, eine Reduzierung der Kanäle zugunsten möglicher besserer verteilter Antennen ist jedoch von Nachteil und führte zu einem geringeren mittleren Durchsatz. Besonders bei hohen Netzlasten kann man davon ausgehen, dass die Verwendung von mehr als den hier benutzten 3 Kanälen, den Durchsatz weiter erhöht, obwohl die Möglichkeiten zur Bildung von VAs dadurch weiter zurückgeht. Die VAs bieten vielmehr eine zusätzliche Möglichkeit die Paketfehler weiter zu reduzieren und die Latenz der Übertragungen zu reduzieren. Dabei kann, wie hier gezeigt, durchaus Einfluss auf die Kanalzuweisung genommen werden, indem z. B. unbenutzte APs einen anderen Kanal verwenden als sie bei der Kanalzuweisung erhalten haben, um so als zusätzliche Empfänger in einer verteilten Antennen zu agieren.

Da die Dichte in drahtlosen Netzwerken in Zukunft weiter zunimmt, ist anzunehmen, dass selbst bei Verwendung aller zur Verfügung stehender Kanäle, die Dichte der APs pro Kanal deutlich höher sein wird und so die verteilten Antennen bessere Ergebnisse erzielen. In dieser Arbeit war besonders die Anzahl der APs relativ gering. Die Messung des Interferenzgraphen war hier der begrenzende Faktor, da die Dauer quadratisch mit der Anzahl der APs wächst.

Kapitel 7

Zusammenfassung

In dieser Arbeit wurden untersucht, wie sich Kanalzuweisung und verteilte Antennen miteinander kombinieren lassen, um die Leistung im Netzwerk gegenüber der isolierten Anwendung eines der beiden Verfahren zu steigern. Dazu wurde zunächst auf die Zuweisung der Kanäle in einem Infrastruktur-Netzwerk eingegangen. Da es sich dabei um eine NP-hartes Problem handelt, wurden im darauf folgenden Abschnitt verschiedene Heuristiken vorgestellt. Das Augenmerk richtete sich dabei nicht nur auf die Komplexität des jeweiligen Verfahrens, sondern auch darauf, inwieweit sich Beschränkungen in der Kanalwahl, z. B. durch externe Störquellen, berücksichtigen lassen und eine verteilte Realisierung möglich ist. Der für die Kanalzuweisung benötigte Interferenzgraph wurde erklärt und verschiedene Methoden vorgestellt, wie dieser ermittelt werden kann.

Im folgenden Kapitel wurde das Konzept der verteilter Antennen vorgestellt. Es wurden verschiedene Ansätze diskutiert, welche sich entweder innerhalb der MAC-Schicht oder als zusätzliche Schicht zwischen MAC- und Netzwerkschicht umsetzen lassen. Zu ersteren gehören u. a. das Slotted Acknowledgement und das daran angelehnte Cognitive Acknowledgement. Das vorgestellte MRD benötigt hingegen eine zusätzliche Schicht oberhalb der MAC-Schicht. Die Protokolle wurden zudem dahingehend untersucht, ob sowohl Sender und Empfänger angepasst werden müssen, oder dies nur bei letzteren nötig ist. Das Cognitive Acknowledgement und das verteilte Bestätigen durch Sendediversität benötigen lediglich Änderungen auf Seiten des Empfängers. Ein weiteres Kriterium zur Bewertung stellte die benötigte Bandbreite im Backbone-Netzwerk, welche durch mögliche Duplikate bei Verwendung mehrerer Empfänger, ansteigt. Das Cognotive Acknowledgement und das Slotted Acknowledgement bieten dabei den Vorteil, dass durch das Protokoll jeder potentielle Empfänger erkennen kann, welcher der anderen die selben Pakete empfangen hat. Dadurch kann ein mehrfaches Weiterleiten der Pakete an den zentralen Controller verhindert werden. Im Vergleich aller vorgestellte Verfahren erfühlte das Cognitive Acknowledgement die meisten Anforderungen. Dieses Protokoll basiert darauf, dass ein AP das Senden einer Bestätigung eines anderen APs erkennt. Es wurden drei mögliche Optionen für dieses Erkennen diskutiert.

Sowohl die Heuristiken für die Kanalzuweisung als auch das Cognitive Acknowledgement wurden im Netzwerksimulator implementiert, getrennt sowie in Kombination evaluiert. Bei hoher Netzlast war die Anzahl der verwendeten Kanäle und die Kanalzuweisung ein entscheidender Faktor für den Durchsatz im Netzwerk. Die zufällige Kanalzuweisung erzielte erstaunlich gute Ergebnisse, die in Abhängigkeit der Netzwerklast trotzdem z. T. deutlich von den anderen verwendeten Verfahren, wie z. B. Simulated Annealing, übertroffen wurden. Der mittlere Durchsatz lag beim Simulated Annealing um bis zu 13 % über jenem, der bei zufälliger Kanalzuweisung erreicht wurde. Die Ergebnisse von Simulated Annealing, Merge und LRU waren hingegen ähnlich. Der mittlere Durchsatz unterschied sich um weniger als 5 %. Die Kanalzuweisung durch LRU erwies sich jedoch als das vielseitigste Verfahren, da sich dies zum einen verteilt umsetzen lässt und zum anderen auch externe Störquellen berücksichtigt werden können.

Für das bei verteilten Antennen zum Einsatz kommende Cognitive Acknowledgement wurden drei verschiedene Optionen zum Erkennen von Übertragungen anderer APs implementiert und in verschiedenen Szenarien evaluiert. Als Kriterium wurde neben der Verbesserung des Durchsatzes auch die Anzahl der erkannten Bestätigungen und der Kollisionen verwendet. Die drei Verfahren erkennen eine gesendete Bestätigung anhand der Signalstärke, wobei der Grenzwert für eine erkannte Übertragung jeweils unterschiedlich ist. Das Verfahren welches die Signalstärke, die auf eine Übertragung durch einen anderen AP innerhalb der verteilten Antenne hinweist, dynamisch ermittelte, stellte sich dabei als das effektivste heraus. Es misst den Rauschpegel kurz nach dem Ende der Datenübertragung und berechnet daraus den Schwellwert. Dadurch wurde das Protokoll auch bei mehreren APs bzw. Clienten im Netzwerk wenig durch parallele Übertragungen gestört. Durch die verteilten Antennen konnte der mittlere Durchsatz in großen Netzwerken um bis zu 14 % gesteigert werden. Besonders schwache Links, welche also eine hohe Paketfehlerrate aufwiesen, konnten von den verteilten Antennen überproportional profitieren. Die Latenz konnte ebenfalls durch die verteilten Antennen reduziert werden. So sank z. B. in einem Netzwerk mit 10 APs und 10 Clienten der Anteil der Übertragungen, die mehr als 20 ms benötigten von 30 % auf 12 %.

Die Ergebnisse zeigten, dass der Gewinn durch verteilte Antennen stark von der Dichte des Netzwerkes abhängt. In sehr dichten Netzwerken ist die Menge potentieller verteilter Antennen größer, jedoch ist durch den geringen Abstand zwischen den Clienten und den APs die Fehlerrate sehr gering, so dass die zusätzlichen Empfänger innerhalb der verteilten Antenne wenig Gewinn bringen. Bei geringer Netzwerkdichte ist die für die verteilten Antennen nötige Koordination zwischen den APs aufgrund der größeren Entfernung zwischen ihnen in weniger Fällen gewährleistet und somit die Menge potentieller verteilter Antennen geringer.

Sowohl eine effiziente Kanalzuweisung als auch verteilten Antennen verbessern den Durchsatz. Beide Verfahren lassen sich jedoch nicht so einfach kombinieren, da die Verwendung von mehreren Kanälen zu einer Verringerung der Dichte von APs pro Kanal führt und somit die Menge möglicher verteilter Antennen reduziert wird. Die Evaluation, bei welcher LRU und das Cognitive Acknowledgement kombiniert wurden, zeigte, dass bei hoher Netzwerklast der Paketverlust vorrangig durch Kollisionen (Interferenz) verursacht wurde. Die Verwendung mehrerer Kanäle konnte die Interferenz und somit die Paketfehlerrate reduzieren und so den Durchsatz erhöhen. Bei geringerer Netzwerklast sind geringe Signalstärken (Weak-Signal) durch Shadowing und Fading die Ursache für Paketverluste. In solchen Situationen können verteilte Antennen die Paketfehlerrate reduzieren und den Durchsatz steigern, da die Links durch mehrere Empfänger robuster werden. Jedoch können auch zusätzliche Kanäle den Durchsatz erhöhen, da so mehr parallele Übertragungen gemacht werden können und jedes Gerät häufiger auf das Medium zugreifen und somit auch mehr (Neu-)Übertragungen machen kann. Der Paketverlust wird dadurch jedoch nicht verringert.

Es zeigte sich, dass die Reduzierung der Kanäle zugunsten besserer verteilter Antennen zu keiner zusätzlichen Steigerung des Durchsatzes führt. Die verteilten Antennen konnten vielmehr zusätzlich den Durchsatz durch Reduzierung der Paketfehler steigern.

Kapitel 8

Ausblick

Die Verbesserung der Netzwerkleistung, welche durch Einsatz von verteilten Antennen und der Verwendung von mehreren Kanälen in Verbindung mit einer effizienten Kanalzuweisung erzielt werden kann, ist wie in Kapitel 6 gezeigt, stark von der vorliegende Netzwerklast und der Anzahl der Benutzer abhängig. Die Ergebnisse dieser Arbeit können eine Grundlage für den Entwurf eines dynamischen Systems bilden, bei welchem die Anzahl der Kanäle und die Größe von verteilten Antennen der vorliegenden Situation angepasst wird. Durch Analyse des Netzwerkverkehrs kann ein zentraler Controller ermitteln, ob die Ursache vorliegende Übertragungsfehler eine schwache Signalstärke oder Kollisionen sind, wie Rayanchu et al. in [36] zeigen. Die Anzahl der Kanäle kann bei starker Interferenz erhöht werden, um Störungen zu minimieren, wodurch jedoch die Möglichkeit zur Bildung von verteilten Antennen reduziert wird.

Viele weitere Möglichkeiten bieten sich auch bei der Kombination von verteilten Antennen und Kanalzuweisung. Anders als in dieser Arbeit können z. B. zunächst die verteilten Antennen gebildet werden, um ihnen im nächsten Schritt einen Kanal zuzuweisen.

Neben der Verwendung von mehreren Kanälen stellt die dynamische Kontrolle der Sendeleistung eine weitere Möglichkeit dar, die Interferenz in drahtlosen Netzen, deren Dichte zukünftig weiter steigen wird, zu reduzieren. Jedoch hätte auch dies Einfluss auf den Einsatzmöglichkeiten von verteilten Antennen. Zwei weitere Technologien, welche den Durchsatz in drahtlosen Netzwerken verbessern, sind Superpositioncoding[44] und Sendediversität (Transmit-Diversity). Jedoch schränkt auch hier die Verwendung von mehreren Kanälen den Einsatz dieser beiden Verfahren ein. Der in dieser Arbeit verwendete Netzwerksimulator kann dahingehend erweitert werden, um auch eine Kombination dieser drei Ansätze mit verteilten Antennen bzw. der Verwendung mehrerer Kanäle zu evaluieren.

Eine weitere Möglichkeit der Erweiterung ist die gezielte Kanalzuweisung bzw. das gezielte Bilden von verteilten Antennen, um bestimmten Benutzern im Netzwerk eine bessere Verbindung zu ermöglichen. Einen Operator eines solchen Netzwerken kann u.a. bestimmte Vorgaben (Policies) machen, um so z. B. bevorzugten Kunden (Premium User) einem bessere Qualität (Quality of Service, Qos) zu liefern. Ein solcher Benutzer bekommt z. B. einen weniger benutzen Kanal zugewiesen oder mehrere APs bilden eine verteilte Antenne für ihn. Es ist außerdem möglich eine bestimmte Art des Netzwerkverkehrs zu bevorzugen. Die Empfängern des selben Multicast-Datenstroms können z. B. gezwungen werden, sich mit dem selben AP zu assoziieren, um so die Anzahl der benötigten Übertragungen zu reduzieren.

Software-Defined Radio (SDR), wie das Calradio[17], ermöglichen es, Verfahren wie das in dieser Arbeit vorgestellte Cognitive Acknowledgement auch auf realer Hardware umzusetzen, da sich die Funktionen der MAC-Schicht bei diesen Geräten verändern lassen. Bei einigen Geräten, wie z. B. dem Universal Software Radio Peripheral[26] und dem Warp Board[41], wird lediglich das analoge Signal in einen digitalen Datenstrom umgewandelt. Die weitere Verarbeitung wird durch Software vorgenommen, wodurch z. T. sogar auf physikalischer Schicht eine Kooperation zwischen mehreren Empfängern möglich ist[27, 20].

Anhang A

Verteilte Antennen mit Standard 802.11 MAC

Im Abschnitt 6.2 wurde das Cognitive Acknowledgement anhand eines einfachen Szenarios evaluiert. Dabei bildeten zwei APs eine verteilte Antenne. Der Client hatte in den einzelnen Simulationen unterschiedliche Abstände zu den APs. Auch die Abstände zwischen den APs wurden variiert. Die Auswertung der Ergebnisse zeigte, dass je nach verwendetem Verfahren zur Erkennung einer gesendeten Bestätigung, ab einem Abstand von 120 - 140 m der zweite AP der verteilten Antenne vermehrt die Übertragung nicht erkannt hat (Abbildung 6.4). Dennoch konnte z. T. eine Steigerung des Durchsatzes ermittelt werden. Dies soll in diesem Abschnitt anhand einiger Überlegungen mathematisch begründet werden.

Es wird wieder ein Szenario wie in Abschnitt 6.2 angenommen, bei welchem beide APs eine verteilte Antenne bilden. Das Protokoll für die verteilte Bestätigung wird jedoch stark vereinfacht. Jeder AP, der ein Paket des Clienten fehlerfrei empfängt, bestätigt dieses. Dabei wird das Senden der Bestätigung auch nicht verzögert, um die Belegung des Mediums zu überprüfen, da dies entfällt. Sollten beide APs das Paket empfangen, so senden also auch beide gleichzeitig eine Bestätigung. In diesem Fall kommt es zu einer Kollision und es wird angenommen, dass der Client keine Bestätigungen erhält. Dies ist eine härtere Annahme als sie im Simulator umgesetzt wurde. Dort wird auf Basis der Differenz der Signalstärken beider Bestätigungen entschieden, ob beide oder nur eine von beiden nicht empfangen wird. Bei hohen Unterschieden in der Signalstärke kann der Client das stärkere Signal und somit eine der Bestätigungen empfangen (Capture-Effekt).

Da das Bestätigungspaket klein ist (14 Bytes) und zudem immer auf der Basisdatenrate gesendet wird, ist die Fehlerrate kleiner, d. h. Bestätigungen werden mit höherer Wahrscheinlichkeit korrekt empfangen als die Datenpakete. Aus diesem Grund werden in den folgende Abschnitten diesbezüglich zwei Annahmen untersucht. Zunächst wird angenommen, dass die Bestätigung außer bei einer möglichen Kollisionen immer empfangen werden. Danach wird für die Bestätigung die selbe Fehlerwahrscheinlichkeit angenommen wie für die Datenpakete.

Fehlerfreie Bestätigung

In diesem Abschnitt wird angenommen, dass eine gesendete Bestätigung immer empfangen wird, außer eine weitere Bestätigung wird gleichzeitig übertragen. In diesem Fall kommt es zu einer Kollision und keine der Bestätigungen kann empfangen werden. Wie bereits beschrieben, besteht das betrachtete Szenario aus den beiden APs A und B.
Zunächst werden folgende Empfangswahrscheinlichkeiten angenommen:

1. $P(A) = x$ (Wahrscheinlichkeit, dass A das Paket r empfängt)
2. $P(\bar{A}) = (1 - x)$ (Wahrscheinlichkeit, dass A das Paket r nicht empfängt)
3. $P(B) = y$ (Wahrscheinlichkeit, dass B das Paket r empfängt)
4. $P\left(\bar{B}\right) = (1 - y)$ (Wahrscheinlichkeit, dass B das Paket r nicht empfängt)

Beide APs bilden eine verteilte Antenne, d. h. beide können Pakete vom Sender empfangen und bestätigen. Die Empfangswahrscheinlichkeiten werden dabei als unabhängig voneinander betrachten.

1. $P(A \cup B) = x \cdot y$ (Wahrscheinlichkeit, dass A und B das Paket r empfangen)
2. $P(\bar{A} \cup B) = (1 - x) \cdot y$ (Wahrscheinlichkeit, dass B das Paket r empfängt, A jedoch nicht)
3. $P(A \cup \bar{B}) = x \cdot (1 - y)$ (Wahrscheinlichkeit, dass A das Paket r empfängt, B nicht)
4. $P(\bar{A} \cup \bar{B}) = (1 - x) \cdot (1 - y)$ (Wahrscheinlichkeit, dass A und B das Paket r nicht empfangen)

Sollten beide APs das Paket r empfangen (1.), werden die Bestätigungen beider, welche sie bei diesem einfachen Verfahren senden, immer kollidieren. Hier führt eine verteilte Antenne aus den APs A und B also zu einem Verlust gegenüber einem einzelnen AP A. Im 2. Fall ergibt sich ein Gewinn durch dieses Verfahren, da B ein Paket bestätigt, welches A nicht empfangen hat. Die letzten beiden Fälle empfängt B das Paket nicht und somit besteht kein Unterschied zum einzelnen AP A.

Durch den Vergleich von 1. und 2. lässt sich ermitteln, unter welchen Bedingungen bei diesem Verfahren der Gewinn (Fall 2) der verteilten Antenne größer ist als der Verlust (Fall 1). Der Gewinn ist dabei die Differenz der Empfangswahrscheinlichkeiten mit und ohne verteilter Antenne. Es muss gelten:

$$\begin{aligned} P(A) \cup P(B) &< P(\bar{A}) \cup P(B) \\ \Rightarrow x \cdot y &< (1 - x) \cdot y \\ x &< (1 - x) \\ 2 \cdot x &< 1 \\ \Rightarrow x &< 0,5 \end{aligned}$$

Der Gewinn, welcher durch die verteilte Antenne erzielt wird, ist unabhängig von der Empfangswahrscheinlichkeit von AP B solange AP A weniger als die Hälfte der Datenpakete korrekt empfängt. Da beide APs innerhalb der verteilten Antennen vertauscht werden können, muss die Empfangswahrscheinlichkeit von B ebenfalls kleiner als 0,5 sein, da dieser sonst alleine einen höheren Durchsatz erzielen könnte als beide APs gemeinsam.

Der Gewinn G dieses vereinfachten Verfahrens lässt sich mit Hilfe der gemachten Annahmen ermitteln. Dazu wird die Empfangswahrscheinlichkeit eines einzelnen APs A mit der einer verteilten Antenne, bestehend aus AP A und B verglichen. Es gilt folgendes:

$$\begin{aligned} P(A) + G &= P(\bar{A}) \cup P(B) + P(A) \cup P(\bar{B}) \\ \Rightarrow x + G &= (1 - x) \cdot y + x \cdot (1 - y) \\ &= y - x \cdot y + x - x \cdot y \\ \Rightarrow G &= y - 2 \cdot x \cdot y \\ &= y(1 - 2x) \end{aligned}$$

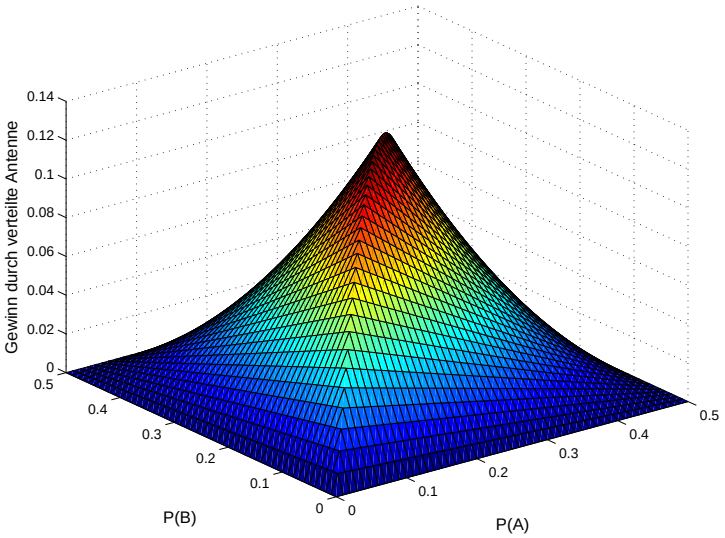

Abbildung A.1: Gewinn durch den Einsatz einer verteilten Antenne mit 2 APs mit $P(A) > P(B)$ bei einer fehlerfreien Bestätigung.

Auch hier sieht man sofort, dass es keinen Gewinn bzw. einen Verlust gibt, wenn die Empfangwahrscheinlichkeiten von AP A gleich oder größer als 0,5 ist. Die Abbildung A.1 zeigt den Gewinn in Abhängigkeit von den Empfangswahrscheinlichkeiten von A und B, wobei für beide nur das Intervall von 0 bis 0,5 betrachtet wird, da nur dort ein Gewinn zu erwarten ist, wie oben bereits erwähnt wurde.

Wie der Abbildung A.1 entnommen werden kann, ist der Gewinn maximal, wenn die Empfangswahrscheinlichkeiten beider APs 0,25 beträgt. Es ergibt sich daraus:

$$\begin{aligned} G &= y - 2 \cdot x \cdot y \\ \Rightarrow G &= 0,25 - 2 \cdot 0,25 \cdot 0,25 \\ &= 0,125 \end{aligned}$$

Eine verteilte Antennen aus zwei APs, die jeweils eine Empfangswahrscheinlichkeit von 0,25 haben, hat eine Empfangswahrscheinlichkeit von 0,375, liegt also um 0,125 höher. Sie wird also um 50 % erhöht.

Fehlerhafte Bestätigung

Im vorherigen Abschnitt wurde angenommen, dass die einzelnen Bestätigungen immer erfolgreich übertragen werden. Im folgenden Abschnitt ist die Annahme, dass die Wahrscheinlichkeit für ein erfolgreiches Übertragen der Bestätigung genauso hoch ist wie für die Übertragung des Datanpaketes. Zunächst wird ermittelt unter welchen Bedingungen eine Gesamtübertragung in beiden Fällen, d. h. bei Verwendung eines einzelnen APs A bzw. einer verteilten Antenne bestehend aus den APs A und B, erfolgreich ist. Dazu gehört neben dem korrekten Empfang des Datenpaketes eine erfolgreiche Übertragung der Bestätigung.

Für einen einzelnen AP A ergibt sich die Wahrscheinlichkeit für eine erfolgreiche Gesamtübertragung $P_G^E(A)$ aus der Empfangswahrscheinlichkeit eines einzelnen Paketes $P(A)$.

1. $P_G^E(A) = P(A) \cdot P(A)$

Für einen AP innerhalb einer verteilte Antenne ist dies recht ähnlich, jedoch darf hier der jeweils andere AP das Paket nicht erhalten, da es sonst durch das gleichzeitige Senden der Bestätigungen zu einer Kollision kommt.

1. $P_G^{VA}(A) = P(A) \cdot P(\bar{B}) \cdot P(A)$
2. $P_G^{VA}(B) = P(B) \cdot P(\bar{A}) \cdot P(B)$

Für den Gewinn eines einzelnen APs gegenüber einer verteilten Antenne ergibt sich:

$$\begin{aligned} P_G^E(A) + G &= P_G^{VA}(A) + P_G^{VA}(B) \\ \Rightarrow x^2 + G &= x^2 \cdot (1-y) + y^2 \cdot (1-x) \\ G &= y^2 \cdot (1-x) - x^2 \cdot y \end{aligned}$$

Die Abbildung A.2 zeigt den Gewinn in Abhängigkeit der einzelnen Übertragungswahrscheinlichkeiten von AP A und B. Der Gewinn innerhalb des abgebildeten Intervalls hat sein Maximum von $0,\overline{037}$ bei $P(A) = P(B) = 0,\overline{3}$. Die Übertragungswahrscheinlichkeit wird um 11 % gesteigert.

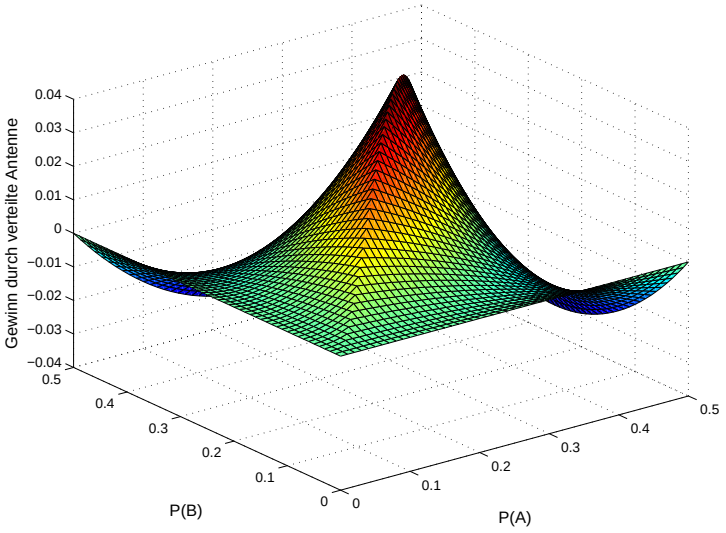

Abbildung A.2: Gewinn durch den Einsatz einer verteilten Antenne mit 2 APs mit $P(A) > P(B)$.

Zusammenfassung

Die Rechnungen in den beiden vorherigen Abschnitten können die in den Simulationen gemachten Beobachtungen erklären. In [29] konnte Kurth et al. durch Messungen zeigen, dass ein gleichzeitiges Bestätigen durch mehrere Empfänger gegenüber den hier gemachten Annahmen nicht immer destruktiv ist. Die gleichseitig gesendeten Signale können sich sogar konstruktiv überlagern und so zu einer Erhöhung der Signalstärke beim Empfänger führen. Zudem kann der Empfänger bei großen Unterschieden der Signalstärken das stärkere Signal dekodieren (Capture-Effekt). Es kann dabei also eine der Bestätigung empfangen werden. In diesen Fällen erzielt ein solches Verfahren für verteilte Antennen, bei welchem alle Empfänger gleichzeitig das Paket bestätigen, eines viel höheren Vorteil gegenüber einem einzelnen AP.

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACI ..... Adjacent-Channel Interference
ACK ..... Acknowledgement
AID ..... Association Identity
AP ..... Access Point
ARQ ..... Automatic Repeat Request
BSS ..... Basic Service Set
BSSID ..... Basic Service Set Identifier
CCA ..... Clear Channel Assessment
CFP ..... Contention Free Period
CIR ..... Carrier-To-Interference-Ratio
CRC ..... Cyclic Reduncancy Check
CSMA ..... Carrier Sense Multiple Access
DCF ..... Distributed Coordination Function
DFS ..... Dynamic Frequency Selection
DS ..... Distribution System
ETX ..... Expected Transmission Count
FEC ..... Forward Error Correction
IEEE ..... Institute of Electrical and Electronics Engineers
IFS ..... Interframe Space
JiST ..... Java in Simulation Time
LOS ..... Line-of-sight
MAC ..... Medium Access Control
MISO ..... Multi Input Single Output
MRD ..... Multi Radio Diversity
NAV ..... Network Allocation Vector
NLOS ..... Non-Line-of-sight
OSI ..... Open Systems Interconnection
PCF ..... Point Coordination Function
PER ..... Packet Error Rate
PSR ..... Packet Success Rate
RRM ..... Radio Resource Measurement
RSSI ..... Receive Signal Strength Indication
SIR ..... Signal-To-Interferenece-Ratio
SNR ..... Signal-To-Noise-Ratio
SSID ..... Service Set Identifier
STA ..... Station (Client)
TPC ..... Transmission Power Control
VoIP ..... Voice over IP

WLAN ..... Wireless Local Area Network
WoW ..... Wake on WLAN

Literaturverzeichnis

[1] *IEEE 802.11 Working Group*. http://grouper.ieee.org/groups/802/11/, 1999

[2] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band*. http://standards.ieee.org/getieee802/download/802.11a-1999.pdf, 1999

[3] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*. http://standards.ieee.org/getieee802/download/802.11b-1999.pdf, 1999

[4] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher Data Rate Extension in the 2.4 GHz Band*. http://standards.ieee.org/getieee802/download/802.11g-2003.pdf, 2003

[5] A. Zubow, M. K. ; Redlich, J.-P.: Multi-Channel Opportunistic Routing. (2007)

[6] *Actix*. www.actix.com, 2009

[7] Ahmed, N. ; Keshav, S.: SMARTA: a self-managing architecture for thin access points. In: *CoNEXT '06: Proceedings of the 2006 ACM CoNEXT conference*. New York, NY, USA : ACM, 2006. – ISBN 1–59593–456–1, S. 1–12

[8] Alamouti, S. M.: A simple transmit diversity technique for wireless communications. In: *Selected Areas in Communications, IEEE Journal on* 16 (1998), Nr. 8, 1451–1458. http://dx.doi.org/10.1109/49.730453. – DOI 10.1109/49.730453

[9] Alk, Robert ; Arepally, Anurag: Dynamic Channel Assignment in IEEE 802.11 Networks. (2007)

[10] Allen Miu, Hari B. ; Koksal, Can E.: Improving Loss Resilience with Multi-Radio Diversity in Wireless Networks. (2005)

[11] Anand Prabhu Subramanian, Himanshu G. ; Das, Samir R.: Minimum-Interference Channel Assignment in Multi-Radio Wireless Mesh Networks. (2007)

[12] Anatolij Zubow, Mathias K. ; Redlich, Jens-Peter: Considerations on Forwarder Selection for Opportunistic Protocols in Wireless Networks. (2008)

[13] Bahl, Paramvir ; Hajiaghayi, Mohammad T. ; Jain, Kamal ; Mirrokni, Vahab ; Qiu, Lili ; Saberi, Amin: Cell Breathing in Wireless LANs: Algorithms and Evaluation. (2008)

[14] Barr, Rimon ; Haas, Zygmunt J. ; Renesse, Robbert van: JiST: an efficient approach to simulation using virtual machines. In: *Software: Practice and Experience* 35 (2005), Nr. 6, S. 539–576

[15] Bejerano, Y. ; Han, S.-J.: Cell Breathing Techniques for Load Balancing in Wireless LANs. (2006)

[16] Bernhard H. Walke, Stefan M. ; Berlemann, Lars: *IEEE 802 Wireless Systems*. Wiley, 2007

[17] *CalRadio*. `http://calradio.calit2.net`, 2009

[18] Chaitin, Gregory: Register allocation and spilling via graph coloring. (2004)

[19] *D-Link DWS-3024L*. `ftp://ftp.dlink.eu/datasheets/DWS-3024L.pdf`, 2009

[20] Dohler, Mischa: *Virtual Antenna Arrays*, University of London, Diss., 2003

[21] Dr. Hussain Al-Rizzo, Dr. Robert A. Mohamad Haidar H. Mohamad Haidar ; Chan, Dr. Y.: Enhanced Channel Assignment and Load Distribution in IEEE 802.11 WLANs. (2008)

[22] Dubois-Ferrière, Henri ; Estrin, Deborah ; Vetterli, Martin: Packet combining in sensor networks. (2005), S. 102–115. `http://dx.doi.org/http://doi.acm.org/10.1145/1098918.1098930`. – DOI http://doi.acm.org/10.1145/1098918.1098930. ISBN 1–59593–054–X

[23] Eric Rozner, Aditya A. Yogita Mehta M. Yogita Mehta ; Qiu, Lili: Traffic-Aware Channel Assignment in Enterprise Wireless LANs. (2008)

[24] *fon*. `http://www.fon.com`, 2009

[25] Garcia, Eduard ; Vidal, Rafael ; Paradells, Josep: Cooperative Load Balancing in IEEE 802.11 Networks with Cell Breathing. (2008)

[26] *GnuRadio*. `http://www.gnuradio.org`, 2009

[27] Grace R. Woo, Dawei S. Pouya Kheradpour K. Pouya Kheradpour ; Katabi, Dina: Beyond the Bits: Cooperative Packet Recovery Using Physical Layer Information. (2007)

[28] Jens Nachtigall, Anatolij Z. ; Redlich, Jens-Peter: The Impact of Adjacent Channel Interference in Multi-Radio Systems using IEEE 802.11. (2008)

[29] Kurth, Mathias ; Zubow, Anatolij ; Redlich, Jens-Peter: Cooperative Opportunistic Routing Using Transmit Diversity in Wireless Mesh Networks. (2008)

[30] *Madwifi*. `http://madwifi-project.org/`, 2009

[31] Mohamad Haidar, Dr. Hussain Al-Rizzo Robert A. Robert Alk ; Chan, Dr. Y.: Channel Assignment and Load Distribution in a Powermanaged WLAN. (2007)

[32] Murty, Rohan ; Padhye, Jitendra ; Chandra, Ranveer ; Wolman, Alec ; Zill, Brian: Designing high performance enterprise Wi-Fi networks. (2008), S. 73–88. ISBN 111–999–5555–22–1

[33] *NS2 - Network Simulator*. http://www.isi.edu/nsnam/ns/, 2009

[34] *olsrexperiment.de*. `http://berlin.freifunk.net/`, 2009

[35] Paramvir Bahl, Lenin R. Jitendra Padhye P. Jitendra Padhye ; Singh, Manpreet ; Wolman, Alec ; Zill, Brian: DAIR: A Framework for Managing Enterprise Wireless Networks Using Desktop Infrastructure. (2005)

[36] Rayanchu, S. ; Mishra, A. ; Agrawal, D. ; Saha, S. ; Banerjee, Suman: Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal. In: *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, 735–743

[37] Rech, Jörg: *Wireless LANs - 802.11-WLAN-Technologie und praktische Umsetzung im Detail*. Heise, 2006

[38] Silva, Jos´ Ferreira de R. d.: A Dynamic Channel Allocation Mechanism for IEEE 802.11 Networks. (2006)

[39] *Simulated annealing*. `http://en.wikipedia.org/wiki/Simulated_annealing`, 2009

[40] *T-Mobile Hotspot*. `http://www.t-mobile.de/hotspot`, 2009

[41] *WARP*. `http://warp.rice.edu`, 2009

[42] Youngseok Lee, Kyoungae K. ; Choi, Yanghee: Optimization of AP Placement and Channel Assignment in Wireless LANs. (2002)

[43] Zubow, A.: *Kooperatives Forwarding in drahtlosen Maschennetzen*, Diss., 2009

[44] Zubow, A. ; Graul, Moritz: Uplink Superposition Coding and Multi-User Diversity. (2009)

Danksagung

An dieser Stelle möchte ich mich noch einmal bei allen bedanken, die mir bei der Fertigstellung dieser Arbeit geholfen haben. Mein größter Dank gilt meinem Betreuer Anatolij Zubow, der mich besonders bei der Umsetzung im Simulator mit vielen Ideen und Ratschlägen unterstützte.
Bedanken möchte ich mich auch bei Mathias Kurth für die wertvollen Hinweise zum Thema der Arbeit. Außerdem möchte ich meiner Freundin und meiner Cousine für das Korrekturlesen der Arbeit und ihren kritischen Anmerkungen danken.

Selbstständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Berlin, den 5. November 2009

Robert Sombrutzki

Einverständniserklärung

Ich erkläre hiermit mein Einverständnis, dass die vorliegende Arbeit in der Bibliothek des Institutes für Informatik der Humboldt-Universität zu Berlin ausgestellt werden darf.

Berlin, den 5. November 2009

Robert Sombrutzki