Technische Universität München
Lehrstuhl für Kommunikationsnetze

Dienstgüte für vermaschte drahtlose Netze

Dipl.-Ing. Univ. Silke Meister

Vollständiger Abdruck der von der Fakultät Elektrotechnik und Informationstechnik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

genehmigten Dissertation.

Vorsitzende:		Univ.-Prof. Dr.-Ing. Sandra Hirche
Prüfer der Dissertation:	1.	Univ.-Prof. Dr.-Ing. Jörg Eberspächer (i.R.)
	2.	Univ.-Prof. Dr.-Ing. Klaus Diepold

Die Dissertation wurde am 05.04.2012 bei der Technischen Universität München eingereicht und durch die Fakultät für Elektrotechnik und Informationstechnik am 10.10.2012 angenommen.

Dienstgüte für vermaschte drahtlose Netze

Dipl.-Ing. Univ. Silke Meister

29. November 2012

Vorwort

Diese Arbeit fasst die Ergebnisse meiner Tätigkeit als wissenschaftliche Mitarbeiterin am Lehrstuhl für Kommunikationsnetze (LKN) der TU München zusammen.

Mein besonderer Dank gilt meinem Doktorvater Prof. Dr.-Ing. Jörg Eberspächer, der mich in sein Forschungsteam aufnahm und mir dadurch die Gelegenheit zu dieser Arbeit bot. Ich möchte mich bei ihm für die vielen wertvollen Denkanstöße bedanken, vor allem aber für seine Geduld und sein Vertrauen in meine Fähigkeiten, sowie für die Schaffung einer einzigartigen Arbeitsatmosphäre.

Als Mitglied der LKN-Familie durfte ich vom Wissen und den Erfahrungen zahlreicher Kollegen und ehemaliger Kollegen profitieren und hatte wiederholt die Möglichkeit, fruchtbare Diskussionen (nicht ausschließlich fachlicher Art) zu führen. Ich möchte mich in erster Linie bei Dr. Christian Hartmann für die Begleitung meiner Forschungsarbeit und wichtige Beiträge und Anregungen zu meinem Thema bedanken, sowie bei den anderen Kollegen der Forschungsgruppe Mobilfunk, insbesondere Hans-Martin Zimmermann, Robert Nagel und meinen Bürokollegen Robert Vilzmann und Jan Ellenbeck. Für jahrelange moralische Unterstützung danke ich den Kollegen Christoph Spleiß, Peter Hinterseer, Robert Prinz und Quirin Hofstätter. Mein Dank gebührt auch Dr. Martin Maier – er hatte stets eine Lösung für Probleme aller Art, oder wusste zumindest, wen man anrufen muss.

Einige Ideen zu meiner Arbeit stammen aus dem Industrieprojekt QualiMesh. Für die erfolgreiche Zusammenarbeit danke ich Michael Bahr und Dr. Rainer Sauerwein von Siemens Corporate Technology.

Stellvertretend für alle Studenten, die ich während meiner Zeit am Lehrstuhl betreuen durfte, möchte ich hier Bernhard Beyer und Thomas Gehrsitz nennen, die viel Zeit und Energie investierten und in zahlreichen Diskussionen wertvolle Beiträge zu meiner Arbeit leisteten.

Nicht zuletzt danke ich meiner Familie – meinen Eltern Wolfgang und Doris Meister und meinen Schwestern Sabine und Kerstin, die immer für mich da sind und mich in allen meinen Entscheidungen unterstützen.

München, im April 2012 Silke Meister

Kurzfassung

Eine Ausprägung drahtloser Netze sind die Wireless Mesh Networks, also drahtlose vermaschte Kommunikationsnetze. Diese besitzen, im Gegensatz zu Zellularnetzen, keine zentrale Steuerungseinheit (Access Point oder Basisstation), die den Medienzugriff und die Authentifizierung regelt. Ein Vorteil solcher vermaschten Netze besteht darin, dass die Netzabdeckung vergrößert werden kann, da nicht mehr jedes Endgerät in Sendereichweite einer Basisstation oder eines Access Points sein muss, um Zugang zum Netz zu erhalten. Stattdessen kann die Kommunikation über andere Endgeräte erfolgen, welche als Relais fungieren und die Daten weiterleiten.

Herausforderungen sind dabei Datensicherheit, Routing, Managebarkeit und vor allem die Gewährleistung der Dienstgüte. Abhängig von der betrachteten Anwendung kann es notwendig sein, dass eine maximal tolerierbare Verzögerung nicht überschritten wird (z.B. bei IP-Telefonie) oder dass eine hohe Datenrate erzielt wird (z.B. bei Videostreaming). Da in drahtlosen Netzen die verfügbare Bandbreite begrenzt ist und außerdem zwischen den einzelnen Teilnehmern aufgeteilt werden muss, sind spezielle Mechanismen notwendig, um eine effiziente Nutzung sicherzustellen.

In dieser Arbeit wird zunächst eine Architektur entwickelt, welche Dienstgütemechanismen für allgemeine vermaschte drahtlose Netze kombiniert und so in der Lage ist, Dienstgüte bereitzustellen. Die Mechanismen sind flexibel und können für spezielle Szenarien und Anwendungsfälle angepasst werden. Welche Parameterwahl für welchen Betriebsfall geeignet ist, wird sowohl analytisch als auch simulativ untersucht. Darauf aufbauend wird eine Managementarchitektur konzipiert, die es dem Betreiber ermöglicht, den Zustand des Netzes zu überwachen. Das in ihr gesammelte Netzwissen wird außerdem genutzt, um eine optimale Einstellung der Parameter der Dienstgütemechanismen zu erreichen.

Die wesentlichen Neuheiten dieser Arbeit sind:

- Kombination existierender Dienstgütemechanismen zu einer kompakten und flexiblen Architektur,
- Analytische Beschreibung der Mechanismen,
- Entwurf einer Managementarchitektur, welche es ermöglicht, die Mechanismen an den aktuellen Zustand des Netzes anzupassen.

Kompatibilität zu bestehenden Konzepten und Standards sowie einfache Anwendbarkeit sind dabei wichtige Randbedingungen.

Abstract

Wireless mesh networks are a form of wireless networks which, unlike cellular networks, do not comprise a central entity (access point or base station) to control medium access and authentication. A basic advantage of a meshed network is increased coverage, since not every terminal needs to be in transmission range of a base station or access point to gain access to the network. Instead, data packets can be relayed via other devices.

Research challenges regarding wireless mesh networks include security, routing, manageability, and especially quality of service. Depending on the application, it may be necessary that a maximum tolerable delay is not exceeded (e.g. for IP telephony) or that a high data rate is achieved (e.g. for video streaming). Due to bandwidth limitations in wireless networks, special mechanisms are necessary to ensure efficient use of resources.

The architectur which was developed during the course of this work is suitable to provide quality of service for wireless mesh networks by combining several basic mechanisms. These mechanisms are flexible and can be adapted to specific scenarios and use cases. Parameters suitable for individual operating cases were evaluated both analytically and using simulations. Based on the results, a management architecture was developed which allows the network operator to monitor the state of the network. Knowledge gathered by the management architecture can be used to achieve optimal parameter settings regarding the quality of service mechanisms.

The main contributions of this thesis are:

- combination of existing quality of service mechanisms to a simple and flexible architecture,
- analytical description of the mechanisms,
- development of a management architecture, which allows to adapt the mechanisms according to the current state of the network.

Primary constraints were compatibility with existing concepts and standards, as well as ease of deployment and operation.

Inhaltsverzeichnis

1 Einführung

Mit der Einführung des Mobilfunkstandards GSM (Global System for Mobile Communications) zu Beginn der 1990er Jahre stand mobile Telefonie erstmals der breiten Masse zur Verfügung. Das legte den Grundstein zu einer wichtigen gesellschaftlichen Entwicklung unserer Zeit: Permanente Erreichbarkeit. Parallel zum zellularen Mobilfunk hat sich WLAN (Wireless Local Area Network, zu deutsch drahtloses lokales Netz) für den drahtlosen Internetzugang etabliert. Da neben Telefonie auch Datenübertragung, wie das Versenden von E-Mails und der Austausch über Soziale Netzwerke, eine immer größere Rolle spielt, wird drahtloser Internetzugang (und zwar immer und überall) fundamental für unsere Lebensart.

Zellulare Mobilfunknetze wurden ursprünglich zum Telefonieren konzipiert, was die Benutzung durch den Endanwender relativ teuer, aber Netzabdeckung und Service dafür verhältnismäßig gut macht. Die Verwendung eines eigenen Frequenzbandes garantiert dem einzelnen Benutzer eine (relativ niedrige) Mindestdatenrate. Ein Netz gehört üblicherweise einem Betreiber, der für Aufbau und Wartung sowie die Abrechnung der Nutzungsgebühren verantwortlich ist. WLANs werden hingegen nicht zentral verwaltet, sondern üblicherweise in Privathaushalten oder Firmen verwendet. Sie bilden kein zusammenhängendes Netz, sondern viele kleine Teile, die sich oft sogar gegenseitig stören. Durch die Verwendung eines öffentlich verfügbaren Frequenzbandes sind zwar höhere Datenraten erzielbar, können hier aber nicht garantiert werden. Beim ursprünglichen Anwendungsgebiet (hauptsächlich Datenverkehr) war dies jedoch auch nicht nötig.

Obwohl die beiden Netzarten ursprünglich für unterschiedliche Zwecke konzipiert waren, sind die Grenzen heute nicht mehr so starr. Datentransport über Mobilfunknetze ist heute bereits möglich und wird in zukünftigen Mobilfunkstandards (siehe LTE) eine noch größere Rolle spielen. Auf der anderen Seite ermöglicht IP-Telefonie die Übertragung von Sprachdaten über das Internet. Auch bei den Endgeräten sieht man einen deutlichen Trend zur Konvergenz: Smart Phones eignen sich zum Telefonieren genauso wie zum Surfen im Internet. WLAN und zellulare Mobilfunknetze werden daher immer mehr zu Konkurrenten. Gleichzeitig entwickeln sie sich entsprechend den Ansprüchen ihrer Nutzer technisch in eine ähnliche Richtung.

Endnutzer hätten gerne ein ubiquitäres Netz mit hoher Datenrate, das alle Arten von (Sprach- und Daten-)Verkehr unterstützt und dessen Nutzung am besten kostenfrei ist. Um diesen Wunsch zu erfüllen, müsste Mobilfunk noch erheblich schneller und preisgünstiger, oder WLAN großflächiger verfügbar werden. Ein Schritt in diese Richtung sind Wireless Mesh Networks (WMN), also vermaschte drahtlose Netze.

Bei dieser Weiterentwicklung von WLAN können Endgeräte direkt miteinander kommunizieren und die Daten anderer Netzteilnehmer weiterleiten. Dadurch wird die Netzabdeckung vergrößert, ohne dass sich dabei die Kosten für die Infrastruktur des Netzes erhöhen.

Durch diese Vergrößerung werden die Netze allerdings auch schlechter überschaubar, was die Frage der Managebarkeit eines Netzes aufwirft. Unter Management fällt dabei sowohl die Überwachung des Zustandes eines Netzes (Teilnehmerzahl, Auslastung, etc.) als auch der Eingriff in die Funkionalität. Dazu sind spezielle Protokolle erforderlich.

Drahtlose Netze gewinnen zwar immer mehr an Bedeutung, aber große Nachteile gegenüber drahtgebundenen Netzen sind nach wie vor ihre Unzuverlässigkeit und begrenzte Kapazität. Deshalb sind entsprechende Mechanismen notwendig, um sie für die Anforderungen der Zukunft (zeitkritische Anwendungen wie Sprachübertragung und Anwendungen, die eine hohe Datenrate erfordern, wie Echtzeitvideo) zu rüsten. Durch höhere erzielbare Datenraten wird diese Problematik nur vorübergehend gelöst, da sich gleichzeitig auch die Anwendungen weiterentwickeln werden. Eine effiziente Nutzung der Ressourcen wird deshalb immer wichtig sein.

Die in dieser Arbeit vorgestellte Architektur adressiert genau diese Punkte: Dienstgüte und Management für vermaschte drahtlose Netze.

Da WMNs vielseitig einsetzbar sind, ist es wichtig, dass sich die verwendeten Mechanismen ebenfalls für verschiedene Szenarien und Einsatzgebiete eignen. Dies ist bei vielen existierenden Mechanismen, die oft für sehr spezielle Anwendungsfälle entworfen wurden, leider nicht der Fall. Ziel dieser Arbeit war es daher, eine QoS- und Managementarchitektur zu entwerfen, die geringe Komplexität aufweist und sich gleichzeitig flexibel an die äußeren Umstände anpassen lässt. Die Managementkomponente dient dabei dazu, den Zustand des Netzes zu beurteilen und die Dienstgütemechanismen entsprechend zu parametrisieren, um eine bestmögliche Nutzung der Ressourcen zu ermöglichen.

Abb. 1.1 verdeutlicht den Aufbau der Arbeit.

In Kapitel 2 werden zunächst die grundlegenden in dieser Arbeit verwendeten Begriffe geklärt. Darunter fällt die Beschreibung der Netzstruktur sowie verschiedener Dienstgüte- und Managementmechanismen, auf denen in den nachfolgenden Kapiteln aufgebaut wird.

Kapitel 3 beschreibt die entwickelte QoS-Architektur. Dabei wird auf die Kriterien für das Design eingegangen, der Aufbau der einzelnen Mechanismen wird dargelegt und die Funktionalität anhand von Simulationsergebnissen belegt.

Kapitel 4 umfasst die mathematische Beschreibung eines Teils der in Kap. 3 vorgestellten Mechanismen. Die Ergebnisse werden den Simulationsergebnissen aus Kap. 3 gegenübergestellt. Das entwickelte Markovmodell wird anschließend verwendet, um

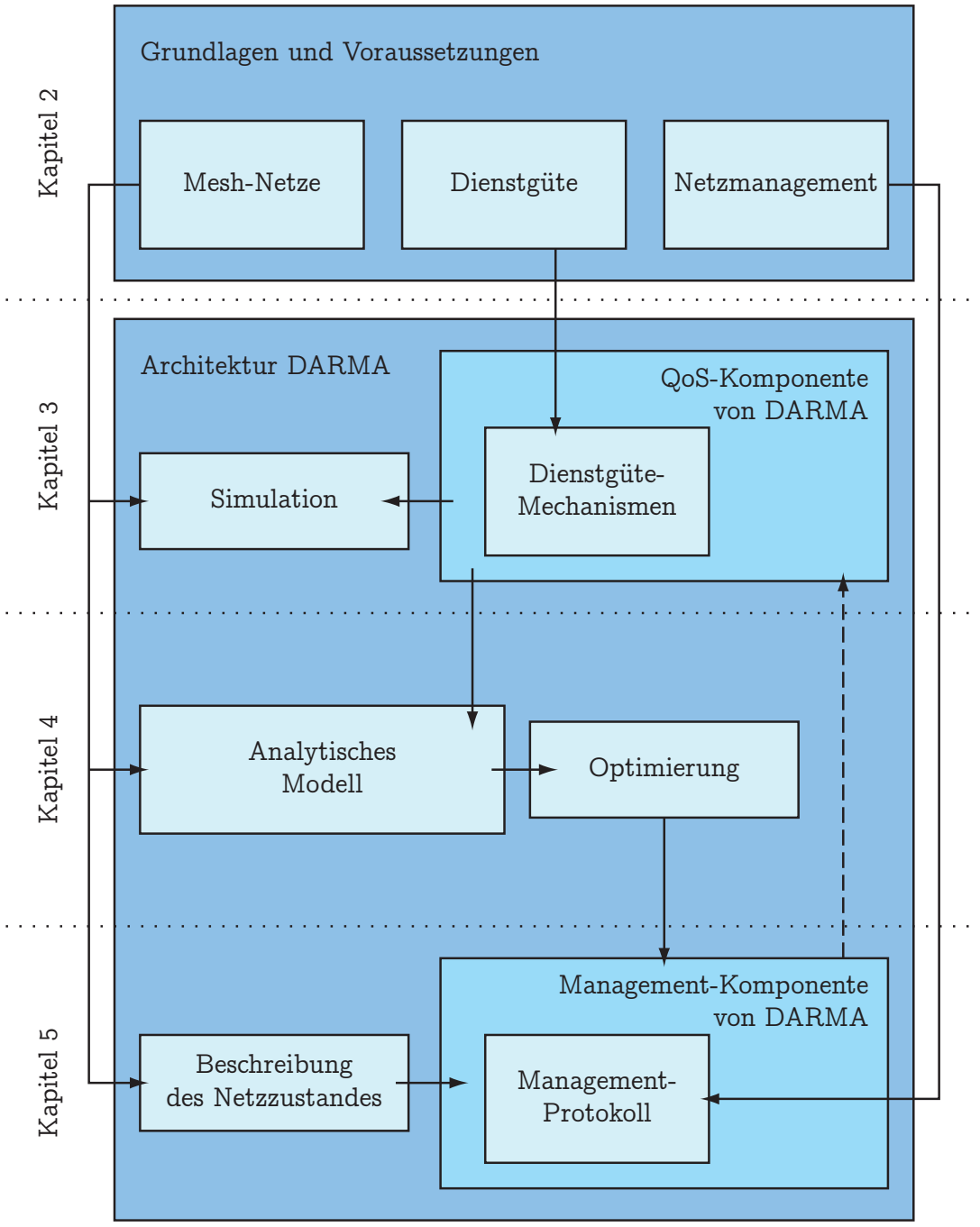


Abbildung 1.1: Zusammenhänge zwischen den einzelnen Kapiteln dieser Arbeit

optimale Parameter für die untersuchten Dienstgütemechanismen unter Berücksichtigung verschiedener Randbedingungen zu ermitteln.

Kapitel 5 beschreibt die Managementkomponente der Architektur. Neben Möglichkeiten der Beschreibung und Erfassung des Netzzustandes wird ein Protokoll zum Auslesen und Ändern der Parameter vorgestellt. Unter Zuhilfenahme der Ergebnisse aus Kap. 4 kann damit die optimale Einstellung der Dienstgüteparameter veranlasst werden.

Zusammenfassung und Ausblick in Kapitel 6 runden die Arbeit ab.

Der Anhang gibt einen Überblick über die grundlegende Funktionalität von IEEE 802.11 und der beiden verwendeten Simulatoren sowie Details des in Kap. 4 beschriebenen Markovmodells.

2 Grundlagen und Voraussetzungen

Zunächst sollen einige grundlegende Begriffe aus dem Bereich der Kommunikationsnetze geklärt werden, die in dieser Arbeit verwendet werden.

- Ein Kommunikationsteilnehmer ist ein Gerät, welches über ein Kommunikationsmedium (z.B. Kabel oder Funkkanal) mit einem Netz verbunden ist und mit Hilfe vordefinierter Protokolle mit anderen Geräten kommunizieren kann. In dieser Arbeit werden die Begriffe Knoten, Station und Endgerät als Synonyme für Kommunikationsteilnehmer verwendet. Hierbei kann es sich um diverse Geräte handeln, in erster Linie wird hier jedoch von PCs, Laptops und Mobiltelefonen ausgegangen.

- Das OSI-Modell (OSI-Schichtenmodell oder OSI-Referenzmodell [70], OSI steht für Open Systems Interconnection) wurde von der ISO als Designgrundlage für Protokolle in Kommunikationsnetzen entwickelt. Es definiert sieben voneinander abhängige Schichten (engl.: layers), wobei jeweils die untere Schicht Dienste für die darüberliegende Schicht bereitstellt. Die einzelnen Schichten sind von unten nach oben: 1. Bitübertragung (Physical Layer, auch physikalische Schicht), 2. Sicherung (Data Link), 3. Vermittlung (Network), 4. Transport, 5. Kommunikationssteuerung (Session), 6. Datendarstellung (Presentation), 7. Anwendung (Application). Häufig werden jedoch die drei oberen Schichten unter dem Begriff *Anwendungsschicht* zusammengefasst. Die Sicherungsschicht wird in zwei Unterschichten (sub layers) unterteilt, nämlich Medium Access Control (MAC, Medienzugriffssteuerung, 2a) und Logical Link Control (LLC, 2b). Eine genauere Beschreibung des OSI-Modells findet sich beispielsweise in [54]. In der vorliegenden Arbeit liegt der Fokus hauptsächlich auf der MAC-Schicht.

- Ein Datenpaket bezeichnet allgemein eine in sich geschlossene Dateneinheit, die von einem Sender an einen Empfänger geschickt wird. Insbesondere sind damit Dateneinheiten auf Schicht 3 des OSI-Modells gemeint. In dieser Arbeit wird der Begriff *Paket* jedoch unabhängig von der Schicht für alle Dateneinheiten verwendet, insbesondere auch auf der MAC-Schicht.

- Der Begriff *Verbindung* kann im Deutschen verschiedene Bedeutungen haben. Eine physikalische (drahtgebundene oder Funk-) Verbindung zwischen zwei Kommunikationsteilnehmern zeigt an, dass ein Kommunikationsmedium vorhanden ist, über welches eine Datenübertragung möglich ist (engl.: link). Eine Nachrichtenverbindung (engl.: connection) bezeichnet eine Datenübertragung zwischen zwei Teilnehmern, die den Aufbau eines physikalischen oder logischen Kanals voraussetzt.

In dieser Arbeit wird in erster Linie von verbindungslosen Datenübertragungen ausgegangen. Die Begriffe (Daten-)Übertragung, Verkehrsfluss, Verkehrsstrom, Datenfluss und Datenstrom werden dabei synonym für Kommunikationsbeziehungen zwischen zwei Endgeräten verwendet (engl.: traffic flow).

- Multihop (engl.: multi hop – mehrere Sprünge) bedeutet, dass zwischen zwei Kommunikationspartnern keine direkte physikalische Verbindung besteht. In diesem Fall sind Datenübertragungen nur über eine oder mehrere zwischenliegende Stationen möglich, welche als Relais fungieren und die Daten weiterleiten. Die Daten werden dabei über mehrere Schritte bzw. Hops von einem Knoten zum nächsten transportiert. Eine Datenübertragung, die auf eine Relaisstation zurückgreift, umfasst demnach zwei Hops: einen vom Sender zum Relais und einen vom Relais zum Empfänger.

Viele Fachbegriffe in der Kommunikationstechnik entstammen der englischen Sprache. Soweit möglich, wurden in dieser Arbeit die äquivalenten deutschen Ausdrücke verwendet. Eine Auflistung der verwendeten Begriffe mit der jeweiligen Übersetzung findet sich am Ende dieser Arbeit.

2.1 Wireless Mesh Networks

In einem vermaschten drahtlosen Netz (Wireless Mesh Network, WMN) sind die beteiligten Knoten über die Luftschnittstelle miteinander verbunden, ohne dass eine zentrale Einheit (z.B. Access Point, AP oder Basisstation, BS) die Datenübertragungen koordiniert. Im Gegensatz zu Ad-hoc-Netzen sind WMNs im Voraus geplant und decken ein bestimmtes Gebiet ab. Nicht alle Knoten in einem WMN sind mobil, feststehende Knoten sorgen für eine grundlegende Konnektivität im Netz. Nach IEEE 802.11s [66] werden folgende Arten von Knoten unterschieden:

Mesh-Knoten (engl.: mesh points) sind Knoten, die Mesh-Fähigkeiten haben (u.a. Routing). Sie bilden das Rückgrat des WMNs.

Mesh-Gateways sind Mesh-Knoten, die gleichzeitig als Gateways zu anderen Netzen agieren, wie z.B. dem Internet oder Mobilfunknetzen.

Mesh-Access-Points sind Mesh-Knoten, die gleichzeitig als Access Point (AP) fungieren und den Knoten, die nicht mesh-fähig sind, Zugang zum WMN bieten.

Endgeräte haben keine speziellen mesh-bezogenen Fähigkeiten.

Die Eigenschaften von WMNs sind in Tab. 2.1 denjenigen von Ad-hoc-Netzen und WLAN gegenübergestellt. Ein umfangreicher Vergleich mit verschiedenen Arten von drahtlosen Netzen findet sich auch in [1].

Man kann WMNs grob in zwei Kategorien einteilen [7], die abhängig vom vorliegenden Szenario Einsatz finden:

Tabelle 2.1: Vergleich zwischen WMN, WLAN und Ad-hoc-Netzen

Parameter	WMN	WLAN	Ad-hoc
geplantes Netz	✓	✓	–
statische Knoten	✓	✓	–
multihop	✓	–	✓
selbstkonfigurierend	✓	–	✓
zentrale Kontrolleinheit	–	✓	–
Lebensdauer	lang	lang	kurz

- Ein Backbone-Mesh-Netz besteht aus Mesh-Access-Points, die drahtlos miteinander verbunden sind. Stationen können sich mit einem dieser APs verbinden, um Zugang zum Netz zu bekommen (Abb. 2.1).
- In einem Client-Mesh-Netz ist jedes Endgerät ein Mesh-Knoten und unterstützt Routing und das Weiterleiten von Nachrichten. In diesem Fall kann jeder Knoten zu allen anderen Knoten in Reichweite eine direkte Funkverbindung aufbauen.

Natürlich sind auch Mischformen zwischen den beiden Fällen denkbar.

2.1.1 Einsatzgebiete

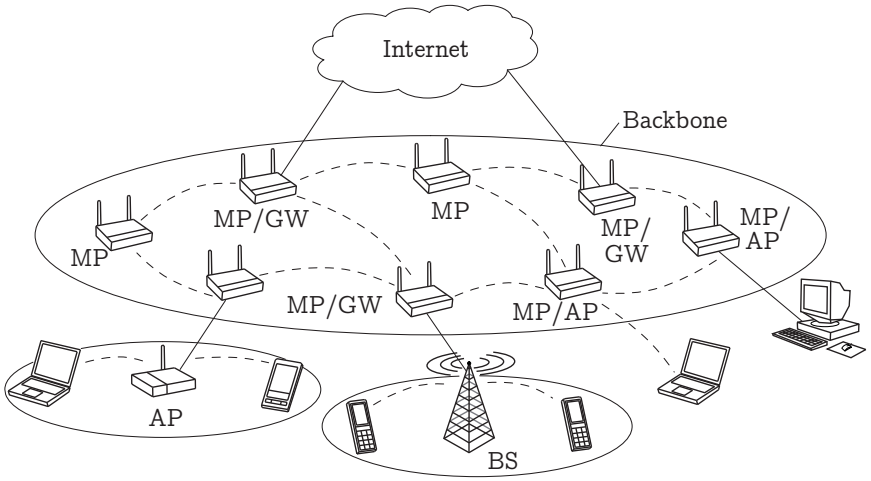
Ein vermaschtes drahtloses Netz kann drahtgebundene Netze überall dort ersetzen, wo letztere nicht realisierbar sind und der Einsatz eines traditionellen WLANs nicht praktikabel ist. Beispiele hierfür sind:

Campus-Szenario: Großflächiger Internetzugang, beispielsweise auf einem Universitätscampus. Hierfür wird eine große Anzahl an WLAN-Access-Points benötigt, um flächendeckenden Internetzugang zu gewährleisten. Wenn man diese APs drahtlos miteinander verbindet, werden Kosten gespart, da so nicht jeder eine drahtgebundene Anbindung an das Internet braucht.

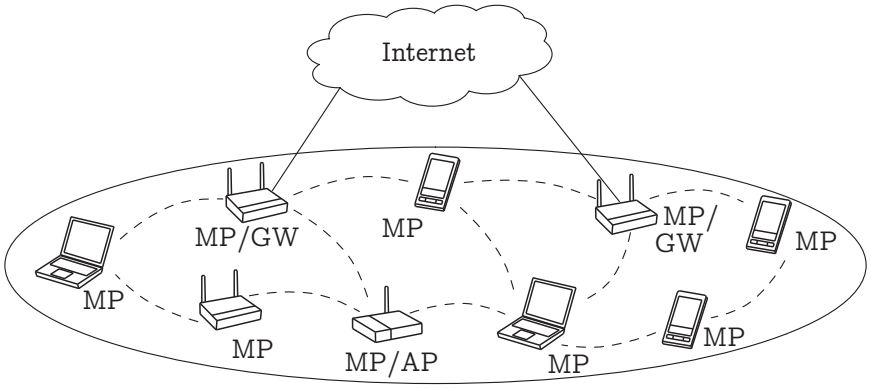
Office-Szenario: In denkmalgeschützten Gebäuden oder an Orten, die oft umgebaut werden (z.B. Film-Sets) kann ein WMN das drahtgebundene Büronetz ersetzen.

Emergency-Szenario: In Katastrophengebieten, wo keine Infrastruktur (mehr) vorhanden ist, bietet ein WMN den Vorteil, dass es schnell aufgebaut werden kann. Mit nur einigen wenigen Knoten, die eine Internetanbindung haben (über Kabel oder Satellit), kann großflächig Internetzugang bereitgestellt werden.

WMNs sind dezentral und selbstkonfigurierend, und wegen dieser Ähnlichkeiten mit Ad-hoc-Netzen können viele Mechanismen mit leichten Abänderungen wiederverwendet werden. Es gibt jedoch auch neue Herausforderungen: Wenn ein WMN ein drahtgebundenes Netz ersetzen soll, werden höhere Erwartungen an die Zuverlässig-



(a) Backbone-Mesh-Netz



(b) Client-Mesh-Netz

Abbildung 2.1: Einteilung von Wireless Mesh Networks. Mesh-Knoten (MP) können Daten weiterleiten. Gateways (GW) und Access Points (AP) erlauben die Anbindung an andere Netze und zu Stationen ohne Mesh-Fähigkeiten.

keit gestellt. Hier müssen neue Lösungen für Ausfallsicherheit, Dienstgüte und auch Datensicherheit gefunden werden.

2.1.2 Technologie

Heutige Realisierungen von Wireless Mesh Networks basieren auf unterschiedlichen Technologien, darunter in erster Linie WLAN nach IEEE 802.11 [63] und die zugehörigen Erweiterungen a, b, g und n. Da diese jedoch ursprünglich nicht für den Einsatz in vermaschten Netzen konzipiert wurden, sind sie nicht optimal dafür geeignet. So sind durch Weiterentwicklungen viele proprietäre Lösungen entstanden.

IEEE hat sich des Aspekts der WMNs im Jahr 2003 angenommen und 2004 eine eigene Taskgroup gegründet, um den Mesh-Standard IEEE 802.11s [66] zu entwickeln. Aus

15 eingegangenen Vorschlägen wurden bis 2006 zwei Hauptentwürfe, die dann zu einem ersten Draft zusammengefügt wurden. Die Fertigstellung des Standards wurde mehrfach verschoben. Nach Einarbeitung zahlreicher Kommentare erhielt der Draft 12.0 im Juni 2011 eine Zustimmungsrate von 97,2 %. Im September 2011 konnte der fertige Standard veröffentlicht werden.

Der Hauptvorteil von 802.11s gegenüber bisherigen Lösungen ist das Routing auf Schicht 2 des OSI-Modells, das sogenannte MAC-Relaying. Dadurch sollen die Netze wesentlich effizienter arbeiten können. Weitere Neuerungen sind die Fähigkeit der Stationen, ihre Nachbarschaft zu erkunden (wird bei der Initialisierung des Netzes benötigt), eine Erweiterung des bisherigen IEEE 802.11e [64] für Dienstgüte, sowie eine Änderung des Verfahrens zur Authentifizierung (diese kann in einem WMN nicht mehr auf Client-Server-Basis funktionieren, da alle Stationen gleichberechtigt sind).

Die in dieser Arbeit vorgestellten Konzepte sind parallel zum Standardisierungsprozess entstanden und sind deshalb nicht in allen Punkten konform mit dem Standard. Diese Abweichungen sind als Alternative bzw. Erweiterung zu 802.11s zu betrachten.

2.1.3 Eigenschaften

Die hier betrachteten Netze haben bis zu 32 Mesh-Knoten, von denen jeder auch als Access Point arbeiten kann. Mit jedem Access Point sind maximal zehn Endgeräte verbunden. Diese sind teilweise mobil und können Geschwindigkeiten von bis zu 1 m/s haben. Insgesamt wird in dieser Arbeit jedoch von weitgehend statischen und homogenen Szenarien ausgegangen. Jede Station hat nur eine Luftschnittstelle und kann daher nicht gleichzeitig senden und empfangen. Des Weiteren wird auch nur ein Kanal genutzt. Mesh-Knoten können, müssen aber nicht, mit intelligenten Antennen (ermöglicht Beamforming [51]) ausgestattet sein. Auf physikalischer Schicht wird IEEE 802.11 [63] verwendet, wie auch im Anhang A genauer beschrieben. Übliche Anwendungen sind entsprechend den oben genannten Szenarien das Aufrufen von Webseiten, Versenden von E-Mails, Betrachten von Videos über das Internet und IP-Telefonie, im Katastrophenszenario auch Gruppenkommunikation, Echtzeitvideo und Übertragung von Sensordaten. Einige dieser Anwendungen haben bestimmte Mindestanforderungen an erzielbare Datenrate und/oder Verzögerungszeiten. Im folgenden Kapitel wird hierauf näher eingegangen.

2.2 Dienstgüte

Dienstgüte, oder auch Quality of Service (QoS), beschreibt die Qualität von Kommunikationsdiensten in einem Netz im Zusammenhang mit den Anforderungen des einzelnen Nutzers bzw. der Anwendung. Kriterien für die Beurteilung der Dienstgüte sind unter anderem:

Durchsatz: Multimediaanwendungen, wie beispielsweise Videoübertragungen, senden und/oder empfangen eine große Menge an Daten pro Zeiteinheit. Damit die gewünschten Datenraten erreicht werden können, muss das Netz eine bestimmte Mindestkapazität zur Verfügung stellen können.

Verzögerung: Bei interaktiven Realzeitanwendungen, wie z.B. IP-Telefonie, ist es notwendig, dass die Verzögerung der Datenpakete zwischen Sender und Empfänger einen bestimmten Maximalwert nicht überschreitet.

Paketverlustrate: Wenn ein Paket unterwegs (beispielsweise durch Störungen auf dem Kanal) verloren geht oder der Inhalt unlesbar wird, kann es, abhängig von der Anwendung, entweder erneut gesendet werden, oder es wird verworfen. Beim wiederholten Senden von Paketen muss darauf geachtet werden, dass die Verzögerung zwischen dem Erstaussenden und dem Empfang nicht zu groß wird (siehe *Verzögerung*). Bei Echtzeitanwendungen gelten Pakete, die zu spät ankommen, auch als verloren.

Schwankungen in der Paketverzögerung (Jitter): Für einige Anwendungen ist es wichtig, dass die Datenpakete in annähernd gleichmäßigen Abständen ankommen, um sie wie gewünscht verarbeiten zu können. Dies ist in erster Linie bei interaktiven Realzeitanwendungen der Fall (siehe auch *Verzögerung*).

Reihenfolge der Pakete: Normalerweise erreichen die Pakete den Empfänger in der Reihenfolge, in der sie ausgesendet werden (außer Paketen, die verloren gehen und neu angefordert werden müssen). Eine Ausnahme bilden Netze, in denen mehrere Wege zwischen Sender und Empfänger existieren und auch gleichzeitig genutzt werden. Hier kann es passieren, dass ein Paket, welches später gesendet wurde, früher ankommt, weil es über eine kürzere Route geleitet wurde. Eine Änderung der Reihenfolge der Datenpakete kann als Extremfall von Jitter betrachtet werden.

Fairness: Um Fairness objektiv messen zu können, müssen zunächst Kriterien definiert werden, nach denen beurteilt wird, was *fair* ist. Eine mögliche Vorgehensweise ist, dass allen Stationen die gleiche Menge an Ressourcen zugeteilt wird. Eine andere Strategie bevorzugt „wichtige“ Stationen, sodass diese öfter senden dürfen.

In dieser Arbeit werden hauptsächlich die ersten beiden Kriterien, *Durchsatz* und *Verzögerung*, betrachtet und bewertet. Die *Paketverlustrate* wird ebenfalls berücksichtigt, da abhängig von der jeweiligen Anwendung starke Beeinträchtigungen der Kommunikation die Folge sein können, falls die Paketverlustrate zu hoch ist. In diesem Fall können dann auch keine signifikanten Aussagen über andere Parameter getroffen werden. *Fairness* spielt hier zwar beim Designprozess der Mechanismen eine Rolle, nicht jedoch bei der Auswertung. Die *Reihenfolge* der Pakete kann sich nur ändern, wenn es mehrere unterschiedliche Routen zwischen Sender und Empfänger gibt, die gleichzeitig genutzt werden (Multipath-Routing), oder wenn die Route sich ändert, beispielsweise aufgrund von Mobilität der Teilnehmer. In den hier betrachteten Szena-

rien ist dies nicht der Fall. Schwankungen in der Paketverzögerung sind insbesondere bei IP-Telefonie relevant. Allerdings können diese Schwankungen durch Paketpuffer ausgeglichen werden, solange die Gesamtverzögerung nicht zu groß ist.

2.2.1 Einsatzgebiete

In Netzen, die auf dem Internetprotokoll (IP) basieren, wird üblicherweise keine Dienstgüte garantiert. Das beschleunigt die Verarbeitung der Pakete und spart Kosten für das Equipment. Das Internetprotokoll sieht im Paketheader zwar 8 bit für *Type of Service* (Dienstart) vor, die für die Priorisierung der Datenpakete verwendet werden könnten. Dies wird jedoch nur in seltenen Fällen genutzt. Meistens wird das Feld ignoriert und für alle Pakete die Standardeinstellungen verwendet, genannt *Best Effort*. Das bedeutet, dass alle Pakete entsprechend den verfügbaren Ressourcen so schnell wie möglich behandelt werden. Wenn ausreichend hohe Datenraten erreicht werden können und die Verarbeitungszeit der Pakete in den Routern ausreichend klein ist, sind auch keine zusätzlichen Maßnahmen notwendig, um alle Verkehrsströme ihren Anforderungen entsprechend zu bedienen. Kritisch wird es, wenn das Verkehrsangebot an die Grenzen der vorhandenen Kapazitäten stößt.

Die Forderung nach Dienstgüte wird stärker, je mehr zeitkritischer und ressourcenintensiver Verkehr durch das Netz geroutet werden soll. In den letzten Jahren ist insbesondere der Anteil an Sprach- und Videodaten stark angestiegen, durch Applikationen wie IP-Telefonie und die Verbreitung von Videoplattformen im Internet. Um diesen Anforderungen gerecht zu werden, müssen sich die Netze gleichermaßen weiterentwickeln. Insbesondere bei drahtlosen Netzen sind jedoch (noch) keine entsprechend hohen Datenraten erzielbar. Deshalb werden hier Dienstgütemechanismen benötigt, um die vorhandenen Ressourcen optimal auszunutzen.

QoS-Anforderungen sind aber nicht nur von der Applikation abhängig, sondern werden auch wesentlich durch die Nutzer und deren Erwartungen bestimmt. Diese hängen wiederum von der Art des betrachteten Netzes ab. In einem spontan aufgebauten Ad-hoc-Netz sind die Teilnehmer normalerweise nachsichtiger, da eine langsame Netzanbindung immer noch besser ist als gar keine Anbindung. Bei Festnetzen sind die Nutzer andererseits daran gewöhnt, dass hohe Datenraten und geringe Verzögerungen erzielt werden können. Ebenso hohe Erwartungen werden drahtlosen Netzen entgegengebracht, die ein Festnetz ersetzen sollen. Die drahtlose Lösung findet nur dann Akzeptanz unter den Nutzern, wenn eine ähnliche Dienstgüte bereitgestellt werden kann wie im äquivalenten drahtgebundenden Netz. Um diesen Anforderungen gerecht zu werden, sind passende Dienstgütemechanismen notwendig.

2.2.2 Herausforderungen

Wenn nur begrenzt Ressourcen zur Verfügung stehen, müssen diese effizient genutzt werden. Unter Ressourcen versteht man hierbei unter anderem Kanalkapazität,

Speicherplatz der Knoten (Warteschlangenlänge, wobei längere Warteschlangen zu höherer Verzögerung führen können, gleichzeitig aber natürlich zu niedriger Paketverlustrate), Lebensdauer der Batterie (bei Anschluss an das Stromnetz irrelevant) und Rechenleistung.

In drahtlosen Netzen sind üblicherweise geringere maximale Datenraten realisierbar als in drahtgebundenen Netzen. Darüber hinaus gibt es noch zusätzliche Herausforderungen:

Grundsätzlich gilt für drahtlose Netze, dass die Teilnehmer sich das Kommunikationsmedium, in diesem Fall den Funkkanal, mit benachbarten Stationen teilen. Deshalb ist innerhalb der Sendereichweite der Teilnehmer ohne weitere Vorkehrungen zu jedem Zeitpunkt nur eine Datenübertragung möglich. WLAN nach IEEE 802.11 [63] nutzt außerdem das unlizensierte Spektrum bei 2,4 GHz, welches für industrielle, medizinische und Forschungszwecke freigegeben ist (Industrial, Scientific, Medical Band – ISM). Das hat zur Folge, dass nicht genau bekannt ist, wie viele andere Geräte in der Umgebung das gleiche Frequenzband nutzen. Deshalb können keine exakten Angaben über die grundsätzlich verfügbare Kapazität gemacht werden, da immer zusätzliche Störungen auftreten können.

Aufgrund der Mobilität von Teilnehmern kann es passieren, dass sich die Topologie des Netzes während des Betriebs ändert. Dadurch müssen unter Umständen bestehende Verkehrsströme neu geroutet werden, wenn die genutzte Route nicht länger existiert. Dies kann eine Degradation der Dienstgüte zur Folge haben. Die Bewegung einzelner Teilnehmer kann unter Umständen auch dazu führen, dass das Netz in mehrere Teilnetze zerrissen wird, sodass zu bestimmten Teilnehmern gar keine Verbindung mehr besteht. Dies ist jedoch eher bei Ad-hoc-Netzen als bei Mesh-Netzen der Fall, da letztere ja im Vorhinein geplant werden und daher eine Grundkonnektivität existiert.

Die Qualität des Funkkanals ist unvorhersehbar, da der Kanal variablen Bedingungen und Umwelteinflüssen unterliegt. Diese führen zu Mehrwegeausbreitung, Dämpfung oder Abschattung des Signals, sowie zu Rauschen und Interferenz. Durch die Mobilität der Teilnehmer werden diese Effekte verstärkt. Unter Umständen wird dadurch auf höheren Schichten eine Unterbrechung der Funkverbindung diagnostiziert, obwohl nur ein vorübergehender Engpass vorliegt.

In drahtlosen Netzen mit verteilter Steuerung gibt es keine zentrale Kontrolleinheit, die den Ablauf der Mechanismen regelt und überwacht. Die einzelnen Teilnehmer müssen also selbständig bzw. in Absprache mit anderen Knoten entscheiden, was in bestimmten Situationen zu tun ist. Da jeder Knoten jedoch nur eine lokale Sicht des Netzes hat, müssen diese Entscheidungen auf Basis dieses begrenzt verfügbaren Wissens getroffen werden.

Im Vergleich zu drahtgebundenen Netzen gibt es also eine Vielzahl von Effekten, die zusätzlich berücksichtigt werden müssen. Diese abweichenden Herausforderungen machen neue Mechanismen für die Bereitstellung von Dienstgüte notwendig.

2.2.3 Möglichkeiten der Bereitstellung von Dienstgüte

Üblicherweise wird zwischen zwei Formen der Dienstgüte unterschieden:

absolut: Hier werden jedem Verkehrsfluss Ressourcen zugesichert, die ausreichen, um bestimmte vorher definierte Grenzwerte bezüglich Datenrate und Verzögerung einzuhalten (siehe auch IntServ [74]). Dazu ist es notwendig, die zur Verfügung stehenden Kapazitäten zu kennen und einen Überblick über die einzelnen Verkehrsströme und ihren Ressourcenbedarf zu wahren.

relativ: Hierbei wird jedem Verkehrsfluss entsprechend seinen QoS-Anforderungen eine Priorität zugewiesen, und Pakete von Verkehrsflüssen höherer Priorität werden bevorzugt behandelt (siehe auch DiffServ [75, 76]). Bei mittlerer Auslastung des Netzes reicht das normalerweise aus, um die Anforderungen aller Verkehrsströme zu erfüllen. Im Fall von Überlast oder Störungen von außerhalb des Netzes kann dies jedoch nicht immer gewährleistet werden. Wichtige Pakete werden dann zwar schneller weitergeleitet als andere, aber unter Umständen trotzdem nicht schnell genug.

Wie im vorigen Kapitel bereits erwähnt, ist die Garantie von absoluter Dienstgüte in unlizensierten Bändern nicht möglich. Da nicht bekannt ist, wie viele Ressourcen zur Verfügung stehen, kann auch niemandem garantiert werden, dass er eine bestimmte Menge Ressourcen nutzen darf. Es ist jedoch möglich, die verfügbaren Ressourcen bestimmten Vorgaben entsprechend auf die einzelnen Nutzer bzw. Verkehrsströme zu verteilen, und auf diese Weise für relative Dienstgüte zu sorgen. Das ist ausreichend, wenn Verkehrslast und äußere Störeinflüsse nicht zu groß sind.

Um in verteilten drahtlosen Netzen Dienstgüte bereitstellen zu können, sind demnach drei Komponenten notwendig [21, 44]: Medienzugriffssteuerung, Priorisierung der Verkehrsströme und Zugangskontrolle zum Netz. Die Zugangskontrolle (Admission Control oder auch Connection Admission Control, CAC) sorgt dafür, dass die Verkehrslast im Netz einen vorgegebenen Schwellenwert nicht überschreitet. Der Priorisierungsmechanismus kategorisiert den Verkehr entsprechend der Priorität der Pakete und sorgt so für eine angemessene Aufteilung der vorhandenen Ressourcen. Die Medienzugriffssteuerung dient der effizienten Nutzung des Mediums. Diese drei Mechanismen sind also ausreichend, um QoS bereitzustellen. Störungen von außerhalb (beispielsweise durch andere Geräte, die dasselbe Frequenzband nutzen) können aber trotzdem eine Degradation der Dienstgüte zur Folge haben.

In dieser Arbeit werden Netze ohne zentrale Steuerungseinheit betrachtet. Deshalb werden im Folgenden dezentrale Mechanismen untersucht. Aufgrund der speziellen Eigenschaften von WMNs, durch die sie sich von anderen drahtlosen Netzen unterscheiden, kann aber von bestimmten Voraussetzungen ausgegangen werden, wie z.B. ausreichende Konnektivität, weitgehend statisches Netz, viele stationäre Knoten.

2.2.4 Mechanismen

Im Folgenden werden die Funktionsweise und grundlegende Eigenschaften verschiedener Dienstgütemechanismen erläutert.

Zugangskontrolle (Admission Control)

Wenn jede Station unbeschränkt Daten senden darf, stößt die Kapazität des Netzes schnell an ihre Grenzen, insbesondere wenn sich viele Stationen auf engem Raum befinden oder wenn nur wenig Bandbreite zur Verfügung steht. Die Zugangskontrolle sorgt dafür, dass der Verkehr im Netz nicht zu hoch wird. Dazu wird bei jedem neuen Datenstrom, den eine Station senden möchte, überprüft, ob im Netz noch genügend Kapazität vorhanden ist. Ist dies der Fall, darf die Station senden, ansonsten wird der Verkehrsstom zurückgewiesen. So wird dafür gesorgt, dass die Dienstgüte bereits bestehender Datenströme nicht beeinträchtigt wird.

Der Begriff *CAC* (Connection Admission Control) impliziert, dass es sich um verbindungsorientierten Datenaustausch handelt. Wie zu Beginn von Kap. 2 bereits erwähnt, wird hier jedoch von verbindungsloser Kommunikation ausgegangen. Dabei wird für jeden Datenstrom eine Zugangskontrolle durchgeführt, unabhängig von der Form des Datenaustauschs. Die Abkürzung CAC ist demnach nicht ganz eindeutig, wird hier aber trotzdem verwendet, weil sie in diesem Zusammenhang üblich ist.

Um entscheiden zu können, ob ein neuer Verkehrsfluss zugelassen werden kann oder nicht, muss zunächst der Status des Netzes analysiert werden. Kriterien hierfür sind üblicherweise die verfügbare Kapazität oder die Verzögerung, die ein (Test-)Paket erfährt. Beides kann entweder lokal oder entlang der gesamten vorgesehenen Route zwischen Sender und Empfänger bestimmt werden. Anstatt von Testpaketen können auch Datenpakete bereits bestehender Verkehrsströme verwendet werden [18, 36]. Dies reduziert den Overhead, führt aber unter Umständen zu längeren Wartezeiten, bis genügend Informationen über eine Route vorhanden sind.

Keine der genannten Möglichkeiten ist in der Lage, eine genaue Aussage über die Zukunft zu machen. Es werden lediglich Schlussfolgerungen aus der Vergangenheit gezogen und angenommen, dass diese für eine gewisse Zeit gültig sind. Basierend auf den gewonnenen Daten über den aktuellen Zustand des Netzes wird entschieden, ob der neue Verkehrsfluss zugelassen werden kann. Dazu ist eine Datenbank notwendig, anhand derer der aktuelle Zustand mit der jeweils adäquaten Reaktion abgeglichen wird. Wenn mehrere Stationen gleichzeitig anfangen wollen zu senden, oder wenn sich der Zustand des Netzes aufgrund äußerer Einflüsse ändert, kann es zu Fehlentscheidungen kommen. Deshalb ist es sinnvoll, das Netz fortwährend zu überwachen, und falls notwendig laufende Übertragungen abzubrechen [57, 6] oder die Dienstgüte der Verkehrsströme abzusenken [58, 32].

Anstatt den Zustand des Netzes zu überwachen, besteht auch die Möglichkeit, neue Verkehrsflüsse zunächst probehalber zuzulassen [57]. So kann zunächst der Einfluss

auf laufende Datenströme beobachtet werden, bevor endgültig entschieden wird, ob das Netz den zusätzlichen Verkehrsfluss tragen kann oder nicht. Im Zweifelsfall muss die Datenübertragung dann wieder abgebrochen werden. Der Vorteil dieser Methode ist, dass keine Abschätzung notwendig ist, da die Interaktion der einzelnen Verkehrsströme direkt beobachtet werden kann. Allerdings ist es für den Anwender oft unangenehmer, wenn eine Übertragung abgebrochen wird als wenn sie überhaupt nicht zustande kommt. Des Weiteren wird durch das vorläufige Zulassen von Verkehrsflüssen die Qualität der laufenden Übertragungen unter Umständen erheblich degradiert.

Um Fehlentscheidungen zu vermeiden, gibt es auch die Möglichkeit, Ressourcen entlang der Route zu reservieren [58, 32]. Dies hat jedoch den Nachteil, dass alle Knoten entlang der Route Informationen über die Datenströme speichern müssen.

Obwohl die meisten der genannten Mechanismen für Ad-hoc-Netze entworfen wurden, sind sie auch für Mesh-Netze gut geeignet. Es gibt jedoch auch speziell für Mesh-Netze entwickelte Mechanismen, von denen hier auch eine Auswahl vorgestellt werden soll. Da jedoch ein Großteil der Mechanismen für sehr spezielle Szenarien oder Betriebsarten entwickelt wurde, ist eine Verwendung für allgemeine Anwendungsfälle oft nicht sinnvoll.

In [60] wird ein Infrastruktur-WMN betrachtet, wobei davon ausgegangen wird, dass das Netz weitgehend statisch ist. Zwischen den einzelnen Mesh-Knoten wird ein proaktives Routingprotokoll angenommen. Anhand von Testpaketen wird die verfügbare Kapazität entlang einer Route bestimmt, um Entscheidungen über die Zulassung neuer Verkehrsströme treffen zu können. Ein zentraler Aspekt dieses Verfahrens ist jedoch die Verfügbarkeit unterschiedlicher Kanäle für lokalen und weitergeleiteten Verkehr, was von den in Kap. 2.1.3 definierten Voraussetzungen abweicht.

Die Mechanismen in [24] und [37] beruhen beide auf einer zentralen Kontrolleinheit und sind daher in den in dieser Arbeit betrachteten Netzen nicht einsetzbar.

In [34] wird vorgeschlagen, dass jeder Router den Status aller Routen mitloggt. Ein neuer Verkehrsfluss wird zugelassen, wenn der Status der Route, die verwendet werden soll, dies zulässt. Um Inkonsistenzen zu vermeiden, werden Knoten, die eine Reservierungsnachricht erhalten, vorübergehend gesperrt. Eine zweite Reservierungsnachricht für einen anderen Verkehrsstrom kann erst bearbeitet werden, wenn die Entscheidung über den ersten abgeschlossen ist. Dadurch wird die Zahl der fehlerhaften Zulassungen erheblich reduziert, allerdings auch der Overhead erhöht. Diese als *stateful* oder *zustandsbehaftet* bezeichnete Herangehensweise hat den Nachteil, dass nicht nur Quelle und Senke, sondern auch die zwischenliegenden Knoten Informationen über den Zustand der Verkehrsströme speichern müssen. Im Vergleich zu *zustandslosen* (*stateless*) Verfahren wird mehr Speicher und Rechenzeit benötigt, und mit der zusätzlichen Verantwortung, die den einzelnen Knoten übertragen wird, steigt auch die Komplexität der Mechanismen.

Priorisierung

Wie bereits erwähnt (siehe Kap. 2.2.2 und 2.2.3), können in drahtlosen Netzen äußere Einflüsse nicht kalkulierbare Interferenzen verursachen. Deshalb kann keine definitive Aussage über die Menge der verfügbaren Ressourcen getroffen und somit auch keiner Station eine bestimmte Menge an Ressourcen zugesichert werden. Es ist jedoch möglich, die verfügbaren Ressourcen fair zwischen den einzelnen Stationen zu verteilen. Die Grundlage für die Fairness ist hierbei eine Abschätzung, wie viele Ressourcen von den einzelnen Stationen bzw. von den einzelnen Verkehrsströmen benötigt werden. Hierzu dient eine Einteilung in unterschiedliche Verkehrsklassen (siehe auch [76] sowie Kap. 2.2.3). Pakete werden entsprechend ihrer Zugehörigkeit zu einer Verkehrsklasse markiert und dann dementsprechend behandelt. So wird eine Differenzierung der unterschiedlichen Klassen erzielt, indem Pakete mit höherer Priorität bei der Übertragung bevorzugt werden. Verkehrskategorisierung und Priorisierung werden im Folgenden als Synonyme verwendet.

Medienzugriff

Die Medienzugriffssteuerung ist nicht direkt ein Dienstgütemechanismus, da jedes Kommunikationssystem, in dem die Teilnehmer sich ein gemeinsames Übertragungsmedium teilen, ein Medienzugriffsverfahren braucht. Durch effiziente Mechanismen kann jedoch in Bezug auf die Dienstgüte viel erreicht werden. Generell können Medienzugriffsverfahren grob in zwei Kategorien eingeteilt werden: Ein Verfahren mit fester Rahmenstruktur bietet den Vorteil, dass keine Kollisionen auftreten, wodurch geringere Paketverlustraten erzielt werden können. Allerdings müssen hier die Stationen untereinander zeitlich synchronisiert werden, was in Netzen ohne zentrale Kontrolleinheit zusätzlichen Aufwand bedeutet. Bei wettbewerbsbasierten Verfahren (contention based access) senden die Stationen in zufällig gewählten Zeitschlitzen (Slots). Dabei muss nicht nur bestimmt werden, welche Station wann sendet, sondern auch, wie mit Kollisionen umgegangen wird.

Im Folgenden sollen nur wettbewerbsbasierte Verfahren betrachtet werden. Das Verfahren, welches am häufigsten eingesetzt wird, ist das im Standard IEEE 802.11 [63] verwendete CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), siehe Anhang A.2. Es ist folgendermaßen definiert: Wenn eine Station ein Paket zu versenden hat, überprüft sie zunächst, ob der Kanal frei ist. Hierfür wird für eine bestimmte Zeitdauer, dem Interframe Space (IFS), der Signalpegel auf dem Kanal gemessen. Ist der Kanal frei, kann sofort übertragen werden. Ist dies nicht der Fall, muss zuerst die laufende Übertragung abgewartet werden. Im Anschluss daran beginnt der sogenannte Backoffprozess, d.h. die Station wartet zusätzlich eine zufällige Anzahl von Zeitschlitzen, bevor sie mit der Übertragung beginnt. Diese Wartezeit zufälliger Länge verringert die Wahrscheinlichkeit, dass mehrere Stationen gleichzeitig mit der Übertragung beginnen, und damit die Kollisionswahrscheinlichkeit. Zur Bestimmung der Backoffdauer dient die Größe des Zeitfensters (engl.: Contention Window) CW, welches einen minimalen und maximalen Wert annehmen kann ($CW_{\min}$ bzw. $CW_{\max}$).

Diese beiden Werte sind im Standard festgelegt. Anfangs wird der minimale Wert, $CW_{\min}$, verwendet. Wenn eine Kollision stattfindet, was am Ausbleiben einer Quittung (Acknowledgement, ACK) für das gesendete Paket erkannt wird, dann wird das Fenster CW jedesmal verdoppelt, bis es den maximalen Wert $CW_{\max}$ erreicht hat. Nach einer erfolgreichen Übertragung wird der Wert auf $CW_{\min}$ zurückgesetzt. Die Dauer des Backoffs ist eine zufällige Zahl $b \in \{0, 1, \ldots, CW - 1\}$, multipliziert mit der Dauer eines Zeitschlitzes, und demnach abhängig von der Anzahl bereits stattgefundener Kollisionen.

Für die Unterstützung mehrerer Verkehrsklassen definiert IEEE 802.11e [64] unter dem Namen EDCA (Enhanced Distributed Channel Access) eine angepasste Version des Medienzugriffverfahrens. Jede Station verwaltet dazu mehrere Warteschlangen, eine für jede Verkehrsklasse, die sich wie virtuelle Stationen innerhalb der Station verhalten. Die Priorisierung wird erreicht, indem die Warteschlangen unterschiedliche Parameter zur Verarbeitung der Pakete verwenden: Je höher die Priorität, desto kleiner sind Fenstergröße und IFS (siehe auch Anhang A.2).

Ein entscheidender Nachteil von CSMA/CA ist, dass das Verfahren keine Rücksicht auf den Zustand des Netzes nimmt. Zwar wird bei hoher Kanalausnutzung die Fenstergröße vergrößert, jedoch wird sie nach einer erfolgreichen Übertragung wieder auf den ursprünglichen Wert zurückgesetzt. Sinnvoller wäre es, die Parameter an die aktuelle Netzsituation anzupassen. Hier setzt der DCC-Mechanismus (Distributed Contention Control) an [15], ein probabilistischer Ansatz, der die Fairness zwischen den einzelnen Stationen verbessern soll. Basierend auf einer Abschätzung der aktuellen Kanalausnutzung wird die Kollisionswahrscheinlichkeit für das nächste zu sendende Paket berechnet. Abhängig von dieser wird der Übertragungsversuch mit einer gewissen Wahrscheinlichkeit abgebrochen, um anderen Stationen den Zugriff auf den Kanal zu ermöglichen. Dadurch wird die Kanalausnutzung erhöht, indem die Zahl der Kollisionen verringert wird.

Ein Indikator für die Netzauslastung ist die Nutzungsrate der verfügbaren Zeitschlitze, die von jeder Station während ihres Backoff mit Hilfe folgender Formel berechnet werden kann:

$$SU = \frac{Num\_Busy\_Slots}{Init\_Backoff} \tag{2.1}$$

SU steht für Slot Utilization, also die Nutzungsrate der Zeitschlitze, *Num_Busy_Slots* entspricht der Anzahl der Zeitschlitze, die während des letzten Backoff belegt waren, und *Init_Backoff* bezeichnet den Startwert des Backoff-Counters dieser Station. Aus Gleichung 2.1 und der Anzahl erfolgloser Sendeversuche für das aktuelle Paket *Num_Att*, welche die Dringlichkeit des Pakets widerspiegelt, berechnet die Station ihre Sendewahrscheinlichkeit PT:

$$PT(SU, Num\_Att) = 1 - SU^{Num\_Att} \tag{2.2}$$

Bei hoher Netzauslastung ist die Zahl der belegten Zeitschlitze hoch, wodurch sich die Sendewahrscheinlichkeit verringert. Für jeden erfolglosen Sendeversuch in der Vergangenheit wird sie wieder erhöht. So wird bei einer Übertragung der aktuelle Zustand des Netzes berücksichtigt. Der Ablauf ist dabei wie folgt:

```
falls (der Zeitschlitz für die Übertragung ist erreicht)
  dann berechne SU
       bewerte PT
       falls Rnd() < PT
         dann übertrage
         sonst verzichte auf Übertragung
       falls (Verzicht auf Übertragung) oder (Kollision)
         dann Wiederholung des Pakets
```

Eine Erweiterung des DCC-Mechanismus ist eDCC (EDCA Distributed Contention Control) zur Unterstützung mehrerer Verkehrsklassen [30]. Hier wird für jede Sendewarteschlange getrennt die Kollisionswahrscheinlichkeit berechnet und entschieden, ob die Übertragung stattfinden soll oder nicht. Für die Berechnung der Sendewahrscheinlichkeit werden die folgenden Formeln verwendet:

$$SU(i) = \frac{\mathit{Num\_Busy\_Slots}(i)}{\mathit{Init\_Backoff}(i) + 1} \tag{2.3}$$

$$PT(SU(i), \mathit{Num\_Att}(i)) = 1 - SU(i)^{\mathit{Num\_Att}(i)} \tag{2.4}$$

Hierbei bezeichnet i die Priorität der jeweiligen Verkehrsklasse. In Formel 2.3 wird im Nenner 1 addiert, da der Startwert des Backoffs auch 0 sein kann.

Sowohl bei eDCC als auch bei DCC muss ein Kompromiss gefunden werden: Falls die durchschnittliche Sendewahrscheinlichkeit sehr hoch ist (nahe 1), ist der Gewinn, der durch den Mechanismus erzielt werden kann, sehr gering ($PT = 1$ entspricht dem normalen Medienzugriff ohne DCC). Andererseits führt ein niedriger Wert für PT dazu, dass viele Zeitschlitze frei bleiben, also Kapazität verschwendet wird.

Routing

Routing, auf Deutsch auch Verkehrslenkung, bezeichnet in einem Kommunikationsnetz das Aussuchen von Pfaden, auf denen Daten von einem Sender zu einem Empfänger geleitet werden. Die Route wird anhand einer Metrik ausgewählt. Hierfür gibt es verschiedene Möglichkeiten: Beispielsweise kann der kürzeste Pfad gewählt werden, oder derjenige, der am wenigsten ausgelastet ist. Bei Transitnetzen spielen auch die finanziellen Kosten für die Nutzung eine Rolle. Diese werden anhand von Verträgen zwischen den Netzbetreibern festgesetzt [43].

In drahtlosen Netzen unterscheidet man hauptsächlich zwei grundsätzliche Klassen von Routingprotokollen [61]:

Proaktive Routingprotokolle: Jede Station speichert Informationen über alle verfügbaren Routen in einer Routingtabelle, die regelmäßig aktualisiert wird. Dadurch werden kürzere Reaktionszeiten ermöglicht, da die benötigte Route bereits bekannt ist, bevor Daten versendet werden. Andererseits ist für die Routingtabelle viel Speicherplatz notwendig, und ihre Aktualisierung erzeugt zusätzlichen Verkehr. Proaktive Protokolle sind deshalb bei relativ statischen Netzen sinnvoll, weil die Abstände zwischen den Aktualisierungen dann größer gewählt werden können. Außerdem bringen sie Vorteile in Netzen und Szenarien, in denen ein möglichst schneller Datenversand wichtig ist.

Der bekannteste Vertreter proaktiver Routingprotokolle ist Destination Sequenced Distance Vector Routing (DSDV).

Reaktive Routingprotokolle: Hierbei werden Routen erst dann angelegt, wenn sie tatsächlich gebraucht werden. Dadurch entsteht vor dem Senden eine gewisse Verzögerung, da erst eine Route zum Empfänger gefunden werden muss. Andererseits bedeutet es jedoch weniger Speicherbedarf und weniger zusätzlichen Verkehr. Reaktive Protokolle lohnen sich bei Netzen, die sich häufig ändern, da dort der Aufwand, um die Routingtabelle aktuell zu halten, unverhältnismäßig hoch wäre.

Das bekannteste Beispiel für reaktive Routingprotokolle ist Ad hoc On-demand Distance Vector Routing (AODV).

Routing ist an sich kein Dienstgütemechanismus, kann aber abhängig von der gewählten Metrik einen Beitrag zur Dienstgüte leisten. In einigen QoS-Architekturen (siehe Kap. 2.2.5) wird es deshalb mit behandelt, insbesondere im Zusammenhang mit CAC, da dort zusätzliche Verbesserungen möglich sind, wenn Routing mit in den Entscheidungsprozess einbezogen wird. Dazu ist allerdings eine schichtenübergreifende Betrachtung notwendig.

Im Folgenden wird Dienstgüte unabhängig vom Routing betrachtet.

Beamforming

In zellularen Mobilfunknetzen werden gerichtete Antennen bereits seit längerer Zeit eingesetzt, aber inzwischen sind sie auch für Ad-hoc- und Mesh-Netze interessant geworden [4, 52]. Der Standard IEEE 802.11n [65] beispielsweise spezifiziert den Einsatz von Antennenarrays optional für MIMO (Multiple Input Multiple Output) oder Beamforming.

Geräte mit mehreren Antennenelementen (engl.: antenna array oder phased array) bieten die Möglichkeit, durch gezielte Ansteuerung der einzelnen Elemente gerichtete Sendesignale abzustrahlen. Die einzelnen Signale überlagern sich dabei so, dass

sie in bestimmte Richtungen verstärkt werden oder sich gegenseitig aufheben. Durch geeignete Signalverarbeitungsmechanismen können diese sogenannten intelligenten Antennen so angesteuert werden, dass die Abstrahlungsrichtung variiert werden kann (Beamforming). Dies ist im Mikrosekundenbereich möglich, kann also ausgenutzt werden, um vor jeder Datenübertragung die Antenne neu auszurichten. Dadurch kann die erzielbare Datenrate oder die Sendereichweite erhöht werden, während die Interferenz verringert wird.

Um Beamforming in der Praxis nutzen zu können, sind spezielle Medienzugriffsverfahren notwendig [51]. Ein einfaches Beispiel wäre, dass eine Station vor jeder Datenübertragung die Hauptabstrahlungsrichtung auf den jeweiligen Empfänger ausrichtet. Dadurch wird die Signalleistung in diese Richtung erhöht und damit auch der Signal-zu-Interferenz-und-Rauschabstand (SINR). Die Voraussetzung dafür ist allerdings, dass die Position des Empfängers bekannt ist. Dazu muss vorher bereits ein Datenaustausch (Nutzdaten oder entsprechende Testpakete) stattgefunden haben, um eine Ausrichtung zu ermöglichen.

Beamforming bietet diverse Möglichkeiten, die Dienstgüte zu verbessern:

- Erhöhung der Sendereichweite und dadurch Verbesserung der Konnektivität
- Möglichkeit der Ausblendung von Störsignalen
- Verringerung der Sendeleistung und dadurch Verlängerung der Lebensdauer von batteriebetriebenen Geräten
- SINR-Erhöhung und damit Ermöglichung höherer Datenraten

Zugleich müssen allerdings auch die Nachteile betrachtet werden:

- Das Equipment ist teurer und aufwändiger in der Wartung. Zusätzlich unterliegt es dabei hohen Anforderungen in Bezug auf die Präzision.
- Die Mechanismen zur Ansteuerung der Antennenelemente sind komplex und erfordern daher zusätzliche Rechenleistung.
- Die Größe einer solchen intelligenten Antenne, also der räumliche Abstand der einzelnen Antennenelemente, ist von der verwendeten Frequenz abhängig. Für kleine Endgeräte ist die Technologie deshalb nicht anwendbar.
- Die Funktionalität kann nur dann voll ausgenutzt werden, wenn ein geeignetes Medienzugriffsverfahren eingesetzt wird, was zusätzlichen Aufwand bedeutet.

Die in dieser Arbeit beschriebenen Mechanismen erlauben den Einsatz von Beamforming, im Folgenden soll jedoch nicht speziell darauf eingegangen werden.

2.2.5 Existierende Lösungsansätze für QoS-Architekturen

In der Literatur gibt es verschiedene Ansätze für dezentrale Architekturen, um Dienstgüte für drahtlose Netze bereitzustellen. Einige Vertreter sollen im Folgenden kurz beschrieben werden. Die jeweiligen Vor- und Nachteile sind in Tab. 2.2 dargestellt.

INSIGNIA [32] ist eine IP-basierte QoS-Architektur, welche Ressourcenallokation, Ressourcenreservierung, Zugangskontrolle und Routing umfasst. Der Inband-Signalisierungsmechanismus sorgt für geringen Overhead und ist für schnelle Reservierung und Anpassungen geeignet, weswegen auch sehr dynamische Netze unterstützt werden können. Mit Hilfe von Testpaketen werden auf allen Knoten entlang der Route Ressourcen reserviert. Die maximal mögliche Dienstgüte in jedem Knoten wird dabei jeweils gespeichert und von der Senke an die Quelle übermittelt. Die Quelle informiert dann alle Zwischenknoten über den tatsächlich genutzten QoS-Level. Durch die gesendeten Datenpakete werden die Reservierungen aufgefrischt, und sie altern aus, wenn keine Daten mehr gesendet werden. Prinzipiell können alle Verkehrsströme zugelassen werden, unter Umständen jedoch mit einem geringeren QoS-Level als gewünscht. Im Fall von Überlast werden die betroffenen Pakete entsprechend markiert, und die Senke informiert die Quelle. Diese kann die Datenrate senken oder die Übertragung stoppen. Eine Zurückstufung auf einen niedrigeren QoS-Level ist ebenfalls möglich. Bestehende Verkehrsströme bekommen hierbei immer Vorrang. Es kann jedoch passieren, dass die Dienstgüte kurzzeitig abgesenkt wird, während ein neuer Verkehrsstrom zugelassen wird.

Die Architektur ist zwar flexibel und unterstützt Mobilität, Nachteile sind aber einerseits die Ansiedlung auf der Vermittlungsschicht sowie die Tatsache, dass Zwischenknoten Informationen über die einzelnen Verkehrsflüsse speichern müssen.

SWAN (Service Differentiation for Stateless Wireless Ad hoc Networks) [6] definiert für Echtzeitverkehr einen Zugangskontrollmechanismus, während für Best-Effort-Verkehr Rate Control verwendet wird, also eine Regelung der Datenrate. Um auf Mobilität und Fehler reagieren zu können, wird ECN (Explicit Congestion Notification) eingesetzt. Im Fall von Überlast an einem Knoten markiert dieser Mechanismus die Pakete eines der betroffenen Verkehrsströme, sodass die Quelle den Verkehrsstrom stoppen kann.

Vorteile der Architektur sind die Möglichkeit der Kombination mit beliebigen MAC- und Routingverfahren, sowie die Tatsache, dass Zwischenknoten keine Informationen über die Verkehrsflüsse speichern müssen. Als Nachteile sind zu nennen, dass die Architektur nicht auf der MAC-Schicht arbeitet und nur zwei Verkehrsklassen unterstützt.

MPARC (Multi-Priority Admission and Rate Control) [58] kombiniert ähnlich wie SWAN Zugangskontrolle für Echtzeitverkehr mit Rate Control für Best-Effort-

Verkehr. Außerdem wird Priorisierung für verschiedene Verkehrsklassen verwendet. Diese unterscheiden sich in Fenster- und Paketgröße. Alle Pakete, die von einem Knoten ausgesendet werden, gehören dabei derselben Verkehrsklasse an. Um eine bessere Vorhersage über den Einfluss eines neuen Verkehrsstroms auf bereits bestehende treffen zu können, wird nicht nur der Verkehr in der direkten Umgebung bei der Zulassungsentscheidung berücksichtigt, sondern alles im Umkreis von drei Hops. Dazu senden alle Knoten regelmäßig Benachrichtigungen an ihre Nachbarn, um sie und deren Nachbarn über aktuelle Verkehrslast und verwendete Fenstergröße und Paketgröße zu informieren. Auf dieser Basis sind sehr genaue Entscheidungen bezüglich der Zulassung eines Verkehrsflusses möglich, und es wird sichergestellt, dass den benachbarten Knoten nicht zu viele Ressourcen weggenommen werden. In allen Knoten entlang der Route werden Ressourcen für die einzelnen Verkehrsflüsse reserviert. Wenn die Verkehrslast im Netz steigt, wird die Dienstgüte für Verkehr mit niedriger Priorität abgesenkt. MPARC ist zwar unabhängig vom Routingprotokoll, greift jedoch auf Informationen wie beispielsweise die Anzahl der Zwischenknoten auf einer Route zurück.

Nachteile der Architektur sind der große Overhead durch Signalisierungsnachrichten, da nicht nur die direkten Nachbarn, sondern auch weiter entfernte Knoten über die aktuelle Verkehrslast informiert werden müssen, sowie die Tatsache, dass alle Knoten entlang einer Route Informationen über die einzelnen Verkehrsströme speichern müssen. Dafür können die Einflüsse auf bestehende Verkehrsflüsse sehr genau bestimmt werden.

QPART (QoS Protocol for Ad hoc Realtime Traffic) [57] ist ein schichtenübergreifender Ansatz, welcher Zugangskontrolle, Ressourcenallokation und Konfliktbewältigung umfasst. Alle neuen Verkehrsströme werden zunächst zugelassen. Im ersten Datenpaket eines Verkehrsstroms sind Informationen über die QoS-Anforderungen enthalten, die von allen Zwischenknoten gespeichert werden. Die Zwischenknoten verwenden dynamische Priorisierung, um die Anforderungen in Bezug auf Verzögerung und Durchsatz zu erfüllen. Dazu werden auf der Vermittlungsschicht Zeitfenster eingeführt, deren Größe abhängig von der Verkehrslast und den Realzeitanforderungen der einzelnen Verkehrsströme bestimmt wird. Wenn die Verkehrslast steigt, werden beim Hintergrundverkehr die Fenster vergrößert, um den Realzeitverkehr nicht zu behindern. Da alle Verkehrsflüsse zugelassen werden, muss auf Überlast adäquat reagiert werden können. Dazu bestimmt jeder Knoten den Anteil der Zeit, in der der Kanal frei ist (Channel Idle Time Ratio, CITR). Wenn dieser unter eine bestimmte Schwelle fällt, werden die neuesten Verkehrsströme abgebrochen. Das führt dazu, dass neue Verkehrsströme kurzzeitig die Dienstgüte für bestehende Übertragungen absenken können, bevor erkannt wird, dass nicht mehr genügend Kapazität zur Verfügung steht.

Durch das probeweise Zulassen aller neuen Verkehrsflüsse wird Overhead vermieden, da keine Testpakete oder zusätzlichen Benachrichtigungen benötigt

werden. Die Nachteile dieser Architektur sind allerdings die starke Abhängigkeit sowohl von MAC- als auch Routingverfahren, sowie die Tatsache, dass alle Knoten Informationen über die einzelnen Verkehrsflüsse speichern müssen.

Tabelle 2.2: Vergleich existierender QoS-Architekturen

Name	INSIGNIA	SWAN	MPARC	QPART	DARMA
verteilt	✓	✓	✓	✓	✓
zustandslos	–	✓	–	–	✓
geringer Overhead	✓	✓	–	✓	✓
unabhängig vom Routing	–	✓	–	–	✓
unterstützt 802.11e	✓	–	✓	✓	✓
auf Schicht 2	–	–	–	–	✓

In der letzten Spalte der Tabelle ist die in dieser Arbeit vorgestellte Architektur, DARMA (siehe Kap. 3), eingetragen.

Die oben beschriebenen Architekturen liefern zwar sehr gute Ergebnisse, sind dabei aber auf sehr spezielle Szenarien festgelegt. Wie in Tab. 2.2 dargestellt, unterstützt auch keine der Architekturen alle für WMNs essentiellen Kriterien. Bei der Konzeption von DARMA wurde deshalb besonderer Wert auf Flexibilität, Kompatibilität und Kombinationsfähigkeit mit bestehenden Systemen, sowie geringe Komplexität gelegt. Diese Punkte steigern die Akzeptanz unter den potenziellen Nutzern und bieten Anreize für Netzbetreiber, die Architektur einzusetzen.

2.3 Management von drahtlosen Netzen

Ad-hoc-Netze und auch WMNs sind weitgehend selbstorganisierend: Die Mechanismen sind so gewählt, dass Teilnehmer beitreten oder das Netz verlassen können und dass mit Fehlern wie z.B. Unterbrechungen der Funkverbindung umgegangen werden kann, ohne dass Eingriffe durch Menschen notwendig sind. Für den Betreiber eines Netzes ist es jedoch generell vorteilhaft, wenn eine zusätzliche Kontrollebene in Form eines Managementsystems im Netz vorhanden ist. Der Begriff *Management* lässt sich hierbei in zwei grundsätzliche Aspekte unterteilen:

Extraktion von Informationen über das Netz Für den Betreiber eines Netzes ist es oft von Interesse, eine Möglichkeit zu haben, Informationen über sein eigenes Netz zu erhalten, wie z.B. Anzahl und Fluktuation der Teilnehmer, Auslastung, Art des Verkehrs, etc. Dazu ist es einerseits notwendig, dass das Netz diese Informationen sammelt und bereitstellt, und andererseits wird eine Schnittstelle benötigt, um darauf zugreifen zu können.

Eingriff in die Funktion des Netzes Speziell für Ad-hoc- und Mesh-Netze entwickelte Routing- und Medienzugriffsverfahren sind zwar in gewissem Umfang

in der Lage, ohne äußere Eingriffe auf Änderungen und Fehler zu reagieren, manchmal lässt sich die Leistung des Netzes jedoch erhöhen, indem Parameter während des Betriebs angepasst werden. Dies kann entweder durch einen Netzadministrator geschehen, oder automatisiert auf Basis von Datenbanken.

Allgemein lassen sich fünf verschiedene Bereiche des Netzmanagement unterscheiden [53]: Fehler-, Konfigurations-, Abrechnungs-, Leistungs- und Sicherheitsmanagement. Die Grenzen dazwischen sind nicht immer eindeutig, da viele Ereignisse, die im Netz auftreten können, für mehrere Bereiche relevant sind.

In dieser Arbeit ist das Management nicht als notwendige Grundlage für das Netz gedacht, sondern als Erweiterung zur Verbesserung der Funktionalität. Dabei liegt der Fokus auf Konfigurations- und Leistungsmanagement. Fehlermanagement ist vom Konfigurationsmanagement teilweise mit abgedeckt, Sicherheit ist in dieser Arbeit nicht vordergründig, und Abrechnung ist in den betrachteten Netzen üblicherweise nicht notwendig. Ein Teil des Abrechnungsmanagements, der sich um Nutzerstatistiken kümmert, wird hier mit dem Konfigurationsmanagement zusammengefasst.

2.3.1 Clusteringalgorithmen

Für einige Management- und auch sonstige Aufgaben bietet es sich an, das Netz in Cluster zu unterteilen. Dazu gibt es verschiedene Möglichkeiten (siehe z.B. [11, 10, 17, 41, 20]).

Allgemein ist es notwendig, dass jeder Knoten im Netz eine eindeutige Kennung hat. Das kann z.B. die MAC-Adresse sein oder auch eine eigens zugeteilte Nummer. Jedes Cluster besteht aus einem Clusterhead (CH) und einer variierenden Anzahl von Teilnehmern. Die Clusterheads verwalten Daten der Teilnehmer und sind für die Clusterbildung zuständig. Sowohl die Auswahl der Clusterheads als auch die Zuordnung von Teilnehmern zu CHs kann anhand verschiedener Kriterien erfolgen.

Positionsbasiertes Clustering

Hierbei erfolgt die Clustereinteilung anhand von geographischen Gesichtspunkten: Die Fläche des Netzes wird in einzelne Teile aufgeteilt, und jeder Knoten wird dem Cluster zugeordnet, auf dessen Gebiet er sich befindet [20]. Dazu ist es notwendig, dass die einzelnen Knoten in der Lage sind, ihre Position zu bestimmen (beispielsweise mit Hilfe von GPS). Bei der Aufteilung der Cluster kann beispielsweise die Verteilung der Knoten mit berücksichtigt werden, sodass jedes Cluster ähnlich viele Teilnehmer hat. Eine andere Möglichkeit ist, Cluster zu bilden, deren Fläche in etwa gleich groß ist, was in mobilen Netzen dazu führt, dass die durchschnittliche Anzahl der Knoten pro Cluster über die Zeit relativ konstant ist. Nachdem die Zuordnung der Stationen zu den einzelnen Clustern erfolgt ist, wählt jedes Cluster einen Clusterhead. Dies kann anhand der Kennung geschehen oder anhand eigener Metriken, die beispielsweise die Akkulaufzeit mit berücksichtigen [27].

Topologiebasiertes Clustering

Im Gegensatz zum geographischen Clustering werden hier zuerst die Clusterheads bestimmt, und danach erfolgt die Zuteilung der Knoten zu den einzelnen CHs. In [20] und [11] wird gezeigt, dass es sinnvoll ist, wenn sich alle Teilnehmer in Sendereichweite ihres CHs befinden, damit der Verkehr zwischen ihnen nicht über Zwischenknoten weitergeleitet werden muss. Meistens wird vorausgesetzt, dass jeder Knoten eine Liste aller seiner Nachbarn pflegt. Derjenige Knoten mit der niedrigsten Kennung unter allen Nachbarn (bzw. unter allen Nachbarn, die noch keinem Cluster angehören) ernennt sich selbst zum CH. Alle anderen Stationen in der Umgebung schließen sich dann diesem Cluster an. Statt der Kennung kann auch hier eine Metrik verwendet werden, die die Eignung des Knotens als Clusterhead widerspiegelt.

2.3.2 Existierende Managementprotokolle

Für Festnetze gibt es standardisierte Protokolle, die das Netzmanagement im Sinne von Überwachung und Steuerung übernehmen. Dazu gehört das Sammeln und Bündeln von Informationen sowie die Reaktion auf bestimmte Ereignisse anhand von Datenbanken. Beispiele für solche Protokolle sind das Simple Network Management Protocol (SNMP) der IETF [72] und das Common Management Information Protocol (CMIP) der ITU [71, 69].

Daneben gibt es zahlreiche Erweiterungen, beispielsweise um in heterogenen Netzen ein gemeinsames Managementinterface bereitzustellen [28] oder um den Zugriff über HTTP (Hypertext Transfer Protocol) und demnach von außerhalb über das Internet zu ermöglichen [28, 33]. Insbesondere in großen Netzen kann es von Vorteil sein, statt einer zentralen Datenbank ein verteiltes Managementsystem zu verwenden [33, 31, 9].

Simple Network Management Protocol

SNMP ist der wichtigste Vertreter der Managementprotokolle und am weitesten verbreitet. Im Folgenden soll deshalb kurz die grobe Struktur beschrieben werden (siehe auch [53, 39]). SNMP besteht aus drei Komponenten:

Überwachte Geräte haben eine SNMP-Schnittstelle und erlauben dadurch Zugriff auf knotenspezifische Informationen. Dieser Zugriff kann entweder unidirektional (nur Auslesen von Informationen) oder bidirektional (Lesen und Ändern der Informationen) sein.

Agenten sind spezielle Programme, die auf den überwachten Geräten laufen und die Schnittstelle zum Managementsystem bilden. Sie beobachten den Zustand des Geräts und ermöglichen die Kommunikation mit dem Manager.

(Zentrale) Managementstationen sind Geräte, die das Netz überwachen und mit Hilfe definierter Nachrichten Informationen der überwachten Geräte abrufen

und gegebenenfalls ändern. Üblicherweise gibt es eine Managementstation pro Netz, es kann aber auch mehrere geben, die verschiedene Aufgaben haben.

In Form einer virtuellen Datenbank (Management Information Base, MIB) ist definiert, welche Informationen verfügbar sind und abgerufen werden können. Dies ist nicht Teil des eigentlichen Protokolls, sondern kann für das jeweilige Anwendungsgebiet entsprechend definiert werden. Alle Daten in der MIB sind durch *Object Identifier* (OIDs) eindeutig identifiziert.

Für das Abrufen und Ändern der Daten stellt SNMP spezielle Nachrichten bereit. Diese sind *GetRequest* zum Auslesen von Daten, *SetRequest* zum Ändern von Daten, *GetNextRequest* und *GetBulkRequest* zum gleichzeitigen Auslesen mehrerer Datenwerte, *Response* als Antwort auf die zuvor genannten Nachrichten, *InformRequest* und *Trap* zum asynchronen Senden von Informationen (ohne vorherige Aufforderung).

Managementsysteme für drahtlose Netze

Die grundlegende Funktionalität von Managementprotokollen kann für drahtlose Netze genauso genutzt werden. Üblicherweise stehen jedoch nur in begrenztem Umfang Bandbreite und Rechenleistung zur Verfügung, weshalb effizientere Lösungen zur Datenaggregation gefunden werden müssen [20]. Das gilt insbesondere für Netze mit unzuverlässigen Funkverbindungen, sei es durch hohe Mobilität oder Fluktuation der Teilnehmer oder durch äußere Störeinflüsse.

In [31] wird als Basis IPv6 verwendet, um mobile Teilnehmer unterstützen zu können. Das in [42] beschriebene Managementmodell geht von einer zentralen Steuerungseinheit aus. Es eignet sich insbesondere für Weitverkehrsnetz (WAN), wie beispielsweise im Standard IEEE 802.16 [67]. Das ANTLER-Protokoll [38] für WLANs reduziert im normalen Betriebsfall die Menge der erfassten Daten auf ein Minimum. Erst wenn eine Störung erkannt wird, werden in kürzeren Intervallen Informationen gespeichert.

Im Bereich drahtloser Sensornetze gibt es eine Vielzahl von Protokollen, deren Hauptaufgabe darin besteht, Informationen zu sammeln und weiterzuleiten. Das Ad hoc Network Management Protocol (ANMP) [20] ist dem bereits erwähnten SNMP [72] nachempfunden und erweitert dieses um einige für Ad-hoc-Netze relevante Parameter. Aufgrund der Kompatibilität zu SNMP kann es in hybriden Netzen eingesetzt werden. Das in [16] beschriebene System hat als Ziel, eine lückenlos fortwährende Beobachtung der Umgebung zu gewährleisten. Dabei wird auch besonderer Wert auf Datensicherheit gelegt. Das in [19] beschriebene Policy-basierte Managementsystem ist sehr flexibel und einfach zu administrieren, erfordert jedoch im Vorfeld einen hohen Planungsaufwand und braucht mehr Ressourcen als andere, vergleichbare Protokolle. Das Sensor Network Management System (SNMS) [49] ist ein stark spezialisiertes System, welches nur geringen Funktionsumfang bietet, dafür aber nur sehr wenige Ressourcen benötigt. Es eignet sich deshalb für den Einsatz in Sensornetzen mit extrem eingeschränkten Ressourcen.

In der vorliegenden Arbeit soll das Managementsystem dafür genutzt werden, den Status des Netzes zu überwachen, gleichzeitig aber auch in der Lage sein, in die Funktion der Dienstgütemechanismen einzugreifen. Deshalb wird im Folgenden eine Architektur entworfen, die Dienstgüte und Management miteinander kombiniert und dadurch flexibel auf den Zustand des Netzes reagieren kann. So ist die Architektur in verschiedensten Szenarien einsetzbar und kann sich an die jeweiligen Gegebenheiten anpassen.

3 Architektur zur Bereitstellung von Dienstgüte

Die meisten Dienstgütemechanismen sind für sehr spezielle Anwendungsfälle und/oder Szenarien entwickelt und liefern für diese Fälle optimale Ergebnisse. WMNs sind jedoch vielfältig einsetzbar. Um nicht für jedes Anwendungsgebiet eigene Mechanismen und Protokolle bereitstellen zu müssen, bietet sich in WMNs der Einsatz einer flexiblen QoS-Architektur an. Diese soll sowohl für verschiedene Szenarien geeignet sein, als auch während des Betriebs dynamisch an die aktuellen Gegebenheiten und Anforderungen (sowohl betreiber- als auch nutzerseitig) angepasst werden können. Aufgrund der Struktur von WMNs soll die Architektur außerdem verteilt arbeiten, also ohne zentrale Steuerungseinheit auskommen.

Kriterien für das Design der Architektur sind demnach:

- Flexibilität – Die Mechanismen sollen für eine breite Auswahl an Szenarien und Betriebszuständen geeignet sein.
- Dezentrale Steuerung – Da in WMNs keine zentrale Steuerungseinheit vorhanden ist, sollen die Mechanismen ohne eine solche auskommen.
- Kompatibilität – Die Architektur soll in bestehenden drahtlosen Netzen eingesetzt werden können und einfach nachzurüsten sein.
- Geringer Overhead – Da in drahtlosen Netzen generell wenige Ressourcen zur Verfügung stehen, sollen diese möglichst effizient genutzt werden.
- Modularität – Die Architektur soll sich auf Schicht 2 des OSI-Modells beschränken und somit unabhängig vom Routingmechanismus sein. Dadurch kann sie mit verschiedenen Routingverfahren kombiniert werden.

Die im Folgenden vorgestellte QoS-Architektur *DARMA* (Distributed Adaptive Resource Management Architecture) [3] erfüllt diese Anforderungen.

Ein Überblick über die Architektur ist in Abb. 3.1 zu sehen: Die einzelnen Komponenten, die notwendig sind, um QoS zu gewährleisten, wurden in Kap. 2.2.4 schon kurz vorgestellt und sollen in den folgenden Kapiteln noch näher erläutert werden. Das Bild stellt die Abläufe auf der Sicherungsschicht (Schicht 2 des OSI-Modells) eines einzelnen Knotens beim Versenden eines Pakets dar. Das Paket wird zunächst von der Vermittlungsschicht entgegengenommen. Falls es zu einem Datenstrom gehört, der bereits zugelassen wurde, wird es entsprechend seiner Verkehrsklasse vom

Medienzugriffsverfahren bearbeitet und verschickt. Handelt es sich um eine Anfrage für einen neuen Datenstrom, wird zunächst überprüft, ob ausreichend Ressourcen verfügbar sind. Daraufhin wird der Verkehrsstrom entweder zugelassen oder abgelehnt. Erst dann können Pakete versendet werden.

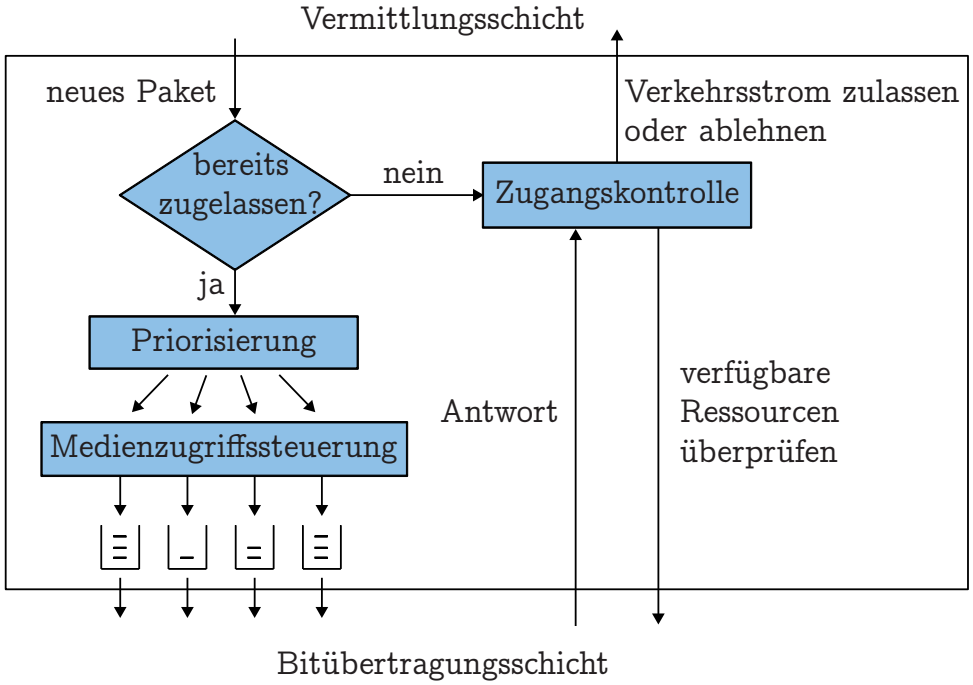


Abbildung 3.1: Distributed Adaptive Resource Management Architecture (DARMA)

3.1 Basiskomponenten

Im Folgenden werden die Dienstgütemechanismen, aus denen DARMA sich zusammensetzt, näher erläutert.

3.1.1 Zugangskontrolle

Ein vermaschtes drahtloses Netz lebt davon, dass viele Stationen teilnehmen, weil so die Reichweite und Konnektivität erhöht werden. Stationen werden außerdem zum Weiterleiten von Nachrichten benötigt. So gesehen ist es von Vorteil, möglichst viele Stationen im Netz zu haben, und demnach einzelnen Stationen den Zugang zum Netz nicht zu verwehren (der Sicherheitsaspekt sei an dieser Stelle außen vor gelassen). Den größten Nutzen für das Netz bringt jedoch eine Station, die Pakete

nur weiterleitet und keine eigenen Daten sendet. Deshalb soll hier unter Zugangskontrolle nicht der physikalische Zugang zum Netz (Authentifizierung) verstanden werden, sondern vielmehr die Erlaubnis, Daten zu senden. Indem nur so viele aktive Datenübertragungen zugelassen werden, wie vom Netz verarbeitet werden können, wird Überlastung und Verkehrsstau vermieden, und somit auch die Degradation der Dienstgüte. Da es keine zentrale Kontrolleinheit gibt, die den Datenverkehr überwachen kann, ist hier jede Station selbst dafür zuständig, zu entscheiden, ob ein Verkehrsstrom gestartet werden kann, d.h. ob genügend Ressourcen zur Verfügung stehen.

Die grundlegenden Aufgaben eines CAC-Mechanismus wurden in Kap. 2.2.4 erklärt. Die Vor- und Nachteile der einzelnen Methoden zur Statusbestimmung des Netzes sind in Tab. 3.1 noch einmal dargestellt.

Tabelle 3.1: Methoden zur Statusbestimmung

	Vorteile	Nachteile
Kapazität	direkter Bezug	maximal verfügbare Kapazität muss bekannt sein
Verzögerung	einfacher zu bestimmen	starke Schwankungen, keine genaue Messung möglich
lokal	einfacher	ungenauer
Ende-zu-Ende	Informationen über die ganze Route	Testpakete notwendig

Designkriterien

Wie zu Beginn von Kap. 3 bereits erwähnt, soll die Architektur modular sein und möglichst geringe Komplexität aufweisen, sodass sie einfach auf bestehenden Systemen implementiert werden kann. Die einzelnen Mechanismen werden nach diesen Kriterien ausgewählt. Zugangskontrollmechanismen lassen sich nach den folgenden Eigenschaften unterscheiden:

Kopplung an das Routingprotokoll Wenn der CAC-Mechanismus Zugriff auf das Wissen des Routingprotokolls hat und umgekehrt, können Ressourcen besser verwaltet werden: So kann bereits beim Finden der Route sichergestellt werden, dass diese die QoS-Anforderungen erfüllt. Dadurch wird die Zugangskontrolle schneller und effizienter. Entkoppelte CAC-Mechanismen sind hingegen weniger komplex und gleichzeitig flexibler, da sie mit unterschiedlichen Routingprotokollen kombiniert werden können. *Aufgrund der Modularität der QoS-Architektur soll der CAC-Mechanismus vom Routing unabhängig sein.*

Kopplung an das MAC-Protokoll Die Vor- und Nachteile sind hier ähnlich wie bei der Kopplung mit dem Routing: Benötigte Parameter, wie beispielsweise die Zeit, in welcher der Kanal frei ist (Channel-Idle-Time), können bei gekoppelten Mechanismen direkt weiterverwendet werden. Die Entkopplung hat den Vorteil, dass verschiedene MAC-Verfahren genutzt werden können. *Da hier nur ein MAC-Verfahren betrachtet wird, ist eine Kopplung problemlos möglich.*

Zustandslos vs. zustandsbehaftet Hiermit ist die Frage gemeint, ob Knoten entlang einer Route Informationen über einen bestehenden Verkehrsfluss speichern oder nicht. Wenn in zwischenliegenden Knoten Informationen vorhanden sind (zustandsbehaftet, stateful), kann auf Änderungen der Netzsituation schneller adäquat reagiert werden. Außerdem ist nur so eine Reservierung von Ressourcen möglich. Andererseits wird dafür zusätzlicher Speicherplatz benötigt, und es ist notwendig, alle Knoten entlang einer Route über bestehende Verkehrsflüsse zu informieren, diese Informationen aktuell zu halten und bei Beenden einer Datenübertragung wieder zu löschen. Die andere Variante (zustandslos, stateless) hat demnach erheblich weniger Overhead, sowohl in Bezug auf Speicher als auch Datenaustausch, hat weniger Anforderungen an die zwischenliegenden Knoten (das kann auch in Bezug auf Datensicherheit relevant sein!) und kann in bestehenden Netzen einfacher nachträglich implementiert werden. *Wie in Kap. 2.2.3 aufgezeigt wurde, ist Ressourcenreservierung in dieser Architektur nicht vorgesehen. Deshalb kann hier die Variante gewählt werden, in der die Zwischenknoten keine Informationen speichern müssen.*

Umgang mit neuen Verkehrsströmen Allgemein gibt es zwei verschiedene Möglichkeiten, um über neue Verkehrsströme zu entscheiden:

1. Der CAC-Mechanismus bestimmt den Zustand des Netzes entweder passiv oder durch das Verschicken von Testpaketen. Die daraus erhaltenen Informationen werden genutzt, um zu entscheiden, ob für den neuen Verkehrsstrom ausreichend Ressourcen vorhanden sind.

2. Der CAC-Mechanismus lässt zunächst alle Verkehrsströme zu, beobachtet das Netz weiter, und entscheidet erst im Anschluss, ob der neue Verkehrsstrom unterstützt werden kann oder wieder abgebrochen werden muss, bzw. ob er mit weniger Ressourcen als gewünscht zurechtkommen muss.

Während die erste Methode deutlich ungenauer ist, da sie nur Abschätzungen über den künftigen Zustand des Netzes machen kann, führt die zweite Methode unter Umständen zu einer Degradation der Dienstgüte für bestehende Verkehrsströme. *Beide Vorgehensweisen haben Vor- und Nachteile. Im Rahmen dieser Arbeit wird die erste Methode betrachtet, da Beeinträchtigungen und Abbruch bestehender Verkehrsströme von Nutzern üblicherweise als störender empfunden werden, als wenn keine Datenübertragung zustande kommt.*

Metrik für die Beurteilung des Netzzustandes Es gibt unterschiedliche Methoden,

um den Zustand des Netzes zu messen. Die meisten CAC-Mechanismen verwenden eines der folgenden Kriterien:

- Der Anteil der Zeit, die der Kanal frei ist (Channel Idle Time Ratio, CITR), wird an jedem Knoten überwacht. Das Minimum entlang der Route wird als Referenzwert verwendet.
- Jeder Knoten entlang der Route schätzt ab, wieviel Kapazität momentan verwendet wird. Dieser Wert wird von der insgesamt verfügbaren Kapazität abgezogen, und wiederum das Minimum entlang der Route verwendet.
- Die Zwischenankunftszeiten von Testpaketen fester Länge werden gemessen, um anhand der Verzögerung die freie Kapazität abzuschätzen.

Die erste Methode ist die einfachste, da sie komplett lokal durchgeführt werden kann und kein Vorwissen erfordert. Die Bestimmung der Restkapazität kann auf verschiedene Arten erfolgen und ist auch lokal möglich, erfordert aber Informationen über die insgesamt verfügbare Kapazität. Das Versenden von Testpaketen bedeutet zusätzlichen Overhead für das Netz, führt aber meistens auch zu genaueren Ergebnissen. *Hier wird auf die Bestimmung der CITR zurückgegriffen, weil dies für die einzelnen Netzteilnehmer den geringsten Aufwand bedeutet.*

Umgang mit Fehlern Bei einem Linkbruch werden die betroffenen Verkehrsströme umgeroutet oder abgebrochen. Umrouten ist allerdings nur bei Kopplung an das Routingprotokoll möglich, außerdem werden dadurch eventuell andere Verkehrsströme gefährdet. *Hier werden CAC-Mechanismen betrachtet, die von der Wahl des Routingmechanismus unabhängig sind. Der Umgang mit Linkbrüchen ist deshalb nicht Aufgabe des CAC-Mechanismus.*

Umgang mit Überlast Überlast kann auftreten, wenn bei der Zulassung neuer Verkehrsströme falsche Entscheidungen getroffen werden, kann aber auch durch Mobilität oder Linkbrüche hervorgerufen werden, wenn bestehende Verkehrsströme umgeroutet werden müssen. Das kann zu einer Degradation der Dienstgüte aller aktiven Verkehrsflüsse in diesem Bereich führen. Wenn dies gezielt verhindert werden soll, gibt es die Möglichkeit, beispielsweise die Dienstgüte nur für ausgewählte niederprioritäre Verkehrsströme zu reduzieren, oder einzelne Verkehrsströme zu beenden, damit Ressourcen frei werden. *Welche Verkehrsströme als erstes abgebrochen werden, spielt hier keine übergeordnete Rolle.*

Existierende Ansätze

Eine gute Übersicht über CAC-Mechanismen für Ad-hoc-Netze findet sich in [25]. In dieser Arbeit sollen jedoch nur diejenigen näher betrachtet werden, die den oben genannten Kriterien entsprechen. Diese sind in Tab. 3.2 einander gegenübergestellt.

Tabelle 3.2: Vergleich verschiedener CAC-Verfahren

Name	Zulassungs-entscheidung	Metrik	zustandslos	Umgang mit Überlast	unterstützte Dienstgüte
SWAN-AC [6]	Testpakete (Probing)	Restkapazität	✓	ECN (Explicit Congestion Notification)	Differenzierung (nicht vorgesehen, aber möglich)
DACME [18]	Testpakete (Probing)	Zwischen-ankunftszeiten der Testpakete	✓	–	Differenzierung (nicht vorgesehen, aber möglich)
INSIGNIA [32]	alles mit niedrigem QoS-Level zulassen, wenn möglich Level erhöhen	Restkapazität	–	Degradation der Dienstgüte	Reservierung
QPART [57]	alles mit niedrigem QoS-Level zulassen, wenn möglich Level erhöhen	CITR (Channel Idle Time Ratio)	–	Beenden der neuesten Verkehrsströme	Differenzierung
MPARC [58]	Testpakete (Probing)	Restkapazität	–	–	Reservierung
IQoSR [34]	Informationen über alle existierenden Routen werden ständig aktualisiert	Restkapazität	–	–	Reservierung

DARMA Admission Control (DAC)

Für die hier betrachteten Einsatzgebiete von WMNs sind folgende Eigenschaften des CAC-Mechanismus wichtig:

- flexibel, damit unterschiedliche Ansprüche erfüllt werden können, abhängig vom Einsatzgebiet des Netzes,
- wenig Overhead, da in drahtlosen Netzen nur begrenzt Kapazität zur Verfügung steht,
- einfach zu implementieren, auch auf bestehender Technologie, da verschiedene Endgeräte zum Einsatz kommen,
- nicht an das Routingprotokoll gekoppelt, da abhängig vom Einsatzgebiet des Netzes verschiedene Protokolle verwendet werden,
- zustandslos, damit Knoten, die Daten weiterleiten müssen, möglichst wenig zusätzlichen Aufwand haben. Außerdem sollen Zwischenknoten aus Gründen der Datensicherheit keine Informationen über die Verkehrsflüsse haben.

Aus Tab. 3.2 lässt sich ablesen, dass nach den oben genannten Kriterien SWAN-AC am besten für die hier betrachteten Netze geeignet ist. Es dient daher als Basis für das verwendete Zugangskontrollverfahren. Im Gegensatz zur in [6] beschriebenen Architektur wird die Zugangskontrolle hier jedoch für alle Verkehrsklassen eingesetzt. Das resultierende CAC-Verfahren wird im Folgenden als *DAC* (DARMA Admission Control) bezeichnet.

Jeder Knoten überprüft die restliche verfügbare Kapzität in seiner Umgebung (CITR-Bestimmung, siehe Kap. 3.1.3), und abhängig davon wird entschieden, ob das Netz den zusätzlichen Verkehrsstrom tragen kann oder nicht. Als Kriterium für die Entscheidung dient ein vorher festgesetzter Schwellenwert für die Netzauslastung, ab dem keine neuen Verkehrsströme mehr zugelassen werden. Abhängig von der Höhe dieses Schwellenwertes wird unter Umständen entweder Bandbreite verschwendet oder zu viel Verkehr zugelassen. Die Wahl des Schwellenwertes hängt deshalb vom Einsatzgebiet ab. Falls die Differenzierung verschiedener Verkehrsklassen im Netz vorgesehen ist, kann der Schwellenwert für jede Klasse einzeln festgelegt werden (es können jedoch auch alle einzelnen Werte auf den gleichen Wert gesetzt werden).

Da die einzelnen Stationen unabhängig voneinander agieren, kann es passieren, dass mehrere Verkehrsströme gleichzeitig zugelassen werden und dadurch einzelne Zwischenknoten überlastet werden. Diese haben die Möglichkeit, die Quelle der betroffenen Verkehrsströme über den Ressourcenengpass zu informieren (ECN, siehe auch Kap. 2.2.5). Die Quelle ist dann dafür zuständig, den entsprechenden Verkehrsstrom zu stoppen. Hierfür ist ein zweiter Schwellenwert sinnvoll, anhand dessen die Knoten entscheiden, wann das Netz überlastet ist. Auch hier haben Verkehrsflüsse mit hoher Priorität Vorrang, niederprioritäre werden zuerst beendet.

Simulationen

Um die Güte von Zugangskontrollmechanismen zu bewerten, kommen verschiedene Kriterien in Frage. Einige davon sind allerdings ungünstig zu ermitteln, wie beispielsweise der Anteil von Verkehrsströmen, die fälschlicherweise zugelassen oder abgelehnt werden, oder auch die Anzahl zugelassener Verkehrsströme pro Kapazitätseinheit. Der Anteil von Verkehrsströmen, die abgebrochen bzw. beendet werden, hängt eng mit dem Anteil an zugelassenen bzw. abgelehnten Verkehrsströmen zusammen. Diese sind alle vom Szenario und speziell vom Verkehrsangebot abhängig. Deshalb ist es sinnvoll, gleichzeitig auch die Paketverlustrate zu betrachten, sodass ein Kompromiss zwischen beidem gefunden werden kann.

Im Gegensatz zu den anderen Simulationen, die in Kap. 3.2 näher beschrieben sind, wurde hier ein Szenario mit 25 Stationen simuliert. Alle Stationen sind gleichartig in Bezug auf ihre Funktionalität, und jede sendet einen Datenstrom mit konstanter Datenrate. Die Pakete haben eine Größe von 160 Byte und werden im Abstand von 20 ms an ein Gateway gesendet, welches sich jedoch nicht in Sendereichweite aller Stationen befindet. Das bedeutet, dass manche Verkehrsströme über mehrere (durchschnittlich zwei) Zwischenstationen zum Gateway weitergeleitet werden müssen. Ohne DAC würde jeder Verkehrsstrom bis zum Ende der Simulation andauern. Die Datenströme starten nicht gleichzeitig, sondern jeweils um 1 s versetzt, damit jeder einzeln vom CAC-Mechanismus bearbeitet werden kann. Die Auswertung der Simulation beginnt erst, wenn alle Verkehrsströme gestartet wurden und dauert weitere 100 s. Als Routingprotokoll wird AODV verwendet. Die Ergebnisse stellen einen Mittelwert aus 20 Simulationsdurchläufen dar.

Als Kriterium zur Bewertung des CAC-Mechanismus dient hier der Anteil von Übertragungen, die fehlerfrei regulär beendet werden und demnach bis zum Ende der Simulation andauern. Fehlerfrei bedeutet in diesem Fall, dass keine Daten verloren gehen, wobei aufgrund des Medienzugriffsmechanismus jedes Paket sechsmal wiederholt werden kann. Das heißt, dass erst nach sieben erfolglosen Sendeversuchen Daten verloren gehen.

In Abb. 3.2 sind die Ergebnisse dargestellt. Hierbei entspricht

$$\textit{DAC-z} \mathrel{\widehat{=}} \frac{\textit{Anzahl erfolgreich beendeter Übertragungen}}{\textit{Anzahl zugelassener Übertragungen}}$$

und

$$\textit{DAC-a} \mathrel{\widehat{=}} \frac{\textit{Anzahl erfolgreich beendeter Übertragungen}}{\textit{Anzahl angebotener Übertragungen}}.$$

Bei *DAC-a* sind also die abgelehnten Verkehrsströme zu den nicht fehlerfreien hinzugerechnet, während sie bei *DAC-z* komplett weggelassen werden.

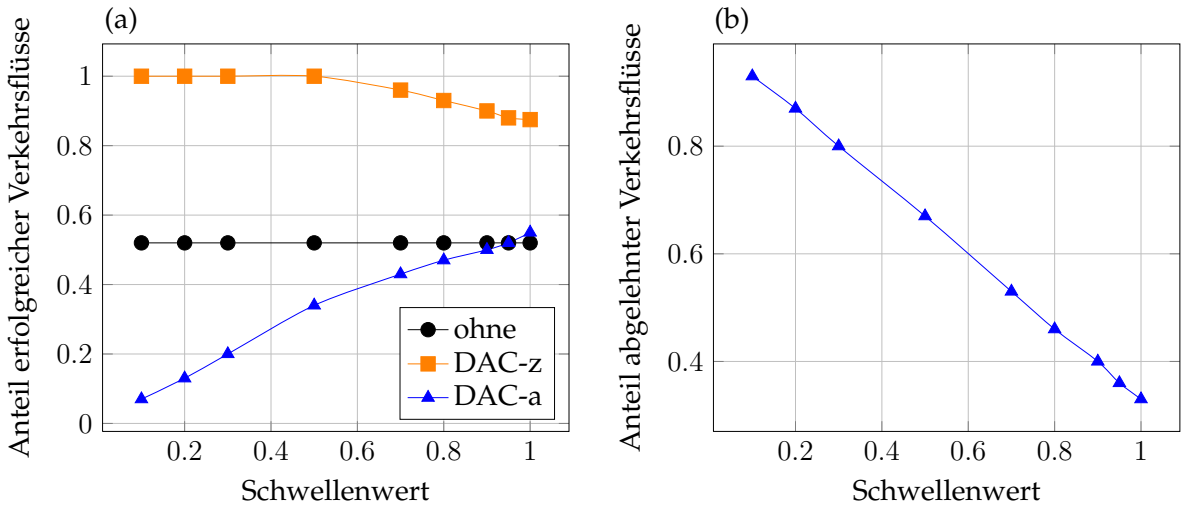


Abbildung 3.2: Zugangskontrolle

Auf der Abszisse ist der Schwellenwert des Zugangskontrollmechanismus aufgetragen, also bis zu welchem Anteil der verfügbaren Kapazität Datenströme zugelassen werden. Dabei steht natürlich trotzdem die gesamte Bandbreite für die Übertragung zur Verfügung, alles oberhalb der Schwelle dient als Reserve, falls zu viel Verkehr zugelassen wurde oder dieser sich ungünstig verteilt. Da das Angebot in diesem Versuch jedoch höher ist als die maximal verfügbaren Ressourcen, werden auch bei einem Schwellenwert von 1 nicht alle Verkehrsflüsse zugelassen.

Bei einem niedrigen Schwellenwert können alle zugelassenen Verkehrsströme fehlerfrei übertragen werden, da genügend Reserve vorhanden ist. Aber selbst bei einer Schwelle von 90% liegt die Rate noch bei 0,9 (*DAC-z*). In Abb. 3.2 b ist der Anteil abgelehnter Verkehrsströme zu sehen, also diejenigen, die vom CAC-Verfahren nicht zugelassen wurden, weil die Schwellenbandbreite bereits überschritten war. In Abb. 3.2 a sind diese unter *DAC-a* mit einberechnet. Bei niedrigem Schwellenwert ist die Zahl der erfolgreich beendeten Übertragungen dadurch erheblich niedriger als ohne CAC-Mechanismus. Hier gilt es jedoch zu bedenken, dass die Zugangskontrolle zwei entscheidende Vorteile mit sich bringt. Erstens wird es vom Benutzer als erheblich störender empfunden, wenn eine Datenübertragung abbricht, als wenn sie gar nicht erst zustande kommt. Zweitens führt der ECN-Mechanismus dazu, dass einzelne Verkehrsströme komplett abgebrochen werden, wodurch für andere wieder Ressourcen frei werden. Dadurch sinkt die Fehlerrate in bereits laufenden Übertragungen. Wenn keine Zugangskontrolle verwendet wird, bleiben alle Verkehrsströme erhalten und stören sich weiter gegenseitig. Andererseits entsteht durch den CAC-Mechanismus ein zusätzlicher Overhead durch das Versenden von Testpaketen und zusätzliche Wartezeit, bis diese Pakete verarbeitet wurden. Da dies aber nur vor dem Senden des ersten Pakets notwendig ist, sind die Unterschiede nur gering.

Ein Schwellenwert von unter 0,5 ist nach diesen Simulationsergebnissen nicht vorteilhaft. Welcher Wert tatsächlich verwendet wird, hängt vom Szenario ab: Werte

zwischen 0,5 und 0,7 sind sinnvoll, wenn die Paketfehlerrate im Netz klein gehalten werden soll. In Szenarien, wo dies nicht so wichtig ist und stattdessen lieber möglichst viele Nutzer bedient werden sollen, bietet sich ein Schwellenwert um 0,9 an.

3.1.2 Verkehrskategorisierung

Differenzierung wird erreicht, indem den einzelnen Verkehrsklassen unterschiedliche Parameter für den Medienzugriff zugewiesen werden. Deshalb ist es nicht möglich, Medienzugriff und Verkehrskategorisierung strikt zu trennen.

Da der Medienzugriff auch ohne Priorisierung möglich ist (nur andersherum nicht), wird die Verkehrskategorisierung hier trotzdem als eigener Mechanismus aufgeführt.

Die Differenzierung kann auf verschiedene Arten erzielt werden, üblicherweise wird eine Anpassung der Fenstergröße (Contention Window) und des Interframe Space verwendet. In [14] wird argumentiert, dass durch IFS-Differenzierung bessere Ergebnisse erzielt werden, weil dadurch die ersten Zeitschlitze im Anschluss an eine laufende Übertragung ausschließlich von Verkehrsklassen mit hoher Priorität genutzt werden können. Allerdings wird dort in erster Linie die Koexistenz mit Geräten, die keine Priorisierung unterstützen, untersucht. Die Ergebnisse gelten außerdem nur, wenn sich alle Stationen in Sendereichweite befinden, was in WMNs nicht der Fall ist. In [55] wird gezeigt, dass eine Differenzierung anhand der Fenstergröße den Vorteil hat, dass die Ergebnisse weitgehend unabhängig von der Netzauslastung und dadurch besser vorhersehbar sind.

Eine andere Möglichkeit ist die Priorisierung mit Hilfe sogenannter Black Bursts (siehe z.B. [62, 35]). Sobald der Kanal frei wird, sendet jede Station ein kurzes Signal, dessen Länge die Priorität des zu sendenden Pakets widerspiegelt (je höher die Priorität, desto länger das Signal). Falls im Anschluss daran der Kanal belegt ist, bedeutet das, dass eine andere Station ein längeres Signal sendet und somit ein Paket mit höherer Priorität zu senden hat. Alle Stationen mit niedrigerer Priorität verzichten daraufhin auf den Kanalzugriff. Dadurch wird erreicht, dass kein Paket mit niedriger Priorität gesendet werden kann, solange irgendeine Station noch Pakete mit höherer Priorität zu senden hat.

Existierende Lösungen

Existierende Mechanismen verwenden unterschiedlich viele Verkehrsklassen, so ist beispielsweise eine Einteilung in zwei Klassen denkbar, nämlich zeitkritischer Verkehr und sonstiger Verkehr [6], oder auch eine genauere Unterscheidung in vier Klassen, nämlich Sprachdaten (höchste Priorität), Videodaten, normaler (Best-Effort-) Verkehr und Hintergrundverkehr, wie unter anderem im Standard IEEE 802.11e [64]. Beispiele für die Verwendung von Black Bursts sind EY-NPMA (Elimination Yield Non Preemptive Multiple Access), welches bei Hiperlan [62] zum Einsatz kommt, sowie PDCF (Priority Distributed Coordination Function) [35]. Da sich Hiperlan in

der Praxis nie durchsetzen konnte, ist es aus Gründen der Kompatibilität mit bestehenden Systemen sinnvoll, 802.11e als Basis zu verwenden.

Designkriterien

Neben der Anzahl der Verkehrsklassen ist ein wesentliches Kriterium, in welchem Verhältnis die verfügbaren Ressourcen auf die einzelnen Verkehrsklassen aufgeteilt werden, insbesondere bei steigendem Verkehrsangebot.

Eine Möglichkeit ist, die Ressourcen in erster Linie für Pakete höchster Priorität zu verwenden, und nur falls noch Kapazität übrig ist, die niedrigen Prioritäten zu bedienen. Eine solche Aufteilung ist z.B. bei der Fahrzeug-zu-Fahrzeug-Kommunikation sinnvoll, da dort sichergestellt werden muss, dass die sicherheitskritischen Daten auf jeden Fall übertragen werden. Niedrige Priorität haben in einem solchen Szenario Unterhaltungsmedien, deren Ausfall keine Auswirkungen auf die Fahrzeugsteuerung hat.

Aufgabe von vermaschten drahtlosen Netzen ist jedoch in den meisten Fällen, Zugang zum Internet zu bieten. Daher ist hier eine Ressourcenaufteilung sinnvoller, die den Verkehr aller Prioritäten absenkt, sodass auch Best-Effort-Verkehr noch eine Chance hat. In Kap. 3.2.3 ist in Abb. 3.11 ein Vergleich zwischen verschiedenen Priorisierungsverfahren dargestellt.

Modifikationen

Der Standard 802.11e definiert die Parameter für die Priorisierung. Statt $CW_{\min}$ und $CW_{\max}$ werden einzelne $CW_{\min}(i)$ und $CW_{\max}(i)$ in Abhängigkeit der Priorität i der Verkehrsklasse eingeführt. Arbitrary Interframe Spaces (AIFS) mit unterschiedlicher Dauer ersetzen den IFS (siehe Formel A.1). Im Standard sind Werte hierfür vorgegeben, wobei Anpassungen möglich sind. Darauf wird in Kap. 4.7 näher eingegangen. Weitere Modifikationen des Priorisierungsmechanismus sind im Zusammenhang mit dem Medienzugriff in Kap. 3.1.3 beschrieben.

Ohne Beschränkung der Allgemeinheit bezeichnet im Folgenden „0“ stets die Verkehrsklasse mit der höchsten Priorität. Die niedrigeren Prioritäten sind von 1 bis $i_{max} - 1$ der Reihe nach nummeriert (höhere Zahl bedeutet niedrigere Priorität).

3.1.3 Medienzugriffssteuerung

Die Basis der DARMA-Architektur ist das Medienzugriffsverfahren (Medium Access Control, MAC). Wie in Kap. 2.2.4 bereits erläutert, soll hier ein wettbewerbsbasiertes Verfahren, welches auf CSMA/CA [64] aufbaut, zum Einsatz kommen, da so keine Synchronisierung der Teilnehmer notwendig ist. Ein weiteres Kriterium ist die Kompatibilität zu existierenden Lösungen. Die heute am weitesten verbreitete Technologie im Bereich der lokalen drahtlosen Netze ist IEEE 802.11 [63], welche auch hier als Basis

dienen soll. Ein entscheidender Nachteil von CSMA/CA ist, dass es sich nicht an den Netzzustand anpasst, wie in Kap. 2.2.4 bereits beschrieben. Die ebenfalls in Kap. 2.2.4 angesprochene Erweiterung eDCC [30] mit Formel 2.4 führt zu nicht optimalen Ergebnissen (siehe auch Kap. 3.2.3): Abhängig vom Szenario können verschiedene Effekte beobachtet werden. Die Verzögerungszeit der Pakete ist in manchen Fällen erheblich höher, in anderen auch erheblich niedriger als ohne eDCC. Das Hauptproblem ist jedoch, dass eDCC in Multihop-Szenarien dem Priorisierungsmechanismus entgegenwirkt. Durch die Verwendung von eDCC hängt der Kanalzugriff hauptsächlich von der Sendewahrscheinlichkeit PT ab, und damit von der Netzauslastung und der Anzahl der Wiederholungen pro Paket. Da diese unabhängig von den Verkehrsklassen sind, geht die Priorisierung weitgehend verloren. Des Weiteren ist die Abschätzung der Kanalbelegung für die höheren Prioritäten recht ungenau, da sie nur über eine kürzere Zeitdauer stattfindet.

Priority-Aware Distributed Contention Control (PADCC)

Der eDCC-Mechanismus hat jedoch auch mehrere vorteilhafte Eigenschaften: Er ist einfach, adaptiv, dezentral und kompatibel zu 802.11e. Deshalb wird hier eine Erweiterung von eDCC vorgeschlagen [2, 3], um die oben genannten Probleme zu beheben: Priority-Aware Distributed Contention Control (PADCC).

Bei hohem Verkehrsangebot ist die Kollisionsrate der Pakete sehr hoch. Das verringert den Gesamtdurchsatz, da eine Kollision Zeit benötigt, in der keine Daten empfangen werden können. Der Hintergedanke von DCC ist es, die Kollisionsrate zu verringern. Am besten wäre es, wenn zu jedem Zeitpunkt nur genau eine Station sendet (bzw. in größeren Szenarien können auch mehrere Stationen gleichzeitig senden, solange sie sich nicht gegenseitig stören). Das ist bei einem verteilten Medienzugriffsverfahren jedoch nicht ohne weiteres zu bewerkstelligen. Eine grundsätzliche Möglichkeit ist die folgende: Wenn zu einem Zeitpunkt n Stationen gleichzeitig auf den Kanal zugreifen ($n > 1$), gibt es eine Kollision. Damit die Übertragung erfolgreich ist, darf nur eine Station senden. Das bedeutet, die Sendewahrscheinlichkeit PT für jede einzelne Station sollte in diesem Zeitschlitz $\frac{1}{n}$ sein, damit im Durchschnitt genau eine Station sendet. Leider ist n jedoch nicht im Vorhinein bekannt.

Beim ursprünglichen DCC [15] wird PT deshalb anhand der Nutzungsrate der Zeitschlitze SU abgeschätzt. Deren Berechnung nach Formel 2.3 ist jedoch sehr ungenau, insbesondere bei Verkehrsklassen mit hoher Priorität, da diese im Allgemeinen einen kürzeren Backoff haben. Die beobachtete Kanalbelegung ist außerdem nicht von der Verkehrsklasse abhängig, sondern von der Station. Deshalb reicht es, wenn jede Station die Kanalbelegung berechnet bzw. abschätzt und alle Verkehrsklassen auf diesen Wert zurückgreifen.

Der Zugangskontrollmechanismus muss die Auslastung des Netzes beurteilen und berechnet dafür den Anteil der Zeit, in der der Kanal frei ist (CITR). Das Medienzugriffsverfahren kann auf diesen Wert zugreifen, da sich beides auf Schicht 2 des

OSI-Modells abspielt. Dadurch entsteht also kein zusätzlicher Aufwand. Für die Berechnung wird jeweils der Zustand des Kanals für die letzten 2000 Zeitschlitze (entspricht 40 ms) abgespeichert („0“ entspricht *frei* und „1“ entspricht *belegt*). Diese 2000 Werte werden zyklisch überschrieben, sodass jeweils die aktuellen Werte verwendet werden. Für die CITR-Berechnung ist jedoch nicht interessant, wie lange der Kanal belegt ist, sondern wie oft ein Kanalzugriff stattfindet. Deshalb wird die Anzahl der leeren Zeitschlitze gezählt und mit der Anzahl der Kanalzugriffe in Verhältnis gestellt, also eine „1“, die auf eine „0“ folgt:

$$CITR = \frac{\textit{Anzahl freier Zeitschlitze}}{\textit{Anzahl freier Zeitschlitze} + \textit{Anzahl Kanalzugriffe}} \tag{3.1}$$

$$SU = 1 - CITR \tag{3.2}$$

Dadurch, dass die Kanalbelegung nicht mehr nur während eines Backoffs gemessen wird, sondern über längere Zeit, wird eine genauere Schätzung des aktuellen Zustandes erreicht, sofern dieser sich nicht sprunghaft ändert. Außerdem ist die Messung jetzt unabhängig von der Verkehrsklasse und behebt dadurch das Problem, dass die höchste Priorität insgesamt ungenauere Schätzwerte zur Verfügung hat.

Das in [15] geschilderte Problem, dass PT immer zwischen den Werten 0 und 1 hin- und herspringt, wenn die naheliegende Formel

$$PT = 1 - SU \tag{3.3}$$

verwendet wird, wird bei PADCC umgangen, indem die Priorität i der jeweiligen Verkehrsklasse mit in die Berechnung der Sendewahrscheinlichkeit einbezogen wird. Die Abhängigkeit von der Anzahl der Sendeversuche, die aus ebendiesem Grund ursprünglich eingeführt wurde, ist damit nicht mehr notwendig. Verkehrsklassen mit höherer Priorität haben jetzt eine höhere Wahrscheinlichkeit zu senden. Die Formel zur Berechnung von PT lautet dann [2]:

$$PT'(SU, i) = 1 - SU + \frac{1}{2} - \frac{i}{i+1} \tag{3.4}$$

Da die Werte, die PT' annehmen kann, nicht mehr zwischen 0 und 1 beschränkt sind, müssen sie noch entsprechend abgebildet werden:

$$PT(SU, i) = \begin{cases} 1 & \text{falls } PT' > 1 \\ 0{,}2 & \text{falls } PT' < 0{,}2 \\ PT' & \text{sonst} \end{cases} \tag{3.5}$$

Werte unter 0,2 werden nicht zugelassen, um die Zahl der Zeitschlitze zu verringern, die frei bleiben, wenn alle sendewilligen Stationen auf den Kanalzugriff verzichten.

Die Sendewahrscheinlichkeit ist bei PADCC also unabhängig von der Anzahl der Wiederholungen und hängt stattdessen von der jeweiligen Verkehrsklasse ab. Dadurch bleibt die Priorisierung erhalten, und der Algorithmus liefert insgesamt eine genauere Abschätzung für SU und damit bessere Ergebnisse.

3.2 Simulationsergebnisse

Um die Leistungsfähigkeit der vorgestellten Mechanismen zu evaluieren, wurden verschiedene Szenarien simuliert. Für alle Simulationen in diesem Kapitel wurde der Network Simulator (ns-2) [81] mit der Erweiterung für 802.11e [79] verwendet. Die Simulationsparameter entsprechen der Spezifikation für 802.11n [65] und sind in Tab. 3.3 dargestellt. Eine umfassendere Auflistung der verwendeten Parameter ist im Anhang A angegeben.

Tabelle 3.3: IEEE 802.11e: Spezifikation

Parameter	Wert	Beschreibung
Frequenz	2,4 GHz	
Basisdatenrate	6 Mbit/s	Übertragungsrate für Signalisierungsnachrichten
Datenrate	65 Mbit/s	maximale Übertragungsrate für Datenpakete
t_{Slot}	20 µs	Dauer eines Zeitschlitzes
SIFS	10 µs	Short Interframe Space
Paketgröße	512 Byte	Nutzdaten

Das verwendete Routingprotokoll ist DSDV. Als Ausbreitungsmodell dient ein erweitertes Freiraumausbreitungsmodell mit $\gamma = 2$ als Pfadverlustkoeffizient für Sichtverbindungen (line of sight) und $\gamma = 4$ falls keine Sichtverbindung besteht (siehe auch Anhang B.2.3). In jedem Szenario gibt es vier Sender-Empfänger-Paare, zwischen denen je ein UDP-Verkehrsstrom mit konstanter Datenrate übertragen wird. Im Fall von Verkehrskategorisierung hat jeder dieser Verkehrsströme eine andere Priorität. Die Simulationszeit beträgt jeweils 100 Sekunden.

Die Simulationen wurden ohne Zugangskontrolle durchgeführt, da der Zugangskontrollmechanismus die Anzahl der Verkehrsströme begrenzt und damit das Verkehrsangebot künstlich verringert. Dadurch ermöglicht er es, das Netz knapp unterhalb der Kapazitätsgrenze zu halten. Im laufenden Betrieb des Netzes ist das sinnvoll, aber zur Bewertung der Leistungsfähigkeit der Dienstgütemechanismen sind Simulationen in einem voll ausgelasteten Netz notwendig. Deshalb wurden für die Zugangskontrolle separate Simulationen durchgeführt, die in Kap. 3.1.1 dargestellt sind.

3.2.1 Szenarien

Im Folgenden werden verschiedene grundlegende Szenarien betrachtet, um die wichtigsten Eigenschaften der Mechanismen zu beurteilen. Die einzelnen Szenarien sind in Abb. 3.3 dargestellt.

Singlehop-Szenario: Acht Stationen befinden sich jeweils in Sendereichweite zu allen anderen Stationen. Die Anordnung der Stationen ist zufällig.

Multihop-Szenario: Hier sind Sender und Empfänger nicht in Funkreichweite, sondern können nur über zwischenliegende Knoten miteinander kommunizieren. Insgesamt befinden sich 20 Stationen im Szenario, wobei jeweils fünf zu einem Datenstrom gehören.

Flaschenhalsszenario: Im Gegensatz zum Multihop-Szenario sind hier vier Multihop-Verkehrsströme geographisch so angeordnet, dass sie ein Kreuz bilden. Die Station, die sich in der Mitte befindet, stellt dabei einen Flaschenhals dar, da sie alle Pakete aller vier Datenströme weiterleiten muss. Hier befinden sich insgesamt 17 Stationen im Szenario.

3.2.2 Parameter

In jedem Szenario gibt es mehrere Verkehrsströme, deren Gesamtdurchsatz, Verzögerung und Paketverlustrate gemessen werden. Diese Parameter sind im Einzelnen wie folgt definiert:

Datendurchsatz – im Englischen als *Goodput* bezeichnet – ist die erzielte Empfangsdatenrate auf Anwendungsschicht. Im Unterschied dazu ist *Throughput* die Empfangsdatenrate auf physikalischer Schicht. Im Folgenden wird das Wort *Durchsatz* als Synonym für Datendurchsatz verwendet.

Verzögerung bezeichnet die durchschnittliche Ende-zu-Ende-Verzögerung der gesendeten Pakete. Gemessen wird dabei vom Zeitpunkt der Ankunft des Pakets auf der MAC-Schicht des Senders bis zur Ankunft auf der MAC-Schicht des Empfängers.

Paketverlustrate ist der Anteil an Paketen, die auf der MAC-Schicht verloren gehen. Das kann durch Kollisionen oder aufgrund eines Pufferüberlaufs passieren. Da das Medienzugriffsverfahren jedes Paket, für das keine Quittung empfangen wird, bis zu siebenmal wiederholt, ist der Anteil an tatsächlich verlorenen Daten erheblich geringer.

Bei den Simulationen wird der angebotene Verkehr variiert, also die Datenmenge, die die einzelnen Stationen pro Zeiteinheit senden wollen. Dadurch kann das Verhalten des Systems für unterschiedliche Auslastungsgrade evaluiert werden. Alle

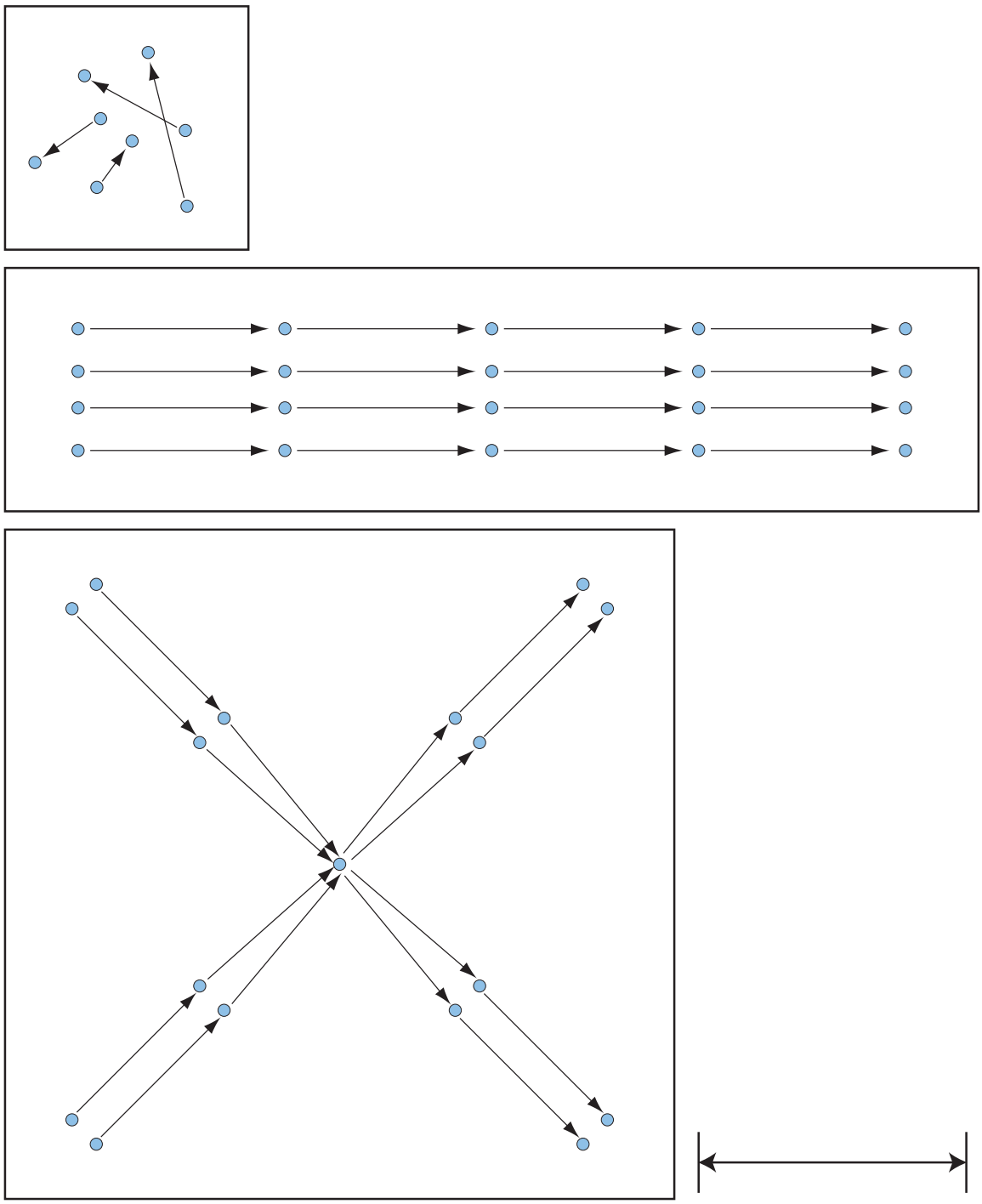


Abbildung 3.3: Singlehop-Szenario (oben), Multihop-Szenario (mitte), Flaschenhalsszenario (unten). Rechts unten ist die Sendereichweite angedeutet.

Simulationsergebnisse in Kap. 3.2.3 sind Mittelwerte aus mehreren Simulationen. Sofern nicht anders angegeben, haben die Simulationsergebnisse ein Konfidenzniveau von 95% bei einem Konfidenzintervall von 5% um den Simulationsmittelwert. Das bedeutet, dass 95% der Werte weniger als 5% vom Mittelwert entfernt sind. Es wurden jeweils so viele Simulationen durchgeführt, bis das Konfidenzintervall in Bezug auf den Durchsatz erreicht war, mindestens jedoch zwölf. Spätestens nach 40 Durchgängen wurde abgebrochen. Für diese Fälle sind die Konfidenzintervalle in den Graphen angegeben.

3.2.3 Ergebnisse

Um die Ergebnisse einordnen zu können, ist eine kurze Überlegung sinnvoll, welcher Durchsatz maximal erwartet werden kann. Dies hängt von den verwendeten Parametern ab, die in Tab. 3.3 aufgelistet sind. Der Durchsatz S bezeichnet die Menge an Nutzdaten, die in einem Zeitintervall übertragen werden und lässt sich demnach berechnen, indem man die Länge eines Pakets durch die durchschnittliche Übertragungsdauer eines Pakets teilt:

$$S = \frac{\textit{Paketlänge}}{\textit{Übertragungsdauer eines Pakets}} \tag{3.6}$$

Bei der Bestimmung der Paketlänge dürfen nur die Nutzdaten berücksichtigt werden. Die Übertragungszeit setzt sich aus der Sendedauer des Pakets t_{Daten}, der Sendedauer der Quittung t_{ACK}, einem Short Interframe Space t_{SIFS}, der abgewartet werden muss bevor die Quittung gesendet werden kann, einem AIFS t_{AIFS}, der abgewartet werden muss bevor der Backoff begonnen wird, und dem Erwartungswert für die Dauer des Backoffs $\mathrm{E}[b] \cdot t_{Slot}$ zusammen. Damit kann S angegeben werden als:

$$S = \frac{\textit{Nutzdaten}}{t_{AIFS} + \mathrm{E}[b] \cdot t_{Slot} + t_{Daten} + t_{SIFS} + t_{ACK}} \tag{3.7}$$

Der maximale Durchsatz ergibt sich unter den gegebenen Parametern, wenn nur der kürzeste Backoff und der kleinste AIFS abgewartet werden muss:

$$S_{\max} = \frac{512\ \text{Byte} \cdot 8\ \frac{\text{bit}}{\text{Byte}}}{50\ \mu\text{s} + 0 \cdot 20\ \mu\text{s} + 110\ \mu\text{s} + 10\ \mu\text{s} + 66\ \mu\text{s}} = 17{,}36\ \frac{\text{Mbit}}{\text{s}} \tag{3.8}$$

$S_{\max}$ stellt eine theoretische Obergrenze für den Durchsatz dar, die in der Realität nicht erreicht wird, da bei hoher Netzauslastung erstens der Erwartungswert für die Backofflänge größer ist als das Minimum und zweitens Pakete mit relativ hoher Wahrscheinlichkeit kollidieren, wodurch zusätzlich Zeit verloren geht. Davon ausgegangen, dass vor jeder Übertragung durchschnittlich zwei Zeitschlitze frei bleiben und

im Schnitt jedes fünfte Paket kollidiert, erhält man mit Formel 3.7 einen Durchsatz von etwa 13 Mbit/s.

Tabelle 3.4: Erklärung der Legenden zu den Simulationsgraphen

Kürzel	Bedeutung
prio x / px	Priorität x; x $\in \{0, 1, 2, 3\}$
ges	gesamt (aggregierter Gesamtverkehr aller Verkehrsklassen)
-m	Multihop-Szenario
-f	Flaschenhalsszenario
-e	Verwendung von eDCC
-PADCC	Verwendung von PADCC

Referenz

Die Simulationsergebnisse für reines 802.11 bzw. 802.11e seien in Abb. 3.4 als Referenz dargestellt und sollen im Folgenden kurz erläutert werden.

In Abb. 3.4 a ist der erzielte Durchsatz im Singlehop-Szenario ohne Verkehrskategorisierung dargestellt. Bei niedriger Auslastung entspricht der Durchsatz dem angebotenen Verkehr, da genügend Ressourcen zur Verfügung stehen, um alle Pakete zu übertragen. Wenn das Angebot größer wird als die Kapazität des Netzes, geht das System in Sättigung. Das ist bei etwas über 12 Mbit/s der Fall. In Abb. 3.4 c und e sieht man, dass gleichzeitig die Verzögerung, die die einzelnen Pakete erfahren, und die Paketverlustrate erheblich ansteigen. Sobald das Netz gesättigt ist, wird die Paketverlustrate hauptsächlich durch Pufferüberläufe beeinflusst. Deshalb steigt auch die Paketverzögerung nicht weiter an, da diese nur für diejenigen Pakete berechnet wird, die tatsächlich gesendet werden. Ein Verkehrsangebot von mehr als 12 Mbit/s ist also nicht sinnvoll.

In Abb. 3.4 b ist die Aufteilung des Durchsatzes auf die einzelnen Prioritäten dargestellt. Bei niedriger Netzauslastung können die Pakete aller Verkehrsklassen übertragen werden. Bei höherer Last bricht der Durchsatz der niedrigeren Prioritäten zugunsten der höheren Prioritäten ein. Mit der Verzögerung verhält es sich äquivalent (Abb. 3.4 d): Mit steigender Netzauslastung steigt die Verzögerung aller Pakete, bei den niedrigeren Prioritäten jedoch erheblich schneller. Die Paketverlustrate für die einzelnen Prioritäten steigt erwartungsgemäß ab dem Punkt, an dem der Durchsatz der jeweiligen Verkehrsklasse einbricht, sprunghaft an (Abb. 3.4 e).

Wenn im Netz ausreichend Ressourcen zur Verfügung stehen, sind keine Dienstgütemechanismen notwendig, da alle Verkehrsströme ihren Anforderungen entsprechend bedient werden können. Interessant ist deshalb der Bereich direkt an der Kapazitätsgrenze, was in diesem Fall einem Verkehrsangebot von 10–15 Mbit/s entspricht. Ein höheres Angebot ist nicht sinnvoll, weil es das Netz überlastet und dadurch zu Verzögerungszeiten und Paketverlustraten führt, die zu hoch sind, um eine sinnvolle Kommunikation zwischen Teilnehmern zu ermöglichen.

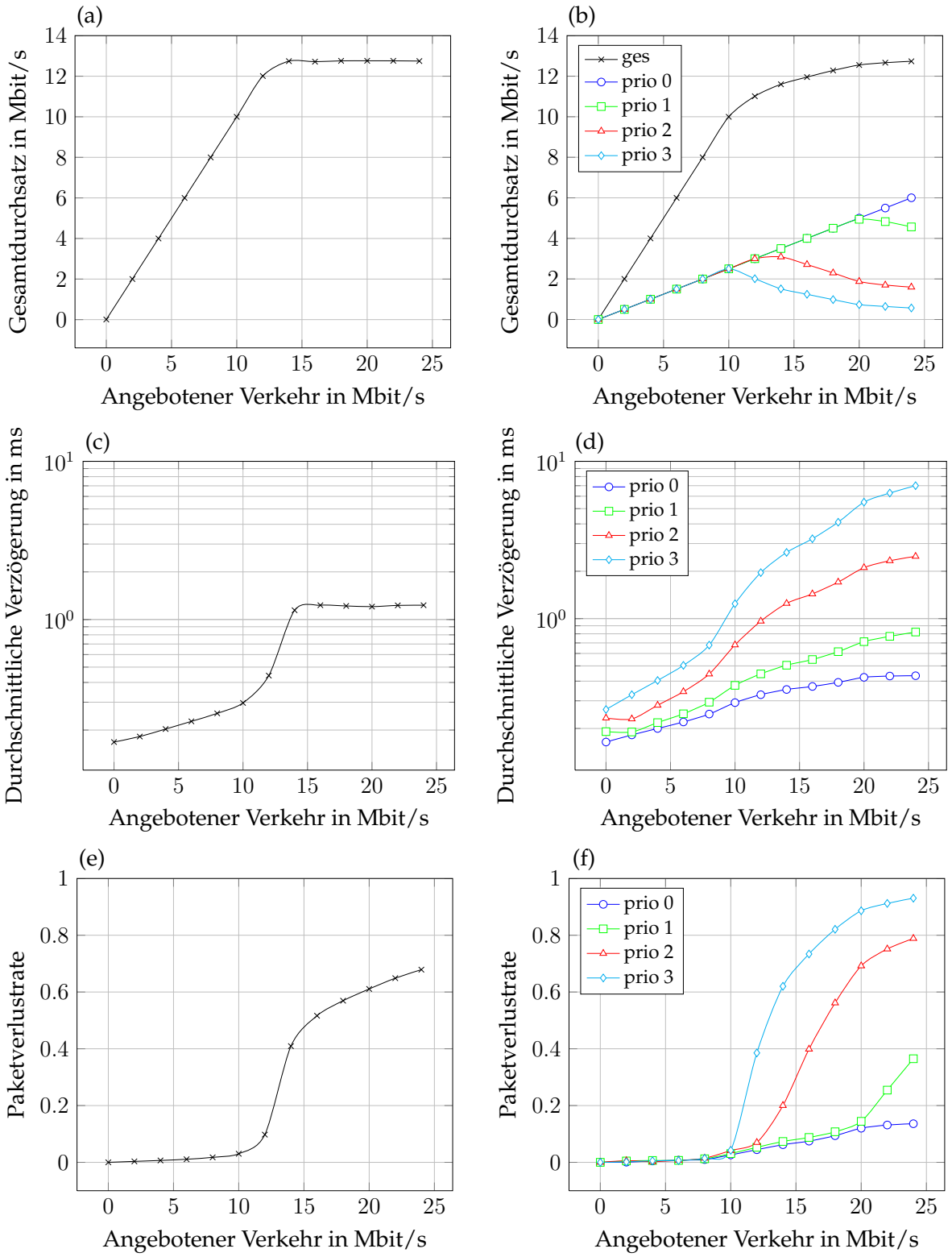


Abbildung 3.4: Singlehop-Szenario (links ohne, rechts mit Priorisierung)

Multihop

In Abb. 3.5 sind die äquivalenten Ergebnisse für das Multihop-Szenario dargestellt. Hier muss jedes Paket viermal übertragen werden, bevor es beim Empfänger ankommt. Dadurch hat jeder einzelne Knoten mehr Konkurrenz beim Kanalzugriff als im Singlehop-Szenario (elf sendende Stationen in Sendereichweite anstatt drei), und durch das Weiterleiten werden zusätzliche Ressourcen verbraucht. Deshalb ist, wie zu erwarten, der Gesamtdurchsatz (Abb. 3.5 a und b) niedriger und die Verzögerung (Abb. 3.5 c und d) deutlich höher als im Singlehop-Szenario.

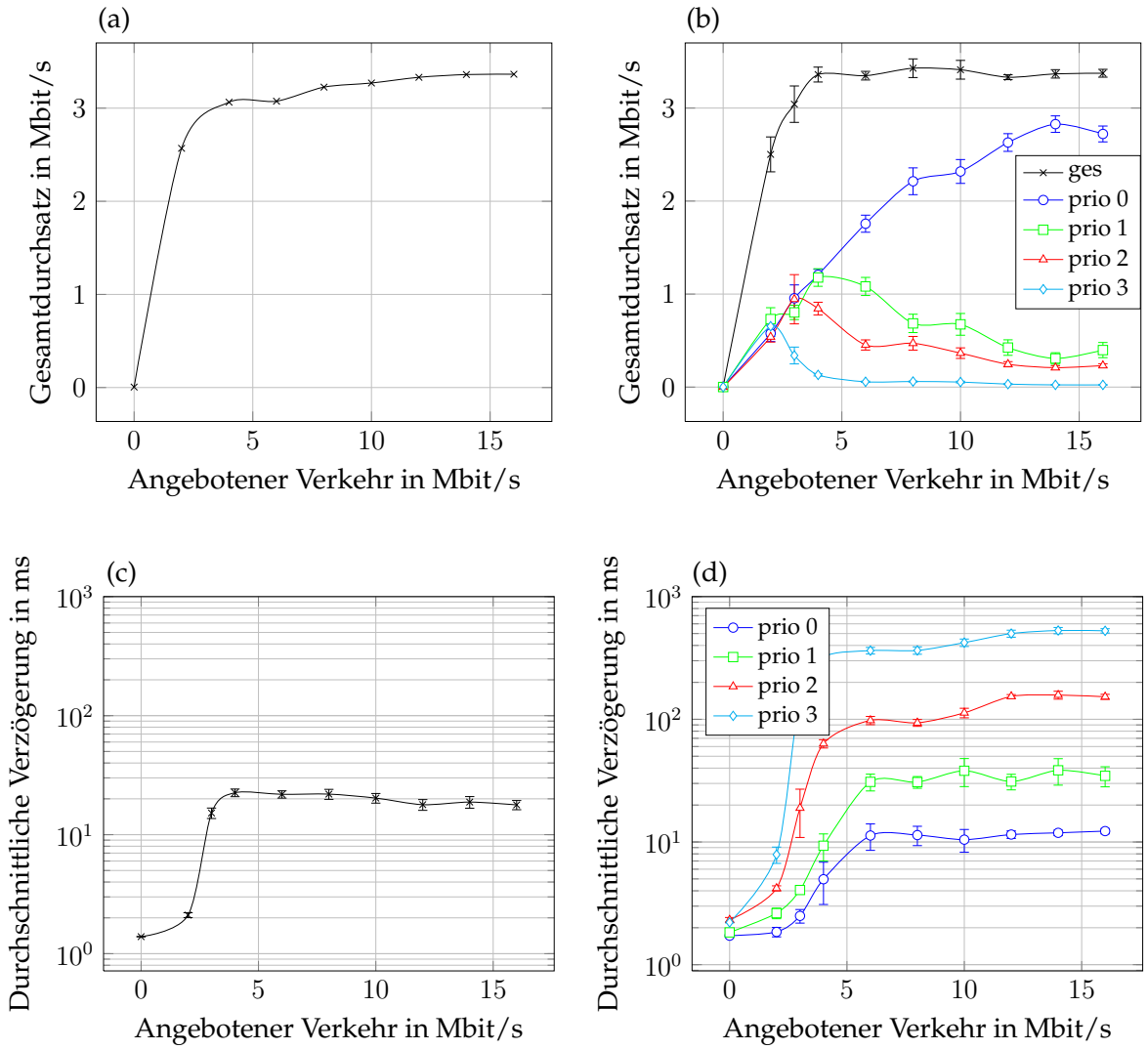


Abbildung 3.5: Multihop-Szenario (links ohne, rechts mit Priorisierung)

Beim Flaschenhalsszenario ist der Gesamtdurchsatz erwartungsgemäß noch etwas niedriger, da die mittlere Station alle Pakete weiterleiten muss. Qualitativ verhalten sich die Ergebnisse ansonsten wie beim Multihop-Szenario. In Abb. 3.6 ist der Vergleich zwischen diesen beiden Szenarien dargestellt: Einerseits der Durchsatz ohne

Verkehrskategorisierung (Abb. 3.6 a), andererseits die Verzögerung mit Verkehrskategorisierung, wobei aus Gründen der Übersichtlichkeit die zweithöchste Priorität weggelassen wurde (Abb. 3.6 b).

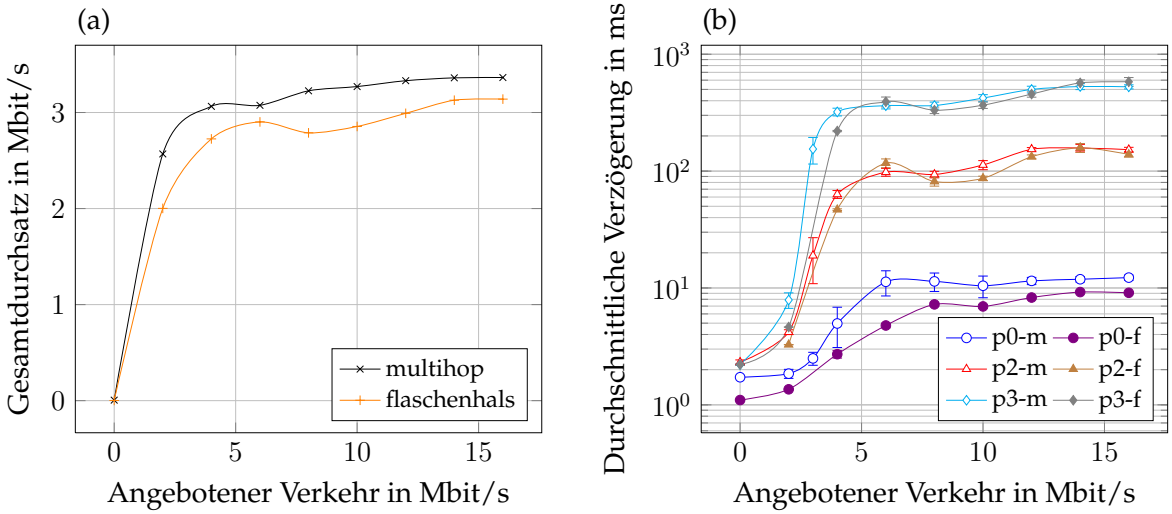


Abbildung 3.6: Vergleich zwischen Multihop- und Flaschenhalsszenario (links ohne, rechts mit Priorisierung)

eDCC

Im Singlehop-Szenario sieht man kaum Unterschiede zwischen eDCC und normalem 802.11/e (siehe Abb. 3.7). Während der Durchsatz ohne Priorisierung durch den Einsatz von eDCC um 2% steigt (Abb. 3.7 a), ist er mit Priorisierung um knapp 3% geringer, was sich hauptsächlich auf die niedrigste Priorität auswirkt (Abb. 3.7 b). Das spiegelt sich auch bei der Verzögerung der Pakete wider, die für die niedrigste Priorität deutlich höher ist, sonst aber kaum Unterschiede aufweist (Abb. 3.7 c). Die Verwendung von eDCC lohnt sich hier also nicht.

Im Multihop-Szenario hingegen sind deutliche Unterschiede zu sehen. Der Gesamtdurchsatz ist zwar auch hier fast gleich (Abb. 3.8 a), doch fällt die Verzögerung bei Verwendung von eDCC deutlich geringer aus (Abb. 3.8 b). Wird Verkehrskategorisierung eingesetzt, ist jedoch ein interessanter Effekt zu beobachten: Die Prioritäten kehren sich um, und in der Verkehrsklasse, die eigentlich die höchste Priorität haben sollte, werden weniger Pakete gesendet als in der zweithöchsten Klasse (siehe auch Kap. 3.1.3). Besonders deutlich ist das im Flaschenhals-Szenario zu sehen (siehe Abb. 3.9 b).

Aufgrund dieser Beobachtungen ist eDCC in seiner ursprünglichen Form nicht für den Einsatz in WMNs geeignet.

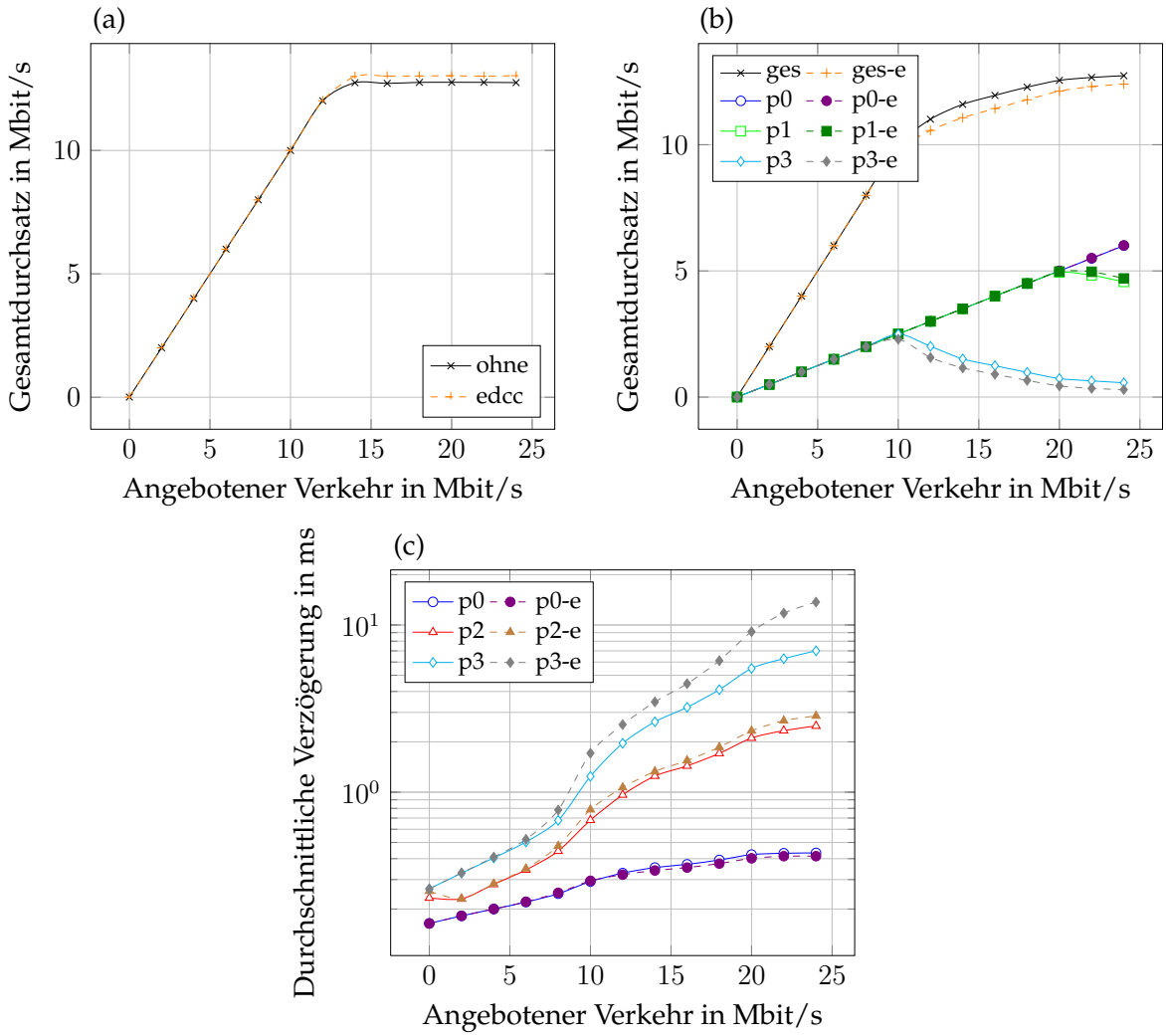


Abbildung 3.7: Vergleich zwischen 802.11/e und eDCC, Singlehop-Szenario

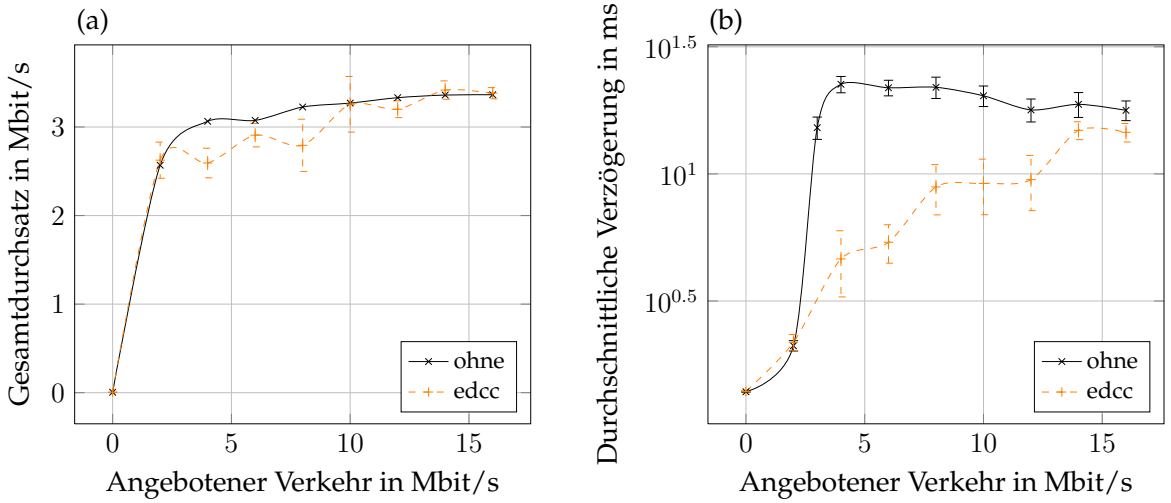


Abbildung 3.8: Vergleich zwischen 802.11e und eDCC, Multihop-Szenario

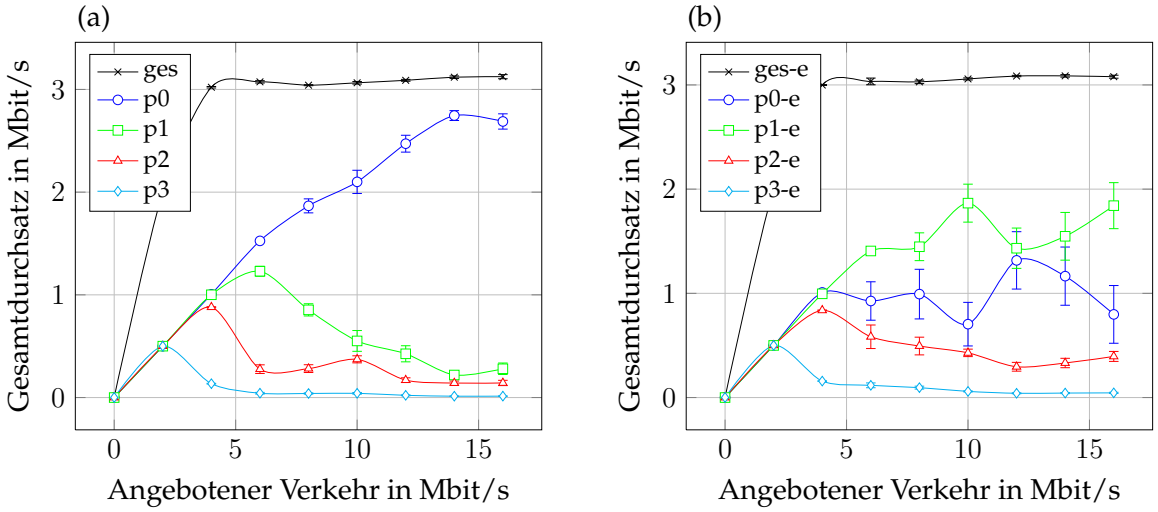


Abbildung 3.9: Vergleich zwischen 802.11e (links) und eDCC, Flaschenhalsszenario

PADCC

Mit den in Kap. 3.1.3 angesprochenen Modifikationen ist es möglich, den Durchsatz im Multihop-Szenario zu steigern (Abb. 3.10 a). Die Inversion der einzelnen Prioritäten, wie sie bei eDCC auftritt, wird dadurch ebenfalls behoben. Die Erhöhung des Durchsatzes wirkt sich auf alle Verkehrsklassen aus. Insgesamt kann eine Steigerung von bis zu 10% beobachtet werden, bei der niedrigsten Verkehrsklasse sind es sogar durchschnittlich 90%. Gleichzeitig verringert sich die durchschnittliche Verzögerung der Pakete (Abb. 3.10 b). Auch hier profitieren alle Verkehrsklassen: Durchschnittlich ist die Verzögerung um 30% niedriger, bei der niedrigsten Priorität sind es sogar bis zu 50%.

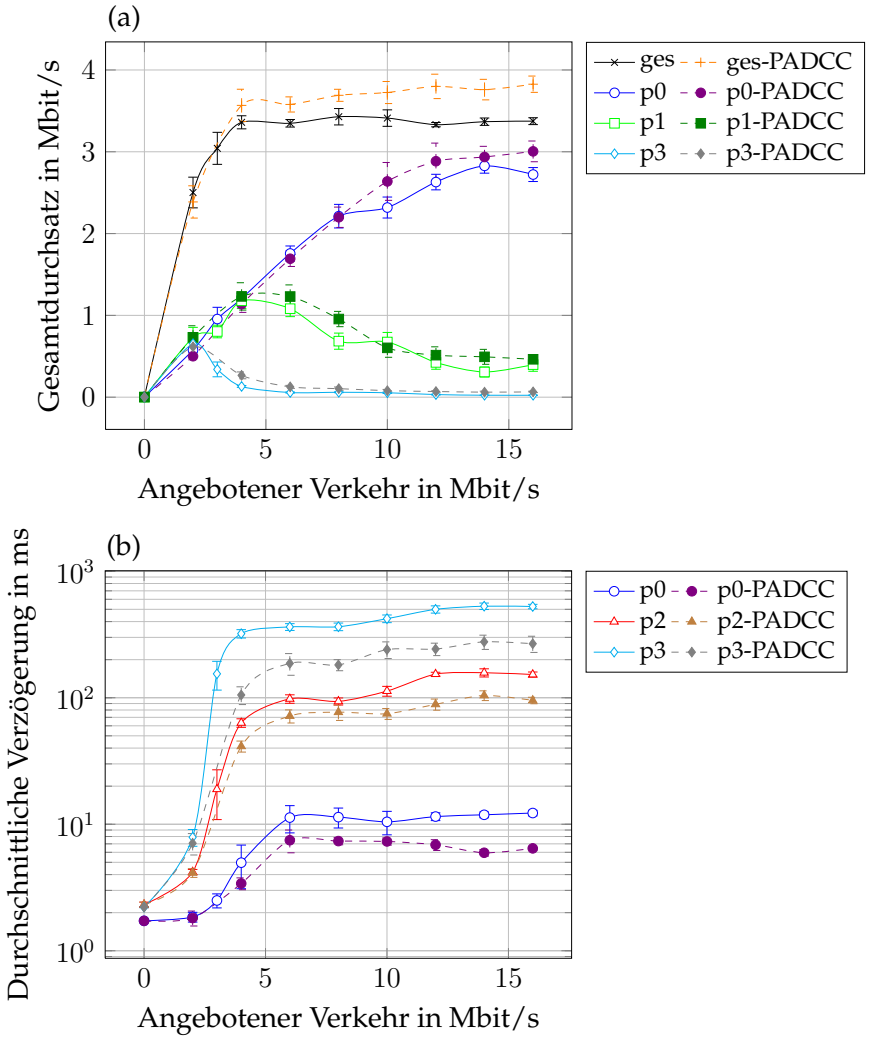


Abbildung 3.10: Vergleich zwischen 802.11e und PADCC, Multihop-Szenario

Priorisierung

Abb. 3.11 zeigt einen Vergleich zwischen den einzelnen Verkehrsklassen bei 802.11e und EY-NPMA [62]. Hier sieht man, dass die Aufteilung zwischen den Prioritäten bei 802.11e den in Kap. 3.1.2 genannten Kriterien entspricht (Abb. 3.11 a): Auch bei hoher Netzlast können die Verkehrsklassen niedriger Priorität noch Pakete senden, natürlich deutlich weniger als die höchste Verkehrsklasse. Dadurch wird insgesamt allerdings ein geringerer Durchsatz erzielt: Bei EY-NPMA (Abb. 3.11 b) sind bei hoher Netzauslastung die Verkehrsklassen mit niedriger Priorität überhaupt nicht mehr am Kanalzugriff beteiligt, wodurch die Konkurrenz kleiner wird und damit auch die Wahrscheinlichkeit für Kollisionen sinkt. Der Durchsatz steigt deshalb gegenüber 802.11e.

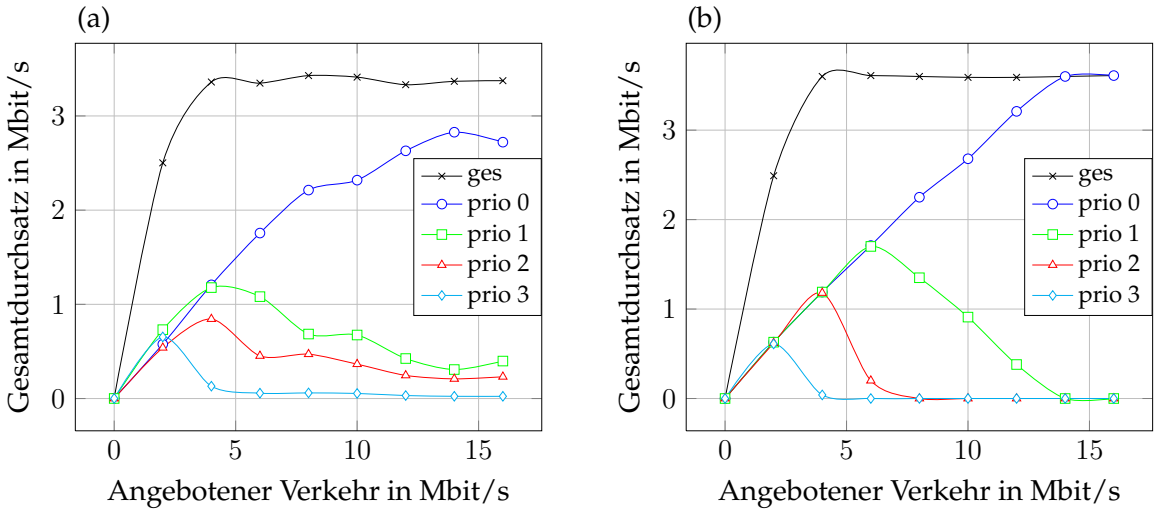


Abbildung 3.11: Vergleich unterschiedlicher Priorisierungsverfahren, Multihop-Szenario (links 802.11e, rechts EY-NPMA)

3.3 Beiträge dieser Arbeit

Hier sollen kurz die Beiträge dieser Arbeit und Neuerungen gegenüber bestehenden Ansätzen aufgezeigt werden.

Die beschriebenen Mechanismen sind Modifikationen von bereits bestehenden Verfahren, um deren Leistungsfähigkeit zu steigern. Die Ergebnisse sind in Kap. 3.2.3 ausführlich dargestellt. In der Literatur wurden die Mechanismen bislang nur unabhängig voneinander betrachtet. In Kap. 2.2.3 wurde jedoch bereits genauer erläutert, dass nur eine Kombination mehrerer Mechanismen in der Lage ist, tatsächlich Dienstgüte zu garantieren. Es gibt zwar bereits ganze Architekturen zur Bereitstellung von Dienstgüte, aber wie in Kap. 2.2.5 beschrieben besitzt keine davon alle grundlegenden Eigenschaften, die für den Einsatz in vermaschten drahtlosen Netzen notwendig sind.

Die besondere Stärke der hier vorgestellten QoS-Architektur ist ihre Flexibilität: Alle Mechanismen sind frei konfigurierbar hinsichtlich der speziellen Anforderungen. Deshalb ist sie nicht nur für ein spezielles Szenario bzw. einen gesonderten Betriebsfall einsetzbar, sondern individuell an die Gegebenheiten anpassbar. Aufgrund ihrer Modularität ist sie außerdem mit anderen Mechanismen und Systemen kombinierbar.

Auf die Frage, wie die Mechanismen für bestimmte Szenarien angepasst werden müssen, wird im folgenden Kapitel näher eingegangen.

4 Theoretische Analyse

Die Modellierung und analytische Auswertung bietet im Vergleich zu Simulationen eine Aufwandsreduzierung und einen Geschwindigkeitsgewinn bei der Auswertung von Ergebnissen. Deshalb eignet sie sich zur Optimierung von Parametern, was durch Simulation nur sehr aufwändig möglich wäre.

Basierend auf [13] soll hier ein Modell vorgestellt werden, welches geeignet ist, den Medienzugriff mathematisch zu beschreiben. Da die Verkehrskategorisierung die Parameter des Medienzugriffs beeinflusst, können diese nicht getrennt voneinander betrachtet werden. Deshalb wird hier ein gemeinsames Modell vorgestellt. Dieses Modell soll in der Lage sein, nicht nur IEEE 802.11 [63] und 11e [64] zu beschreiben, sondern auch eDCC [30] und PADCC [2].

4.1 Basismodell

Zunächst soll das zugrundeliegende Modell [13] kurz erläutert werden. Es besteht aus zwei Teilen, einem Modell für den Kanal und einem für die Stationen. Beide können anhand von Markovketten dargestellt werden.

Das Markovmodell des Kanals kennt zwei Zustände: *frei* und *belegt*, wobei die Übergangswahrscheinlichkeit von frei nach belegt als konstant angenommen und mit p_b bezeichnet wird (siehe Abb. 4.1).

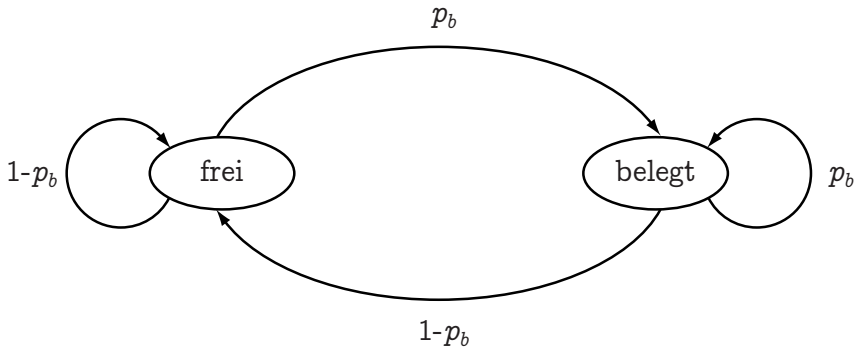


Abbildung 4.1: Markovmodell für den Kanal [13]

Das Verhalten der Stationen wird als zweidimensionaler stochastischer Prozess dargestellt:

$$\begin{aligned} X_k: \quad \mathbb{N} &\rightarrow \quad \mathbb{Z}^2 \\ \omega &\rightarrow \quad (j, b) \\ j &\in \quad \{0, \ldots, j_{\max}\} \\ b &\in \quad \{0, \ldots, b_{\max}\} \end{aligned}$$

Dabei wird einerseits der aktuelle Wert des Backoff-Counters b betrachtet, welcher angibt wie lang eine Station noch warten muss, bevor sie auf den Kanal zugreifen darf, andererseits der Backoff-Level j, also wie viele erfolglose Sendeversuche ein Paket bereits erlebt hat. Die Markovkette ist in Abb. 4.2 dargestellt. Jeder Zustand entspricht einem Zeitschritt, und beschreibt einen der folgenden möglichen Fälle:

- Der Kanal ist frei. Dieser Zustand hat die Länge eines Zeitschlitzes t_{Slot}.
- Der Kanal ist belegt. Dieser Zustand hat die Länge $t_{Daten} + t_{IFS} + t_{Slot} + t_{SIFS}$.

Die Länge eines Zeitschritts berechnet sich aus dem Mittelwert der Länge dieser möglichen Fälle, gewichtet mit der jeweiligen Wahrscheinlichkeit. Auf jeden Zustand (j, b) folgt der Zustand $(j, b-1)$, und sobald $b = 0$ erreicht ist, wird eine Übertragung gestartet. Ob diese erfolgreich ist, hängt davon ab, ob der Kanal in diesem Moment frei ist; die Wahrscheinlichkeit für eine erfolgreiche Übertragung ist also $(1 - p_b)$. Nach einer erfolgreichen Übertragung wird wieder im Zustand $(0, b)$ begonnen, wobei b zufällig aus $\{0, 1, \ldots, CW_0 - 1\}$ ausgewählt wird. Nach einer Kollision folgt als nächstes der Zustand $(j+1, b)$, wobei $b \in \{0, 1, \ldots, CW_{j+1} - 1\}$. CW_j bezeichnet die Fenstergröße im j-ten Backoff-Level.

Die Wahrscheinlichkeit, mit der eine Station im nächsten Zeitschritt eine Übertragung startet, wird als τ bezeichnet und hängt mit p_b über folgende Formel zusammen [13]:

$$p_b = 1 - (1 - \tau)^{m-1} \tag{4.1}$$

Dabei gibt m die Anzahl der Stationen an. Dies gilt unter der Annahme, dass p_b unabhängig ist von etwaigen vorherigen Kollisionen, sowie unabhängig von der Zeit, die vergangen ist, seit der Kanal zuletzt belegt war. Die Werte für p_b und τ können numerisch bestimmt werden (siehe auch Anhang D.3). Mit Hilfe der Annahme, dass jede Station immer ein Paket zu senden hat, kann auch der Systemdurchsatz berechnet werden:

$$Durchsatz = \frac{\mathrm{E}\left[gesendete\ Nutzdaten\ pro\ Zeitschritt\right]}{\mathrm{E}\left[Dauer\ eines\ Zeitschritts\right]} \tag{4.2}$$

Um das Verhalten von IEEE 802.11e analysieren zu können, sind Änderungen am zuvor vorgestellten Modell notwendig. In [29] wird ein Modell vorgeschlagen, welches intuitiver ist als das Originalmodell, da hier jeder Zeitschritt der Länge eines

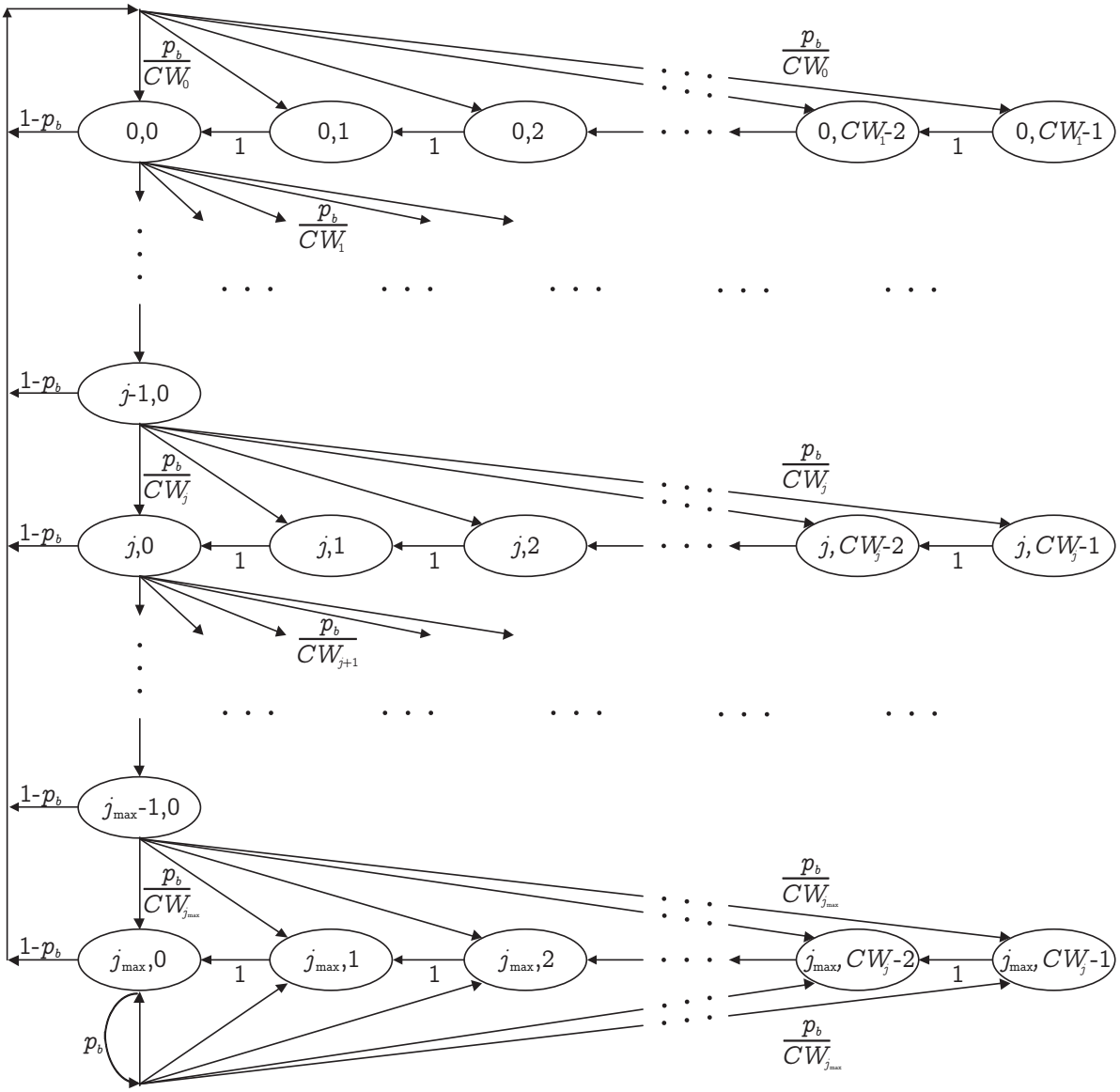


Abbildung 4.2: Markovkette nach [13]

Zeitschlitzes entspricht (in Abb. 4.3 ist ein Ausschnitt der Markovkette für einen Backoff-Level dargestellt). Gleichzeitig wird das vorige Modell erweitert, um mehrere Verkehrsklassen (Access Categories, AC) betrachten zu können. Dazu wird statt τ der Parameter τ_i für jede Verkehrsklasse AC_i eingeführt ($i \in \{0, 1, 2, 3\}$ bezeichnet die Priorität der AC, „0“ ist die höchste). Hierbei wurde in [29] jedoch nicht berücksichtigt, dass, aufgrund der unterschiedlichen Dauer des AIFS der einzelnen Verkehrsklassen, nach einer Übertragung oder Kollision die AC_i mit der höchsten Priorität als erstes wieder auf den Kanal zugreifen kann. Das resultiert in unterschiedlichen Sende- und Kollisionswahrscheinlichkeiten, abhängig von der Priorität der AC_i und der vorher durchlaufenen Zustände. p_b kann also nicht mehr als über alle Zeitschritte konstant angenommen werden. Dieses Problem wurde in [46], [50] und [47] adressiert, indem jede Verkehrsklasse durch eine eigene Markovkette modelliert wird. Das Modell nach [50] kann dabei auch den Längenunterschied zwischen einer erfolgreichen Übertragung und einer Kollision darstellen. Allerdings werden interne Kollisionen nur für die beiden niedrigsten Prioritäten betrachtet. Das Modell in [46] gibt den verschiedenen Verkehrsklassen andere Parameter als die in IEEE 802.11e definierten, und kommt deshalb mit zwei Modellen für die unterschiedlichen Verkehrsklassen aus. In [47] und [59] werden zwar interne Kollisionen berücksichtigt, aber dafür findet keine Unterscheidung zwischen Kollisionen und erfolgreichen Übertragungen statt. Eine weitere Neuerung gegenüber dem ursprünglichen Modell [13] ist, dass die Anzahl der Sendeversuche für jedes Paket begrenzt ist.

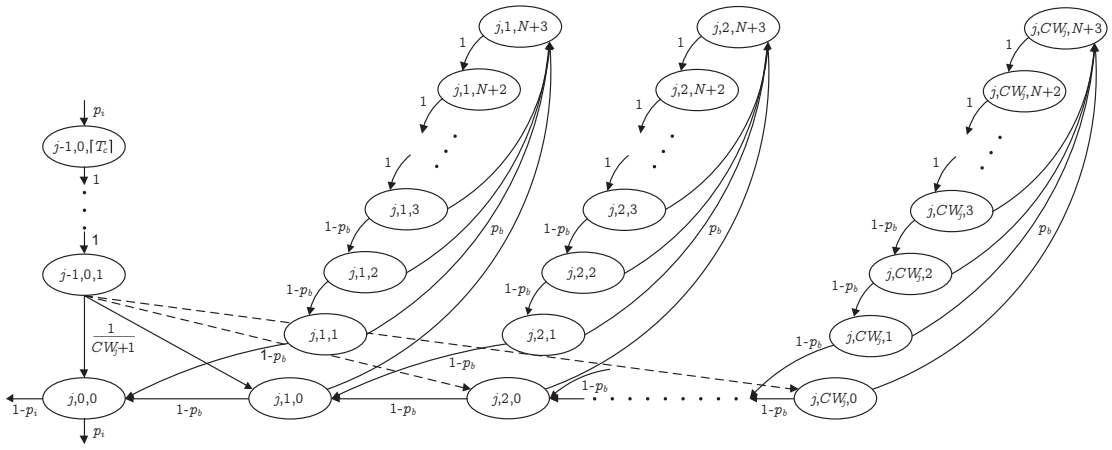


Abbildung 4.3: Ausschnitt der Markovkette nach [29]

Jedes der existierenden Modelle hat also Vor- und Nachteile. Keines ist jedoch in der Lage ist, PADCC zu beschreiben. Hierfür wurde im Rahmen dieser Arbeit ein neues Modell entworfen, welches Ideen aus den oben genannten Ansätzen kombiniert, um präzisere Ergebnisse zu liefern.

4.2 Modellformulierung

Basierend auf den oben genannten Modellen wurde ein verbessertes Modell entworfen, welches im Folgenden genauer beschrieben werden soll. Es gelten folgende Annahmen:

- Die Anzahl der Stationen m im System ist konstant und bekannt. Alle Stationen sind gleichartig.
- Die gesendeten Datenpakete haben eine feste Länge.
- Das System ist in Sättigung, d.h. jede Station hat in jeder Verkehrsklasse immer Pakete zu senden.
- Es wird von einem idealen Kanal ausgegangen, demnach werden Übertragungsfehler nur durch Kollisionen verursacht, nicht durch äußere Störeinflüsse. Wenn zwei Datenpakete kollidieren, gehen beide verloren.
- Alle betrachteten Stationen befinden sich in Sendereichweite, d.h. es wird ein Singlehop-Szenario betrachtet. Das bedeutet, dass das Hidden-Node-Problem (siehe Kap. 4.8.3) nicht auftreten kann, weil jede Station die Übertragungen aller anderen Stationen mithören kann.

Das Modell wird durch einen vierdimensionalen stochastischen Prozess X_k beschrieben:

$$\begin{aligned} X_k: \quad \mathbb{N} &\rightarrow \mathbb{Z}^4 \\ \omega &\rightarrow (j, b, s, t) \\ j &\in \{-1, \ldots, j_{\max}(i)\} \\ b &\in \{-2, \ldots, CW_j(i) - 1\} \\ s &\in \{-3, \ldots, A_i\} \\ t &\in \{0, \ldots, T\} \end{aligned}$$

Backoff-Level *j*: Nach jeder Kollision wird der Backoff-Level erhöht, bis die maximale Anzahl an Wiederholungen für das Paket erreicht ist (retry limit). Der Fall $j = -1$ bezeichnet den Post-Backoff, der nach jeder erfolgreichen Übertragung stattfindet, und in den Vorgängermodellen vernachlässigt wurde.

Backoff-Counter *b*: Zu Beginn wird b zufällig aus $\{0, 1, \ldots, CW_j(i) - 1\}$ gezogen und anschließend in jedem Zeitschlitz dekrementiert, wenn der Kanal frei ist. Die Zustände mit negativem Vorzeichen zeigen an, dass die AC_i gerade sendet, wobei $b = -2$ eine erfolgreiche Übertragung bedeutet und $b = -1$ eine Kollision. $CW_j(i) - 1$ ist der maximale Wert für die Fenstergröße im Backoff-Level j.

Verbleibende Zeit *s*: Wenn der Kanal belegt war, muss danach für die Dauer eines AIFS gewartet werden, bis der Kanal wieder als frei erkannt wird. Da $t_{AIFS}(i)$ von i abhängt, müssen Verkehrsklassen mit niedriger Priorität länger warten,

während solche mit höherer Priorität schon beginnen können, ihren Backoff-Counter zu dekrementieren. s gibt an, wie lange eine AC_i noch warten muss, bis der Kanal als frei erkannt wird, während andere Verkehrsklassen schon wieder senden dürfen. s kann demnach maximal

$$A_i = t_{AIFS}(i) - t_{AIFS}(i = 0) \tag{4.3}$$

sein. Das negative Vorzeichen zeigt auch hier Spezialfälle an, die weiter unten erklärt werden.

Vergangene Zeit *t:* Dieser Parameter hängt eng mit dem vorigen zusammen und dient hauptsächlich der Übersichtlichkeit bei der Berechnung. Abhängig davon, wieviel Zeit seit der letzten Übertragung bzw. Kollision vergangen ist, verändert sich die Anzahl der Verkehrsklassen, die auf den Kanal zugreifen können, und damit auch die Wahrscheinlichkeit für eine Kollision. t gibt die Anzahl der Zeitschlitze an, die seit der letzten Übertragung vergangen sind, abzüglich des kürzesten AIFS, also die Anzahl der Zeitschlitze, in denen prinzipiell eine Übertragung hätte starten können. Da von einem System in Sättigung ausgegangen wird, ist t nach oben beschränkt, weil spätestens nach dem Durchlaufen eines gesamten Backoffs eine Übertragung initialisiert wird.

Wie in [46] wird jede AC_i als eigene Markovkette dargestellt. Da Verkehrsklassen mit höherer Priorität eine bessere Chance haben, auf den Kanal zuzugreifen, kann die Kollisionswahrscheinlichkeit nicht mehr mit p_b gleichgesetzt werden, sondern es gibt eine eigene Kollisionswahrscheinlichkeit p_i für jede Verkehrsklasse i. Der Zusammenhang zwischen p_i und τ bzw. τ_i lässt sich wie folgt beschreiben:

$$\tau = 1 - \prod_i (1 - \tau_i) \tag{4.4}$$

$$p_i = 1 - \left((1 - \tau)^{m-1} \cdot \prod_{i' > i} (1 - \tau_{i'}) \right) \tag{4.5}$$

Die Gleichung 4.5 wurde dabei gegenüber [29] angepasst, um interne Kollisionen zu berücksichtigen. Abb. 4.4 zeigt einen Ausschnitt der Markovkette, nämlich den Übergang von b nach $b-1$ innerhalb eines Backoff-Levels der AC_2. Mit Wahrscheinlichkeit $1 - p(t)$ findet im betrachteten Zeitschlitz keine Übertragung statt. Das bedeutet, dass t um 1 erhöht wird, und gleichzeitig s um 1 erniedrigt (es sei denn, s ist bereits 0; in diesem Fall wird b um 1 erniedrigt). Mit Wahrscheinlichkeit $p(t)$ wird der Backoff im betrachteten Zeitschlitz unterbrochen. Hierbei sind verschiedene Fälle möglich, die durch verschiedenfarbige Pfeile dargestellt sind und weiter unten erläutert werden. Da die beiden niedrigen ACs einen längeren AIFS haben als die beiden höchsten Prioritäten, können sie unterbrochen werden, bevor der AIFS abgelaufen ist. In diesem

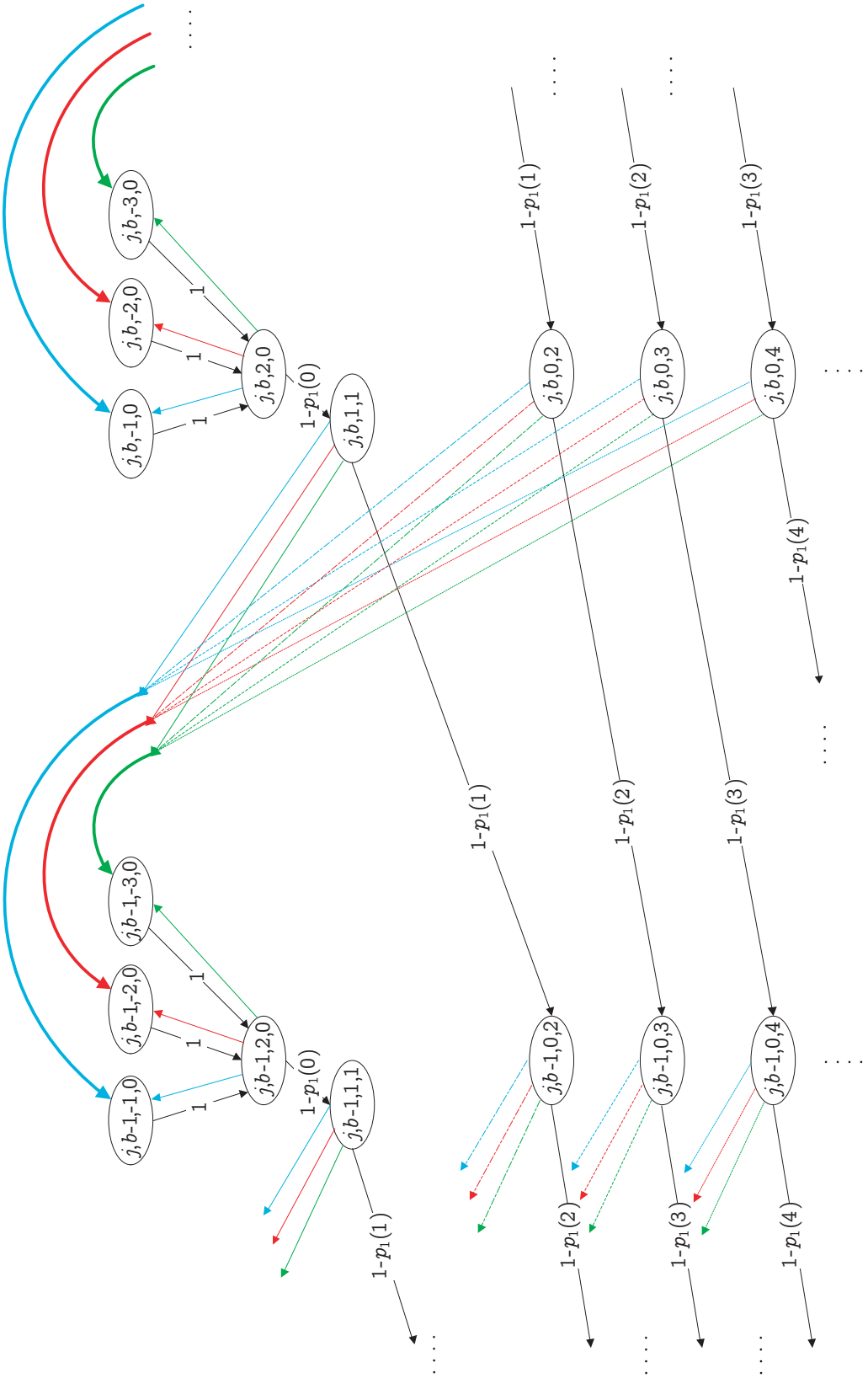


Abbildung 4.4: Ausschnitt aus dem Markovmodell für die AC_2

Fall ist $t = 0$ und der Backoff-Counter ändert sich nicht. Für $t \geq 1$ wird der Backoff-Counter auf jeden Fall im nächsten Schritt dekrementiert. Jeder der Zustandsübergänge, die durch farbige Pfeile dargestellt sind, hat eine eigene Wahrscheinlichkeit und muss einzeln berechnet werden. Die Formeln dazu finden sich im Anhang D.

Die Verwendung von Zeitschlitzen als Zustandsdauer erleichtert zwar das Verständnis, beeinflusst jedoch die Genauigkeit der Ergebnisse, da an einigen Stellen gerundet werden muss. Deshalb wurde hier darauf verzichtet und stattdessen jedem Zustand eine eigene Dauer zugeordnet. Die Zeitdauer einer erfolgreichen Übertragung setzt sich zusammen aus $t_{Daten} + t_{SIFS} + t_{ACK} + t_{AIFS}(i = 0) + A_i$. Während dieser Zeit sehen alle Stationen den Kanal als belegt, danach (abhängig von der Länge von A_i) wird er wieder als frei erkannt. Aufgrund der Annahmen für die Modellierung (alle Stationen können sich gegenseitig hören), können Kollisionen nur auftreten, wenn zwei oder mehr Stationen im selben Zeitschlitz mit einer Übertragung beginnen. Demnach enden die Übertragungsversuche der zwei (oder mehr) Stationen, deren Pakete kollidieren, gleichzeitig nach t_{Daten}. Alle Stationen, die nicht an der Kollision beteiligt sind, sehen den Kanal also lediglich für $t_{Daten} + t_{AIFS}(i)$ als belegt und anschließend wieder als frei, während die kollidierenden Stationen noch das ACK-Timeout abwarten müssen, welches laut Standard 222 µs entspricht [63]. Abhängig von der Zahl der Stationen, die in die Kollision verwickelt sind, ändert sich also die Zahl der Stationen, die direkt im Anschluss an eine Kollision auf den Kanal zugreifen können. Diese Anzahl wird im Folgenden als n bezeichnet. n ist eine Zufallsvariable, deren Verteilung von der Stationenzahl m, der Sendewahrscheinlichkeit τ und von t abhängt (siehe Anhang D.2, Formel D.14).

Im Markovmodell werden deshalb die folgenden Fälle unterschieden:

1. Kollision von Datenpaketen fremder Stationen: Die betrachtete AC_i erkennt den Kanal direkt im Anschluss an die Übertragung der Nutzdaten wieder als frei. Dieser Zustand wird mit $s = -1$ bezeichnet und hat die Dauer $T_c = t_{Daten} + t_{AIFS}(i = 0) + A_i$.

2. Erfolgreiche Übertragung: Unabhängig davon, ob eine andere AC der eigenen Station oder eine AC einer anderen Station sendet, muss die betrachtete AC_i die Quittung für das Paket abwarten bevor der Kanal wieder als frei erkannt wird. Der Zustand wird mit $s = -2$ bezeichnet und dauert $T_s = t_{Daten} + t_{SIFS} + t_{ACK} + t_{AIFS}(i = 0) + A_i$.

3. Kollision einer anderen $AC_{i'}$ der eigenen Station: Die sendende $AC_{i'}$ muss das ACK-Timeout abwarten und blockiert damit die anderen ACs derselben Station. Die betrachtete AC_i kann deshalb ebenfalls für die Länge des ACK-Timeout keine Übertragung starten. Dieser Zustand bekommt die Bezeichnung $s = -3$, die Dauer kann allerdings nur als Erwartungswert angegeben werden. Da ein Szenario unter Volllast vorausgesetzt wird, kann davon ausgegangen werden, dass vor dem Ablauf des ACK-Timeouts mindestens eine andere Übertragung

gestartet wird[1]. Diese Übertragung kann entweder erfolgreich sein oder in einer Kollision enden. Die Dauer T_v des Zustandes $s = -3$ ist demnach die Summe aus T_s, dem Erwartungswert der Dauer bis zum Beginn der nächsten Übertragung, sowie dem Erwartungswert der Dauer dieser Übertragung (abhängig davon, ob sie erfolgreich ist oder nicht). Die genaue Formel für den Erwartungswert findet sich in Anhang D.2, Formel D.15, als untere Grenze kann angegeben werden:

$$T_v \geq 2 \cdot t_{Daten} + t_{AIFS}(i = 0) \tag{4.6}$$

In der Literatur werden diese Unterschiede meistens vernachlässigt (siehe z.B. [47] oder [59]). In [29] werden zwar unterschiedliche Werte für T_s und T_c verwendet, die Autoren geben jedoch nicht an, wie diese berechnet werden.

Durch die möglichen Unterbrechungen im AIFS entstehen Schleifen in der Markovkette, was eine direkte Berechnung der stationären Wahrscheinlichkeiten verhindert. Deshalb muss auf eine iterative Berechnungsmethode zurückgegriffen werden. Aufgrund der Endlichkeit des Zustandsraums kann die Markovkette als stochastische Matrix dargestellt werden, wobei die stationären Wahrscheinlichkeiten den Linkseigenvektor der Matrix zum Eigenwert $\lambda = 1$ bilden. Zunächst sind die Einträge der Matrix jedoch nicht bekannt, da diese von τ abhängen, welches wiederum erst aus der stationären Verteilung bestimmt werden kann. Deshalb muss die Matrix mit geeigneten Startwerten initialisiert werden. Die Berechnung des Eigenvektors für diese Matrix ergibt dann genauere Werte für τ, um im nächsten Schritt eine neue Matrix zu erstellen, die näher an den korrekten Werten ist. So können iterativ die stationären Wahrscheinlichkeiten approximiert werden. Ob eine Lösung gefunden wird, hängt dabei von den Startwerten ab. Das Verfahren kann auch zu divergentem Verhalten oder dem Oszillieren zwischen mehreren Konstellationen führen.

Theoretisch ließe sich der Eigenvektor der stochastischen Matrix exakt berechnen, was jedoch mit hohem Rechenaufwand verbunden ist. Außerdem ist die Matrix dafür im Allgemeinen zu groß (die Markovkette hat je nach Verkehrsklasse zwischen 1500 und 200000 Zustände), und die Einträge des Vektors addieren sich definitionsgemäß zu 1. Daher sind die einzelnen Einträge sehr klein, wodurch man schnell an die Grenzen der Maschinengenauigkeit stößt. Die Ergebnisse der Eigenvektorberechnung werden jedoch im nächsten Iterationsschritt weiterverwendet, sodass der Fehler sich fortpflanzt.

Deshalb wurde hier ein anderes Verfahren angewandt, welches äquivalente Präzision bei erheblich geringerem Rechenaufwand liefert. Dazu wird zunächst das Markovmodell des Kanals genauer betrachtet und um einen Zustand erweitert (Abb. 4.5).

[1] Ein ACK-Timeout dauert ungefähr 11 Zeitschlitze; demnach müssten alle Stationen, die gerade nicht an der Kollision beteiligt sind, einen restlichen Backoff von mehr als 11 haben. Der maximale Backoff der höchsten Priorität beträgt 15 Zeitschlitze, der durchschnittliche Wert ist also selbst bei Volllast weniger als acht. Die Wahrscheinlichkeit dafür, dass keine Übertragung stattfindet, ist demnach verschwindend gering, und die Berücksichtigung dieses Falls würde keinen Genauigkeitsgewinn für das Modell bedeuten.

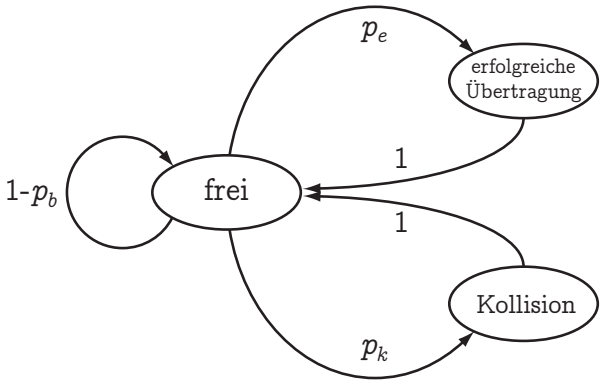


Abbildung 4.5: Neues Markovmodell für den Kanal

Das neue Modell unterscheidet bei belegtem Kanal, ob es sich um eine erfolgreiche Übertragung oder eine Kollision handelt. Dadurch wird eine präzisere Berechnung ermöglicht. Die Wahrscheinlichkeit für p_b, dass der Kanal vom Zustand *frei* in den Zustand *belegt* übergeht, setzt sich dann aus den Wahrscheinlichkeiten für eine Übertragung und eine Kollision zusammen:

$$p_b = p_k + p_e \tag{4.7}$$

Daraus ergibt sich mit Formel 4.4:

$$\begin{aligned} p_b &= 1 - (1-\tau)^n \\ p_e &= n \cdot \tau \cdot (1-\tau)^{n-1} \\ p_k &= p_b - p_e \end{aligned} \tag{4.8}$$

Mit Hilfe dieser Formeln lässt sich n bestimmen (siehe Anhang D.2, Formel D.14).

4.3 Erweiterung des Modells für eDCC und PADCC

Soweit bekannt, gibt es für den eDCC-Mechanismus [30] noch keine mathematischen Untersuchungen. Da eDCC eine Erweiterung des Medienzugriffs nach 802.11e ist, ist es möglich, das oben beschriebene Markovmodell entsprechend zu erweitern, sodass eine Analyse von eDCC damit möglich ist. PADCC und eDCC unterscheiden sich nur in der Berechnung der Sendewahrscheinlichkeit PT. Deshalb ist das Modell bis auf diesen Parameter für beide Mechanismen gültig.

Entsprechend der Definition des eDCC-Mechanismus wird in dem Moment, in dem eine Übertragung begonnen werden kann, mit Wahrscheinlichkeit PT die Übertragung gestartet, mit Wahrscheinlichkeit $(1 - PT)$ wird stattdessen direkt in eine virtuelle Kollision übergegangen (siehe Kap. 2.2.4 und 3.1.3). Für die Bestimmung

von PT ist der Parameter SU erforderlich, der eine Abschätzung der Kanalbelegung darstellt. Da die Kanalbelegung mit Hilfe des Markovmodells berechnet werden kann, ist hier jedoch keine Abschätzung notwendig, sondern es kann der tatsächliche Wert, nämlich die Kollisionswahrscheinlichkeit p_i, verwendet werden. Das ist eine Idealisierung und entspricht dem Fall, dass eine perfekte Abschätzung möglich ist. Gleichzeitig ändert sich damit allerdings die Formel für die Berechnung von p_i, da die virtuellen Kollisionen, die durch eDCC hervorgerufen werden, mit berücksichtigt werden müssen:

$$p_i(j) = 1 - PT(i,j) \cdot (1-\tau)^{n-1} \prod_{i'>i} (1-\tau_{i'}) \tag{4.9}$$

PT hängt jetzt von p_i ab und umgekehrt. Da PT nicht nur von der Verkehrsklasse i abhängt, sondern auch vom Backoff-Level j, ist jetzt auch p_i von j abhängig. Das erfordert eine Anpassung der Berechnung im Markovmodell, beeinträchtigt aber nicht die Berechenbarkeit. Dabei muss berücksichtigt werden, dass es jetzt einen zusätzlichen Fall gibt, wenn nämlich der Kanal frei bleibt, weil alle Stationen, die gerade senden wollen, darauf verzichten.

Für den Fall, dass für SU nicht der idealisierte Wert verwendet werden soll, gibt es auch die Möglichkeit, ihn entsprechend Formel 2.1 zu bestimmen.

Im Folgenden sei p_i^{dekr} die Wahrscheinlichkeit dafür, dass der Backoff in einem beliebigen Dekrementierungsschritt unterbrochen wird:

$$p_i^{dekr} = \mathrm{E}_t \left[1 - \left((1-\tau)^{n-1} \cdot \prod_{i' \neq i} (1-\tau_{i'}) \right) \right] \tag{4.10}$$

Damit gilt:

$$\begin{aligned} SU_{i,j}(t) &= \frac{CW_j(i) - (t - A_i) - 1}{CW_j(i) - (t - A_i)} \cdot \frac{p_i^{dekr} \cdot \frac{CW_j(i)-(t-A_i)-1}{2}}{\frac{CW_j(i)-(t-A_i)+1}{2}} \\ &= \frac{p_i^{dekr} \cdot (CW_j(i) - (t - A_i) - 1)^2}{(CW_j(i) - (t - A_i) + 1) \cdot (CW_j(i) - (t - A_i))} \end{aligned} \tag{4.11}$$

Für die Verkehrsklasse(n) mit dem kleinsten AIFS ist $A_i = 0$. Außerdem gilt: Wenn $t \neq b_{\text{init}}$ (dem Initialwert von b) ist, dann ist sicher, dass eine Unterbrechung stattgefunden hat. Formel 4.11 kann dann wie folgt geschrieben werden:

$$\begin{aligned} SU_{i,j}(t \mid A_i = 0) &= \frac{CW_j(i) - t - 1}{CW_j(i) - t} \cdot \frac{1 + p_i^{dekr} \cdot \frac{CW_j(i)-t-2}{2}}{\frac{CW_j(i)-t+1}{2}} \\ &= \frac{CW_j(i) - t - 1}{CW_j(i) - t} \cdot \frac{2 + p_i^{dekr} \cdot (CW_j(i) - t - 2)}{CW_j(i) - t + 1} \end{aligned} \tag{4.12}$$

4.4 Schlussfolgerungen

Das oben beschriebene Modell ermöglicht die Berechnung von Durchsatz und Verzögerung in Abhängigkeit der Eingangsparameter. Wenn die Anzahl der Stationen im System bekannt ist, kann für eine gegebene MAC-Konfiguration der durchschnittliche Durchsatz bestimmt werden. Andersherum ist es jedoch auch möglich, aus einer Reihe verschiedener Konfigurationen diejenige auszusuchen, die bei fester Stationenzahl beispielsweise den Durchsatz maximiert.

Der Gesamtdurchsatz S_g des Systems ist der Anteil der Zeit, in dem erfolgreiche Übertragungen stattfinden, multipliziert mit der Paketgröße und geteilt durch die Dauer für die Übertragung der Nutzdaten eines Pakets.

$$S_g = \frac{\textit{Zeit(erfolgreiche Übertragung)}}{\textit{Gesamtzeit}} \cdot \frac{\textit{Paketgröße}}{T_s} \tag{4.13}$$

Paketgröße und Übertragungsdauer sind bekannt, interessant ist also der erste Faktor. In Abhängigkeit von t kann angegeben werden, wie lange es dauert, bis das System vom Zustand *frei* wieder in den Zustand *frei* übergeht:

$$\mathrm{E}_t[\textit{Gesamtdauer}] = \mathrm{E}_t[T_f + p_e(t) \cdot T_s + p_k(t) \cdot T_c], \tag{4.14}$$

wobei $p_e(t)$ und $p_k(t)$ jeweils die stationären Wahrscheinlichkeiten in Abhängigkeit von t bezeichnen. T_f ist die Zeitdauer, in der der Kanal frei ist. Der Erwartungswert von T_f lässt sich aus dem kürzesten AIFS und der Anzahl freibleibender Zeitschlitze, deren Erwartungswert von der Verteilung von t abhängt, berechnen. Der Anteil der Zeit, die mit erfolgreichen Übertragungen zugebracht wird, ist $\mathrm{E}_t[p_e(t)] \cdot T_s$. Damit ergibt sich:

$$\mathrm{E}_t[S_g] = \frac{\mathrm{E}_t[p_e(t)] \cdot T_s}{\mathrm{E}_t[\textit{Gesamtdauer}]} \cdot \frac{\textit{Paketgröße}}{T_s} = \frac{\mathrm{E}_t[p_e(t)] \cdot \textit{Paketgröße}}{\mathrm{E}_t[\textit{Gesamtdauer}]} \tag{4.15}$$

Wenn die Verteilung von t bekannt ist, welche aus den stationären Wahrscheinlichkeiten des Markovmodells für die einzelnen Verkehrsklassen abgelesen werden kann, kann der Gesamtdurchsatz bestimmt werden, indem über die einzelnen t summiert wird:

$$S_g = \sum_{T=0}^{t_{\max}} S_g(T) \cdot P(t = T) \tag{4.16}$$

Da alle Stationen das gleiche Verhalten aufweisen, ergibt sich der Durchsatz einer einzelnen Station zu:

$$S_m = \frac{S_g}{m} \tag{4.17}$$

Um den Durchsatz einer einzelnen Verkehrsklasse zu bestimmen, wird zunächst die Wahrscheinlichkeit τ_i^{net} eingeführt. τ_i^{net} gibt an, mit welcher Wahrscheinlichkeit die

AC_i eine Übertragung startet, ohne dass eine $AC_{i'}$ mit höherer Priorität gleichzeitig eine Übertragung beginnt:

$$\tau_i^{\text{net}}(t) = \tau_i(t) \cdot \left(1 - \prod_{i'>i}(1 - \tau_{i'}(t))\right) \tag{4.18}$$

Damit lässt sich in Abhängigkeit von t angeben, mit welcher Wahrscheinlichkeit κ_i eine stattfindende Übertragung von Verkehrsklasse i stammt:

$$\kappa_i(t) = \frac{\tau_i^{\text{net}}(t)}{\sum_i \tau_i^{\text{net}}(t)} \tag{4.19}$$

Der Gesamtdurchsatz pro Verkehrsklasse folgt dann wiederum aus der Verteilung von t:

$$S_i = S_m \cdot \sum_{T=0}^{t_{\max}} \kappa_i(T) \cdot P(t = T) \tag{4.20}$$

Die durchschnittliche Verzögerung D_i eines Pakets, also die Zeit zwischen Initialisierung des ersten Backoffs des Pakets und Verlassen des Systems nach erfolgreicher Übertragung, kann mit Hilfe von ein paar Überlegungen ebenfalls angegeben werden.

λ_i bezeichnet die Paketverlustrate der Verkehrsklasse i. Ein Paket, welches verloren geht, kollidiert in jedem Backoff-Level einschließlich dem letzten und wird am Ende verworfen. Im Erwartungswert wird eines von $\frac{1}{1-\lambda_i}$ Paketen erfolgreich übertragen. Die Zeit, die zwischen zwei erfolgreichen Übertragungen von Paketen der Verkehrsklasse i vergeht, wird mit Δ_i bezeichnet und berechnet sich aus:

$$\Delta_i = \frac{\textit{Paketgröße}}{S_i} \tag{4.21}$$

Wenn man Δ_i und λ_i miteinander in Relation setzt, kann man daraus D_i berechnen:

$$\Delta_i = D_i + \left(\frac{1}{1-\lambda_i} - 1\right) \cdot D_i^l, \tag{4.22}$$

wobei D_i^l die Zeit bezeichnet, die vergeht bis ein Paket endgültig verloren ist. D_i und D_i^l setzen sich aus dem Erwartungswert der Anzahl an Kollisionen und dem Erwartungswert der im Backoffprozess vebrachten Zeit zusammen. Die im Backoffprozess verbrachte Zeit ist wiederum abhängig vom Erwartungswert des Initialisierungswertes von b und dem Erwartungswert der Zeit, die für einen Übergang von b nach $b-1$ benötigt wird ($\mathrm{E}_i[D_i^d]$). Die Formeln hierfür finden sich im Anhang D.2.

4.5 Neuerungen gegenüber vorherigen Modellen

Das hier beschriebene Modell zur analytischen Untersuchung von IEEE 802.11e [64] und PADCC [2] baut auf bereits vorhandenen Modellen auf und erweitert diese. Die

Unterschiede zu den Vorgängermodellen seien im Folgenden kurz zusammengefasst. Bislang gab es kein Modell, welches alle genannten Punkte mit einbezieht.

- Erweiterung des Markovmodells für den Kanal: Unterscheidung zwischen Kollision und erfolgreicher Übertragung
- genauere Berechnung der Wartezeiten in Bezug auf Übertragung und Kollision
- Unterbrechung während des AIFS (siehe auch [46], [50] und [47])
- Berechnung von p_b, sodass interne Kollisionen korrekt berücksichtigt werden (siehe auch [47] und [59])
- Verzicht auf Rundung und somit Erhöhung der Präzision der Ergebnisse
- Berücksichtigung des Post-Backoff
- Berücksichtigung der Tatsache, dass Stationen direkt nach einer eigenen Kollision die nächste Übertragung nicht beeinflussen können
- Möglichkeit der Modellierung von eDCC und PADCC

Für die Untersuchung von PADCC war es notwendig, ein neues Modell zu entwickeln. Dabei wurden die genannten Punkte mit berücksichtigt, um mit vertretbarem Rechenaufwand möglichst realistische Ergebnisse zu erhalten.

4.6 Ergebnisse

Die Ergebnisse aus der mathematischen Analyse sollen hier mit Simulationsergebnissen verglichen werden.

4.6.1 Simulator

Die Simulationen wurden mit einem eigenen MAC-Schicht-Simulator (*Simbo*, siehe Anhang C) durchgeführt, da der im vorigen Kapitel verwendete Simulator ns-2 [81] für den Vergleich nicht gut geeignet ist. Im Gegensatz zum ns-2 wird in Simbo nur der Medienzugriff modelliert. Dadurch werden die Ergebnisse nicht durch Effekte, die beispielsweise durch das Routing oder die physikalische Schicht hervorgerufen werden, beeinflusst. Gleichzeitig verringert sich durch die Verwendung eines kompakteren Simulators die Komplexität der Simulationen und damit auch die Simulationszeit. Um die Ergebnisse in Relation zu setzen, ist am Ende dieses Kapitels der Vergleich mit dem ns-2 dargestellt (siehe Abb. 4.8).

In den Simulationen soll nur der Medienzugriff untersucht werden. Es werden m Stationen dargestellt, von denen jede immer ein Paket zu senden hat. Da sich alle in Sendereichweite befinden, finden Kollisionen genau dann statt, wenn zwei Stationen

gleichzeitig mit dem Senden beginnen. Jede Station wählt eine Backofflänge b zufällig aus $\{0, 1, \ldots, CW_j(i) - 1\}$. In jedem Zeitschritt tritt genau einer der folgenden Fälle ein:

1. Genau eine Station hat ihren Backoff beendet.
2. Mehrere Stationen haben ihren Backoff beendet.
3. Keine Station hat ihren Backoff beendet.

Der 1. Fall bedeutet, dass die betreffende Station erfolgreich senden kann. Die Station wählt dann eine neue Backofflänge, und die Anzahl der erfolgreich gesendeten Pakete wird um 1 erhöht. Im 2. Fall findet eine Kollision statt, die betroffenen Stationen erhöhen ihren Backoff-Level und wählen eine neue Backofflänge. Außerdem wird die Anzahl der kollidierten Pakete um je 1 pro beteiligter Station erhöht. Im 3. Fall bleibt der Kanal frei, alle Stationen dekrementieren ihren Backoff, und die Anzahl leerer Zeitschlitze erhöht sich um 1. Am Ende der Simulation werden die Parameter ausgewertet. Diese sind analog zu Kap. 3.2.2 Durchsatz, Verzögerung, Paketverlustrate und zusätzlich noch die Kollisionsrate der Pakete. Letztere berechnet sich nach folgender Formel:

$$\textit{Kollisionsrate} = \frac{\textit{nicht erfolgreiche Sendeversuche}}{\textit{Gesamtzahl der Sendeversuche}} \tag{4.23}$$

Um die Verzögerung zu berechnen, muss die Anzahl der Wiederholungen der einzelnen Pakete bekannt sein sowie die Zeit, die eine Übertragung bzw. eine Kollision dauert.

4.6.2 Vergleich zwischen Analyse und Simulation

In Abb. 4.6 ist ein Vergleich zwischen Simulationsergebnissen und Analyse dargestellt. „S“ steht dabei immer für Simulation, „A“ für Analyse. Je mehr Stationen sich in Sendereichweite befinden, desto höher ist die Kollisionswahrscheinlichkeit der gesendeten Pakete (Abb. 4.6 b; es wird von einem System in Sättigung ausgegangen). Deshalb steigen mit der Zahl der Stationen auch die Paketverlustrate (Abb. 4.6 d) und die Verzögerung (Abb. 4.6 c), während der Durchsatz absinkt (Abb. 4.6 a). Wenn Paketverlustraten von maximal 10% bis 20% nicht überschritten werden sollen, sind Szenarien nur bis maximal zehn Stationen sinnvoll.

Auch bei Verwendung von PADCC steigt die Kollisionsrate mit der Anzahl der Stationen (Abb. 4.7 b). Der Durchsatz sinkt hier allerdings nicht ganz so stark ab wie bei reinem 802.11e, und es ist generell ein etwas höherer Durchsatz zu beobachten (Abb. 4.7 a). Die Unterschiede zwischen Simulation und Analyse sind hier deutlicher als ohne PADCC. Das liegt daran, dass bei der Berechnung die Sendewahrscheinlichkeit PT iterativ angenähert wird, während bei der Simulation vorher ein durchschnittlicher Wert angegeben wird. Das führt zu Abweichungen im Ergebnis, welche insbesondere bei hohen Stationenzahlen ins Gewicht fallen. Bei Betrachtung von Paketverlustraten bis maximal 20% sind Stationenzahlen über zwölf nicht sinnvoll.

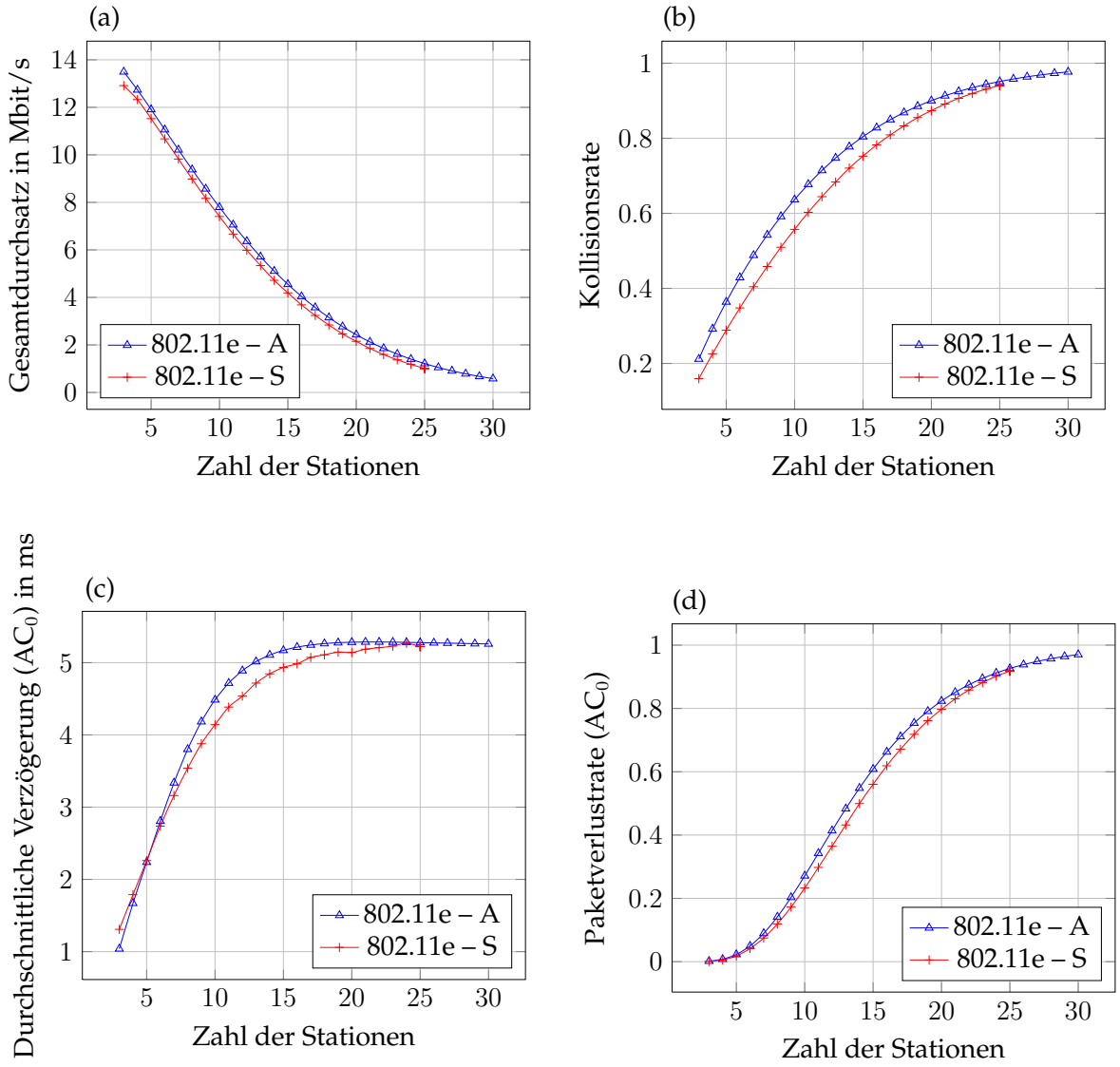


Abbildung 4.6: Vergleich zwischen Analyse und Simulation

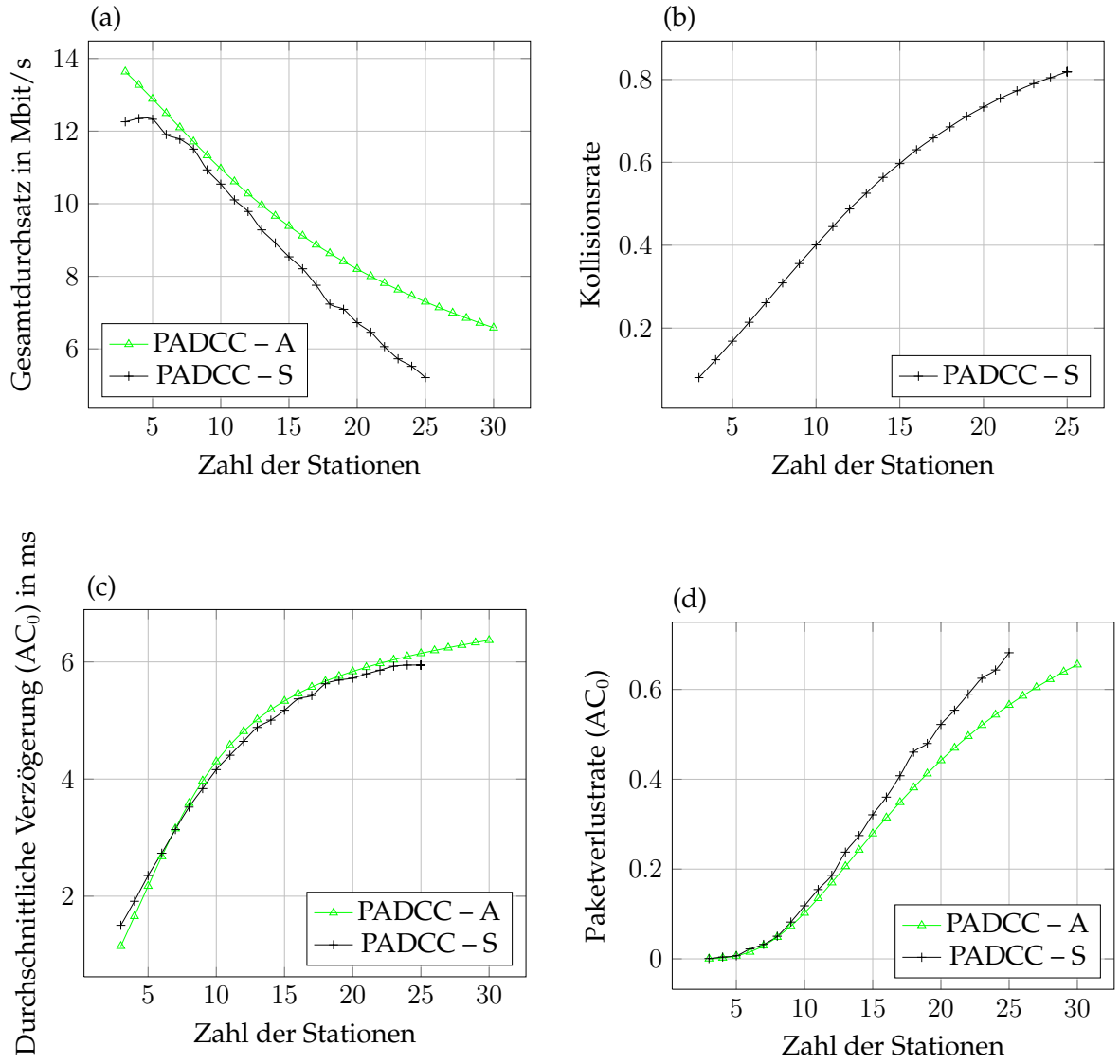


Abbildung 4.7: Vergleich zwischen Analyse und Simulation – PADCC

Abb. 4.8 zeigt den Vergleich mit dem Simulator ns-2. Hierfür wurden die in Kap. 3.2 beschriebenen Simulationsparameter (Singlehop-Szenario) verwendet, wobei diesmal die Sendedatenrate je Station fest auf 2,5 Mbit/s eingestellt wurde und stattdessen die Zahl der Stationen variiert. Der ns-2 zeigt qualitativ das gleiche Verhalten wie die Ergebnisse von Analyse und Simbo. Der etwas niedrigere Durchsatz und die höhere Verzögerung lassen sich dadurch erklären, dass im ns-2 unter anderem die Signalisierungsnachrichten des Routingprotokolls mit berücksichtigt werden. Diese beeinflussen die Simulationsergebnisse und führen zu geringfügig schlechteren Ergebnissen.

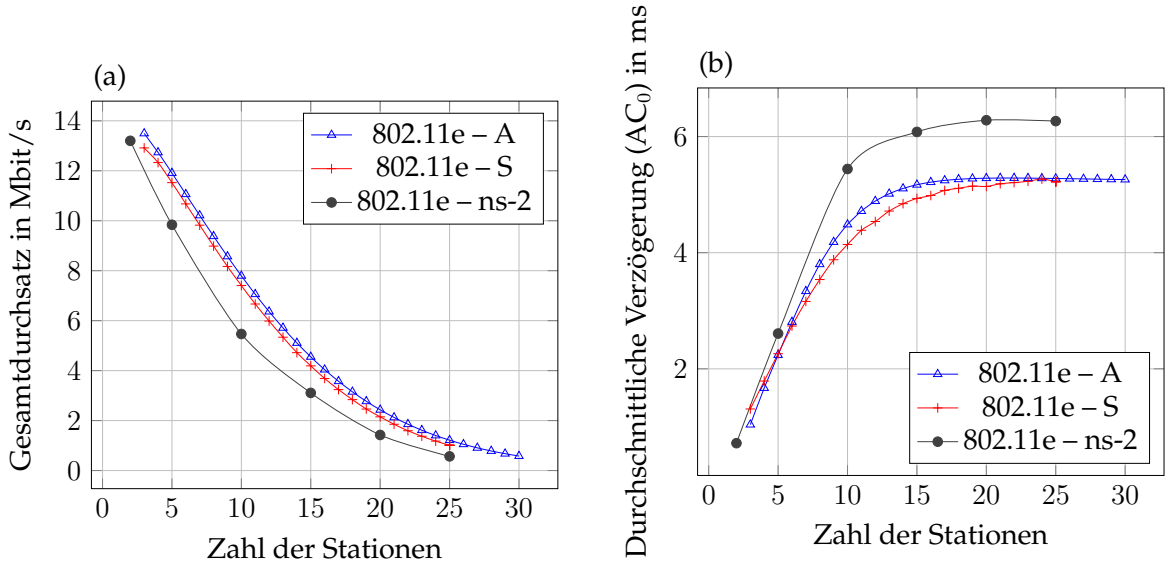


Abbildung 4.8: Vergleich zwischen Analyse, Simbo und ns-2

4.7 Konsequenzen

Mit Hilfe des Markov-Modells ist es möglich, für beliebige MAC-Parametersätze in Abhängigkeit der Stationenzahl m Durchsatz, Verzögerung und Paketverlustrate zu berechnen. Daraus kann man für gegebenes m z.B. den Durchsatz maximieren, indem man die entsprechenden MAC-Parameter (Fenstergröße *CW* und IFS) auswählt.

In Kap. 3.1.2 wurde bereits darauf eingegangen, dass es sinnvoller ist, die Fenstergröße zu verändern als die Dauer des Interframe Space. Um verwertbare Ergebnisse zu erhalten, sollen die Parameter innerhalb der im Standard definierten Grenzen bleiben. Nach [64] gilt für alle i und j: $CW_j(i) = 2^k - 1, k \in \mathbb{N}$. Die Berechnungsvorschrift für die minimale und maximale Fenstergröße der einzelnen Verkehrsklassen findet sich in Tab. 4.1.

Hier sollen nur Werte betrachtet werden mit $2^4 - 1 \leq CW_{\min} \leq CW_{\max} \leq 2^{10} - 1$.

Tabelle 4.1: Berechnungsvorschrift für CW-Werte der einzelnen Verkehrsklassen

i	$CW_{\min}(i)$	$CW_{\max}(i)$
0	$\frac{CW_{\min}+1}{4} - 1$	$\frac{CW_{\min}+1}{2} - 1$
1	$\frac{CW_{\min}+1}{2} - 1$	$CW_{\min}$
2	$CW_{\min}$	$CW_{\max}$
3	$CW_{\min}$	$CW_{\max}$

Die Ergebnisse für die Optimierung sind in Abb. 4.9 und 4.10 (mit und ohne PADCC) zu sehen.

Die einzelnen Farben stellen dabei unterschiedliche $CW_{\min}$ dar. Die unterschiedlichen $CW_{\max}$ sind mit eingezeichnet, aber in der Legende nicht aufgeschlüsselt, da sie nur wenig Auswirkung auf die Gesamtperformance haben. Deutliche Unterschiede zwischen den einzelnen $CW_{\min}$ wirken sich nur auf die niedrigen Prioritäten aus, wie in Abb. 4.9 e dargestellt. Hier ist beispielhaft für $CW_{\min} = 127$ die Aufschlüsselung der $CW_{\max}$ eingetragen. Insgesamt gilt: Für niedrige Prioritäten ist es vorteilhaft, wenn $CW_{\max}$ möglichst niedrig und $CW_{\min}$ relativ hoch ist (Abb. 4.9 e). Für höhere Prioritäten führen tendenziell kleinere $CW_{\min}$ zu besseren Ergebnissen (Abb. 4.9 c).

Kleine Fenstergrößen haben insgesamt eine geringere durchschnittliche Verzögerung (Abb. 4.9 b), aber dafür eine höhere Verlustrate (Abb. 4.9 d) zur Folge. Das liegt daran, dass ein kürzerer Backoff kürzere Wartezeiten vor dem Senden bedeutet, gleichzeitig steigt bei kürzerem Backoff allerdings die Wahrscheinlichkeit, dass mehrere Stationen gleichzeitig mit dem Senden beginnen, was zu einer höheren Kollisionsrate führt.

Um den Gesamtdurchsatz zu maximieren, sollte $CW_{\min}$ entsprechend Abb. 4.9 a ausgewählt werden, wobei darauf zu achten ist, dass die jeweilige Paketverlustrate akzeptabel ist. Da die Anpassung von $CW_{\max}$ kaum Auswirkung auf den Gesamtdurchsatz hat, aber starke Auswirkungen auf den Durchsatz der niedrigen Prioritäten, sollte dieser Parameter möglichst niedrig gewählt werden (es muss gelten: $CW_{\max} \geq CW_{\min}$). Ergebnisse für $m > 15$ sind nicht eingezeichnet, können aber ebenfalls berechnet werden. Eine Auflistung der optimalen Werte für unterschiedliche Stationenzahl m ist in Tab. 4.2 angegeben. Dabei ist $c_{\min} := \mathrm{ld}(CW_{\min} + 1)$ und $c_{\max} := \mathrm{ld}(CW_{\max} + 1)$.

Tabelle 4.2: Optimierte CW-Werte

m		3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
11e	$c_{\min}$	5	6	6	7	7	7	7	7	8	8	8	8	8	8	9	9	9	9
	$c_{\max}$	5	6	6	7	7	7	7	7	8	8	8	8	8	8	9	9	9	9
PADCC	$c_{\min}$	5	5	5	6	6	6	6	6	6	6	7	7	7	7	7	7	8	8
	$c_{\max}$	5	5	5	6	6	6	6	6	6	6	7	7	7	7	7	7	8	8

Bei Einsatz von PADCC (Abb. 4.10) sind die optimalen Werte für die Fenstergröße etwas niedriger. Das lässt sich einfach erklären: Abhängig von der Netzauslastung

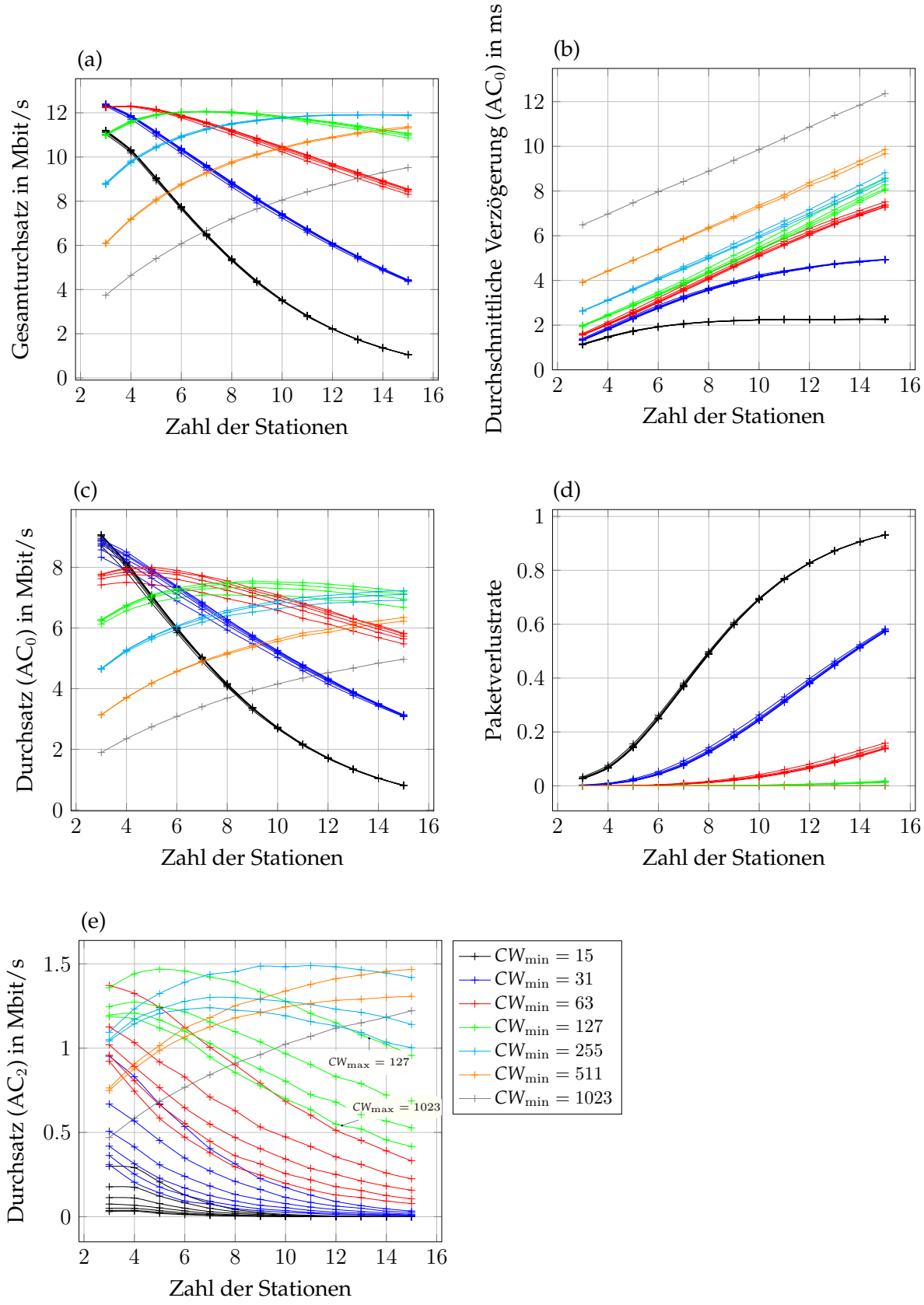


Abbildung 4.9: Optimierungsergebnisse ohne PADCC

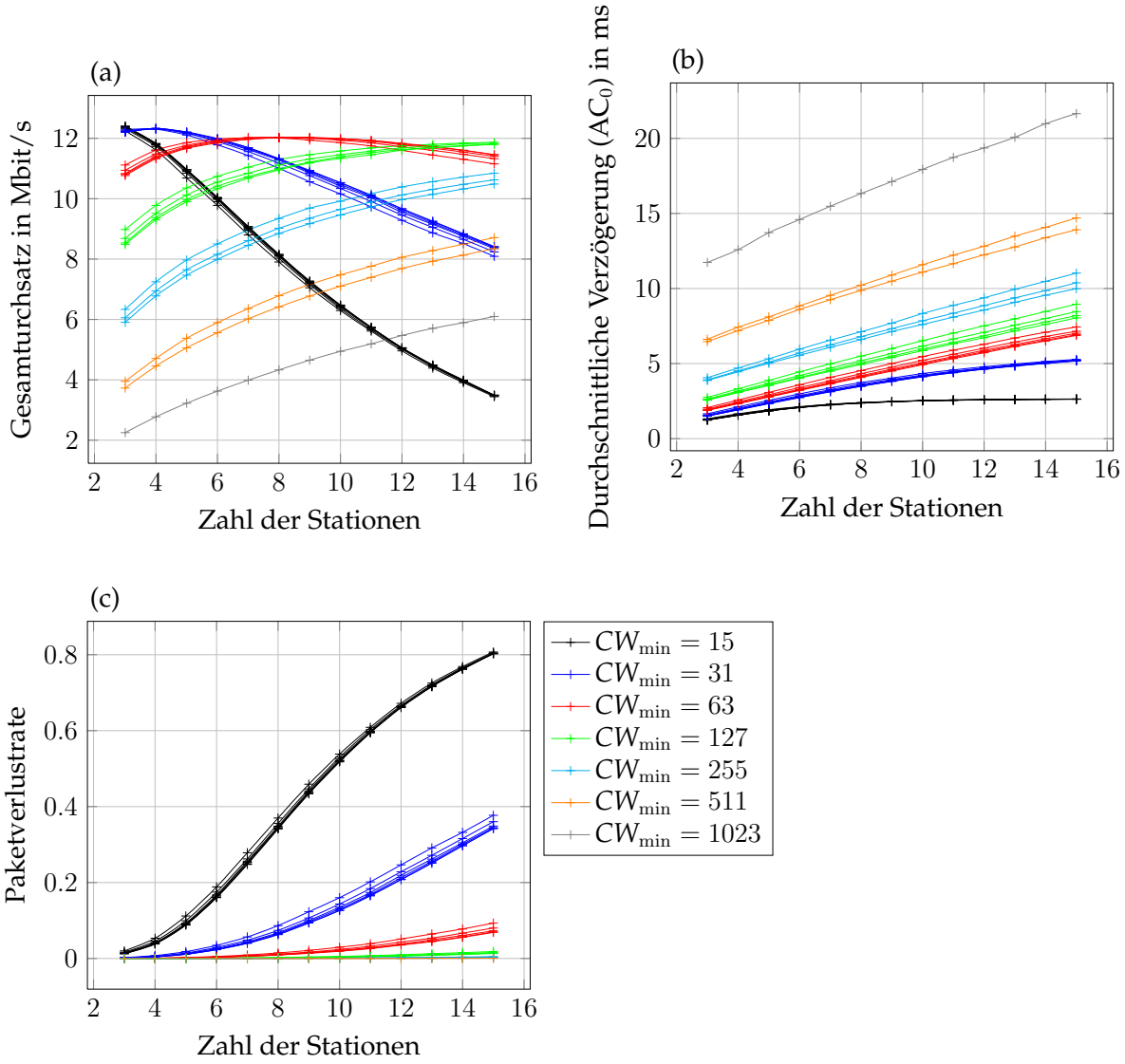


Abbildung 4.10: Optimierungsergebnisse mit PADCC

verzichtet eine Station ab und zu darauf, ein Paket zu senden, und startet stattdessen einen neuen Backoff für dasselbe Paket. Dadurch wird einerseits die durchschnittliche Verzögerung der Pakete größer, andererseits wird auch der Backoff implizit länger, da dieser unter Umständen zweimal durchlaufen wird bevor das Paket zum ersten Mal gesendet wird. PADCC bewirkt demnach, dass bei gleichem *CW* die Wartezeit bis zum ersten Senden länger ist als bei normalem 802.11e. Deshalb ist die optimale Fenstergröße hier etwas niedriger.

Um die optimale Konfiguration nutzen zu können, muss die Zahl der Stationen bekannt sein. Abb. 4.11 zeigt die Ergebnisse für den Gesamtdurchsatz, falls die Zahl der Stationen nicht genau bekannt ist, und um 2 bzw. 4 zu groß (gepunktet) oder zu klein (gestrichelt) geschätzt wird. Als Vergleich ist auch der Gesamtdurchsatz eingezeichnet für den Fall, dass keine Optimierung verwendet wird.

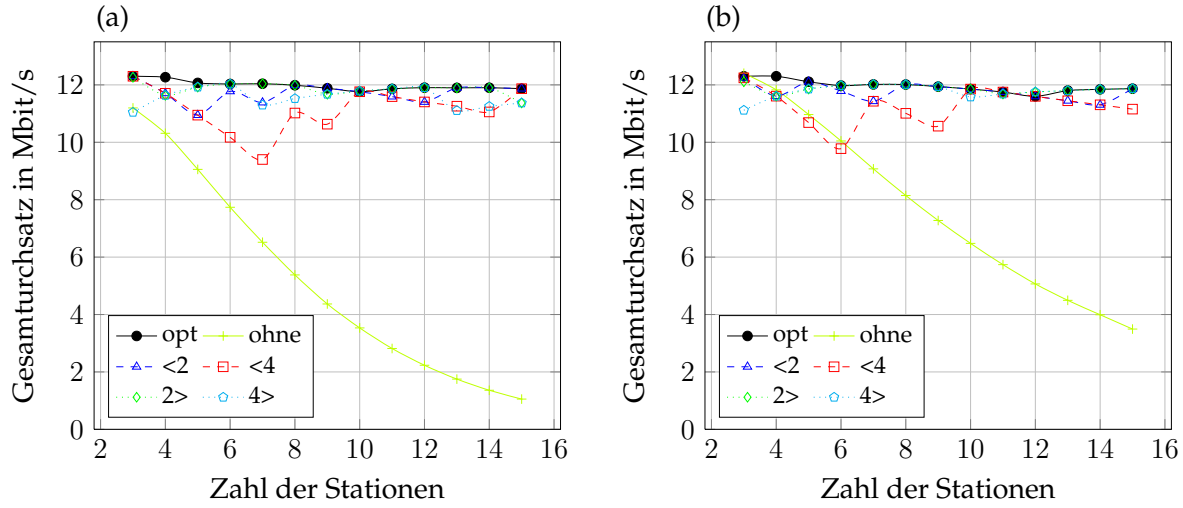


Abbildung 4.11: Optimierungsergebnisse für nicht-optimale Schätzung der Stationenzahl (links ohne, rechts mit PADCC)

Man sieht, dass die im Standard vorgeschlagene Parameterkonfiguration insbesondere bei großen Szenarien keine guten Ergebnisse erzielt. Die Änderung von $CW_{\min}$ in Abhängigkeit der Stationenzahl m lohnt sich also in jedem Fall. Selbst wenn die Anzahl nicht genau bekannt ist, kann der Durchsatz erheblich gesteigert werden. Hierbei ist es tendenziell besser, einen zu großen Wert für m anzunehmen.

Durch die Optimierung der Fenstergröße werden die Vorteile, die PADCC für den Gesamtdurchsatz bringt, verschwindend gering. Wenn die genaue Zahl der Stationen bekannt ist, ist es also gleichgültig, ob PADCC verwendet wird oder nicht. Normalerweise unterliegt die Stationenzahl aber gewissen Schwankungen, und bei ungenauer Schätzung von m hat PADCC wieder deutliche Vorteile. Das liegt daran, dass PADCC besser auf Änderungen reagieren kann, weil die Backofflänge in Abhängigkeit der Netzauslastung angepasst wird. Dadurch sind bei ungenauer Schätzung der Stationenzahl die Verluste gegenüber der optimalen Konfiguration geringer als bei Verwendung von reinem 802.11e.

4.8 Erweiterung des analytischen Modells für Multihop-Szenarien

Die im vorigen Kapitel beschriebene Analyse ist anwendbar, wenn sich alle Stationen in Sendereichweite befinden. In Mesh-Netzen ist dies aber üblicherweise nicht der Fall (siehe Abb. 4.12: Die Sendereichweiten R_{Tx} von Sender S und Empfänger E decken unterschiedliche Bereiche ab). Deshalb soll im Folgenden eine Möglichkeit vorgestellt werden, wie die Ergebnisse auch für Multihop-Szenarien verwendet werden können.

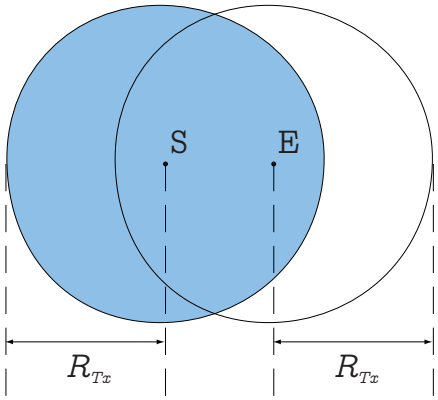


Abbildung 4.12: Sendereichweiten im Multihop-Szenario

4.8.1 Existierende Ansätze

In [26], [5] und [8] werden die Formeln für die Berechnung von Durchsatz und Verzögerung von Singlehop auf Multihop erweitert. Allerdings handelt es sich dabei ausschließlich um Modelle, in denen reines 802.11 (ohne Verkehrskategorisierung) betrachtet wird. Für eine Analyse von 802.11e ist daher ein neues Modell erforderlich, wie im Folgenden näher beschrieben.

4.8.2 Voraussetzungen

Für das Multihop-Szenario wird von nachstehenden Voraussetzungen ausgegangen:

- Es wird auch weiterhin ein System in Sättigung betrachtet, und alle gesendeten Pakete haben die gleiche Länge. Der Kanal wird weiterhin als ideal angenommen, also frei von äußeren Störeinflüssen.
- Die Stationen sind entsprechend einer zweidimensionalen Poissonverteilung zufällig auf der Simulationsfläche verteilt.
- Die Stationen befinden sich nicht mehr alle in Sendereichweite. Zwischen Datenquelle und -senke können also mehrere Stationen liegen, die als Relais fungieren und die Daten weiterleiten.

- Da alle Stationen gleichartig sind, haben auch alle die gleiche Sendereichweite R_{Tx}, die hier näherungsweise als konstant angenommen wird. Daher gilt: Falls eine Station A sich innerhalb der Sendereichweite von B befindet, dann befindet sich B auch innerhalb der Sendereichweite von A.
- Im Gegensatz zum Singlehop-Szenario wird hier der Capture-Effekt mit berücksichtigt: Wenn sich mehrere Sendesignale am Empfänger überlagern, ist es möglich, das Signal mit der größten Empfangsleistung erfolgreich zu dekodieren, falls der Unterschied in der Signalstärke ausreichend hoch ist (siehe Abb. 4.13).

Zunächst sollen einige Begriffe geklärt werden:

Sendereichweite R_{Tx}: Maximale Entfernung, die zwei Stationen haben dürfen, um das Signal der jeweils anderen korrekt dekodieren zu können.

Interferenzreichweite R_I: Maximale Entfernung, die zwei Stationen haben können, damit das Sendesignal der einen Station stark genug ist, um den Empfang der anderen Station zu stören.

Carrier-Sensing- (CS-)Reichweite R_{CS}: Maximale Entfernung, die zwei Stationen haben dürfen, um ein Sendesignal der jeweils anderen Station gerade noch detektieren zu können.

Die Zusammenhänge sind in Abb. 4.13 dargestellt:

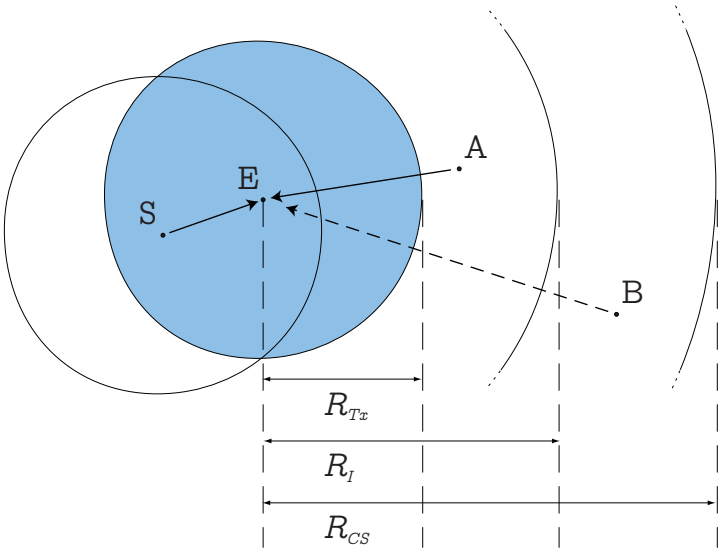


Abbildung 4.13: Veranschaulichung der Radien

E befindet sich innerhalb der Sendereichweite von S, eine Kommunikation zwischen diesen beiden Knoten ist also möglich. A befindet sich innerhalb der Interferenzreichweite von E, aber außerhalb der Sendereichweite. E kann Pakete von A daher

nicht dekodieren, die Signalstärke ist aber so groß, dass A eine Übertragung von S nach E stören kann. B ist von E so weit entfernt, dass das Sendesignal gerade noch detektiert werden kann, aber zu schwach ist, um eine Übertragung zu stören (Capture-Effekt).

In der Literatur wird oft davon ausgegangen, dass die Sendereichweite R_{Tx} der Stationen mit der Interferenzreichweite R_I und der CS-Reichweite R_{CS} übereinstimmt (siehte z.B. [26, 5]). Das bedeutet konkret, dass eine Station jedes Signal, welches sie auf dem Kanal detektiert, auch korrekt dekodieren kann. Diese Annahme stellt eine Vereinfachung für die Berechenbarkeit von Multihop-Szenarien dar. Allgemein gilt $R_{Tx} \leq R_I \leq R_{CS}$ [8, 58, 56].

Damit eine Station den Inhalt eines empfangenen Pakets dekodieren kann, muss die Empfangsleistung über einer bestimmten Schwelle liegen. Diese Schwelle ist von der Sensibilität des verwendeten Equipments abhängig und hängt mit dem Signal-zu-Interferenz-und-Rauschabstand (SINR) auf dem Kanal zusammen. Je kleiner dieser ist, desto größer wird die Bitfehlerwahrscheinlichkeit, bis erfolgreicher Empfang nicht mehr möglich ist.

SINR und Entfernung zwischen Sender und Empfänger hängen eng zusammen, streng genommen besteht jedoch kein linearer Zusammenhang, da auch Abschattung, Streuung und Reflexion des Sendesignals Auswirkungen auf die Signalstärke am Empfänger haben [54]. Um realistische Szenarien abzubilden, reicht es demnach nicht, die Entfernung zwischen Sender und Empfänger zu kennen, um die Signalstärke zu berechnen, sondern es müssen andere Faktoren mit einbezogen werden, wie z.B. ob eine Sichtverbindung besteht, oder ob sich andere Geräte in der Nähe befinden, die zwar nicht zum Netz gehören, aber das gleiche Frequenzband nutzen. Deshalb ist die Fläche, die vom Sendesignal einer Station abgedeckt wird, in der Realität selten kreisförmig. Für die Modellierung eines Netzes ist die Darstellung mit Hilfe von Radien jedoch einsichtiger, man muss sich nur darüber im Klaren sein, dass *Sendereichweite* sich nicht auf die Entfernung zwischen Sender und Empfänger bezieht, sondern auf die Signalstärke. Diese Signalstärke wird dann umgerechnet in die äquivalente Entfernung im Freiraummodell.

4.8.3 Konsequenzen für die Modellierung

Hidden-Node-Problem

Das Hidden-Node-Problem tritt auf, wenn eine Station eine laufende Übertragung stört, weil sie den Sender nicht hören kann. Dies ist in Abb. 4.14 dargestellt. Stationen, die sich innerhalb des grauen Bereichs befinden, können eine laufende Übertragung des Senders S nicht detektieren, weil sie sich außerhalb dessen CS-Reichweite befinden. Da sie sich innerhalb der Sendereichweite von E befinden, können sie jedoch die laufende Übertragung stören, da die beiden Signale sich am Empfänger E überlagern und dadurch korrekten Empfang verhindern.

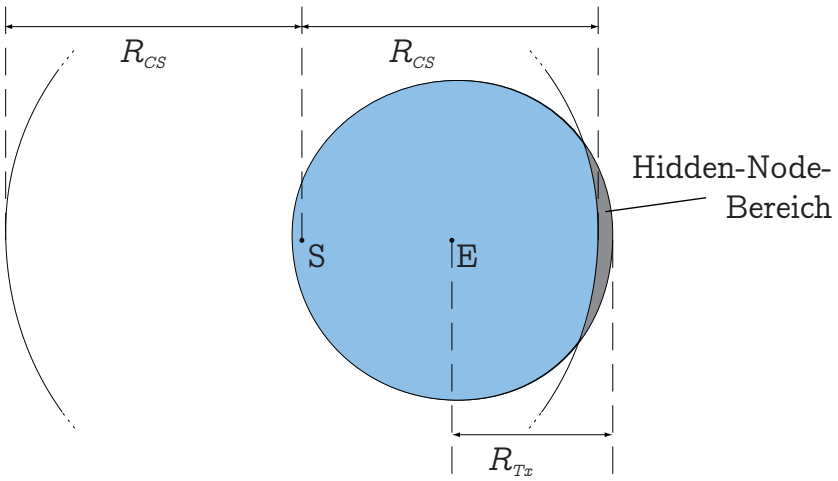


Abbildung 4.14: Das Hidden-Node-Problem

Im Gegensatz zum Singlehop-Fall können Kollisionen also nicht nur dann auftreten, wenn zwei Stationen gleichzeitig mit dem Senden beginnen. Wenn eine Station S im nächsten Zeitschlitz eine Übertragung beginnt (an einen Empfänger E), gibt es eine Kollision, wenn mindestens einer der folgenden Fälle zutrifft:

1. Mindestens eine Station innerhalb der Interferenzreichweite des Empfängers E beginnt ebenfalls im nächsten Zeitschlitz eine Übertragung.

2. Mindestens eine Station innerhalb der Interferenzreichweite des Empfängers E befindet sich gerade in einer laufenden Kommunikation (wenn die andere Station gerade sendet, stört sie den Empfang bei E; wenn sie gerade empfängt, stört sie den Empfang bei E sobald sie mit dem Senden der Quittung beginnt).

3. Mindestens eine Station innerhalb der Interferenzreichweite des Empfängers E beginnt eine Übertragung, während S Daten an E sendet.

4. Mindestens eine Station innerhalb der Interferenzreichweite des Senders S beginnt eine Übertragung, während E die Quittung für die Übertragung sendet.

Der aus dem Singlehop-Szenario bekannte Fall (1), dass zwei Stationen gleichzeitig eine Übertragung beginnen, stellt auch weiterhin eine Quelle für Kollisionen dar. Die anderen Fälle sind spezifisch für Multihop-Szenarien und basieren alle auf dem Hidden-Node-Problem: Eine Station stört eine laufende Übertragung, weil sie nicht in der Lage ist, diese zu detektieren. Im Gegensatz zum Singlehop-Szenario kann eine Übertragung der Station S also nicht nur dann kollidieren, wenn eine Station in Sendereichweite gleichzeitig mit einer Übertragung beginnt, sondern zusätzlich dazu

auch in bestimmten Fällen, wenn eine Station außerhalb der Sendereichweite schon vorher eine Übertragung begonnen hat oder vor dem Ende der Übertragungsdauer mit einer Übertragung beginnt.

Markovmodell für den Kanal

Im Singlehop-Szenario haben alle Stationen die gleiche Sicht auf den Kanal: Wenn eine Station sendet, sehen alle anderen Stationen, dass der Kanal belegt ist. Analog dazu sehen alle Stationen einen freien Kanal, wenn gerade niemand sendet. Im Multihop-Szenario ist das nicht der Fall: Wenn hier eine Station sendet, kann eine weiter entfernte Station den Kanal trotzdem als frei erkennen. Das Übertragungsmedium ist also nicht mehr für alle Stationen gleich, wodurch eine wichtige Voraussetzung für die Singlehop-Modellierung wegfällt (siehe Kap. 4.2).

Im Multihop-Szenario ist es demnach nicht möglich, den Zustand des Kanals für alle Stationen mit Hilfe eines einzigen Markovmodells abzubilden. Das Markovmodell für den Kanal wurde in Kap. 4.2 eingeführt, um die Berechnung mit vertretbarem Rechenaufwand zu ermöglichen. Dieses Verfahren ist hier jedoch nicht mehr anwendbar.

Konsequenzen

Aufgrund der genannten Probleme ist es nicht ohne Weiteres möglich, das in Kap. 4.2 vorgestellte Markovmodell für den Multihop-Fall zu erweitern. Für die Modellierung des Multihop-Szenarios muss daher eine andere Vorgehensweise gefunden werden.

4.8.4 Approximation des Multihop-Szenarios durch das Singlehop-Modell

Die präzise Modellierung des Multihop-Szenarios anhand einer Erweiterung des in dieser Arbeit entwickelten Markovmodells würde in viel zu hoher Komplexität resultieren und ist daher nicht praktikabel (das wäre ein Widerspruch zum Ziel der Analyse, eine schnellere und einfachere Alternative zu Simulationen zu finden). Stattdessen soll im Folgenden eine Möglichkeit vorgestellt werden, das Multihop-Szenario näherungsweise zu modellieren.

Idee: Darstellung des Multihop-Netzes als mehrere Singlehop-„Zellen“. Diese Zellen überlappen sich, weswegen die Interaktion mit benachbarten Zellen auch berücksichtigt werden muss. In Abb. 4.15 ist ein Ausschnitt aus dem Multihop-Szenario dargestellt: Die Station S sendet eigene Daten (gestrichelter Pfeil) und leitet Daten weiter (durchgezogene Pfeile). Die schwarz markierten Knoten befinden sich in Interferenzreichweite von S, die hellblauen Knoten befinden sich in Interferenzreichweite des Empfängers E, aber außerhalb der Interferenzreichweite von S. Dies wird durch die beiden Kreise verdeutlicht. Die weißen Knoten sind von S und E so weit entfernt, dass sie eine laufende Übertragung nicht stören können.

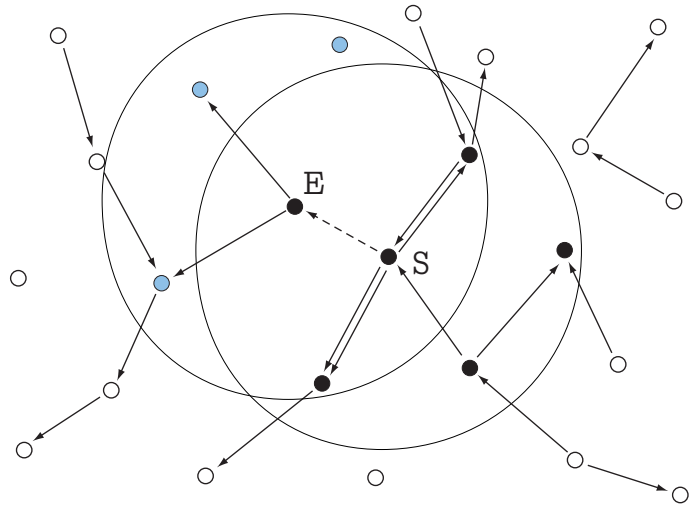


Abbildung 4.15: Ausschnitt aus dem Multihop-Szenario

Um das Multihop-Szenario mit Hilfe des Singlehop-Modells darzustellen, dienen die folgenden Überlegungen:

- Statt der Gesamtzahl der Stationen, wie im Singlehop-Szenario, wird hier nur die Zahl der Stationen, die von einer Übertragung gestört werden bzw. eine Übertragung stören können, betrachtet. Das sind alle Stationen innerhalb der Interferenzreichweite des Senders oder Empfängers (in Abb. 4.15 alle schwarz und hellblau markierten Knoten). Diese Anzahl wird im Folgenden m_I genannt.

- Dadurch, dass sich nicht alle Stationen gegenseitig hören, sind mehrere parallele Übertragungen möglich. Das führt insgesamt zu geringerer Paketverzögerung, da weniger lang gewartet werden muss, bis der Kanal frei wird. Außerdem sinkt dadurch die Kollisionsrate, da gleichzeitiges Senden nicht zwingend zu einer Kollision führt, wenn die beiden Sender bzw. Empfänger ausreichenden Abstand zueinander haben.

- Andererseits steigen die Kollisionswahrscheinlichkeit und die Verzögerung dadurch, dass eine Kollision nicht mehr nur durch den gleichzeitigen Beginn einer Übertragung ausgelöst wird, sondern in bestimmten Fällen auch durch eine bereits laufende Übertragung oder eine Übertragung, die erst später beginnt.

4.8.5 Ergebnisse

Für den Vergleich wurde der in Kapitel 4.6.1 beschriebene Simulator erweitert, sodass auch Multihop-Netze dargestellt werden können. Einzelheiten dazu sind im Anhang C beschrieben. Das Simulationsszenario ist quadratisch, und eine Seitenlänge

entspricht dem Sechsfachen der Interferenzreichweite R_I. Um Randeffekte zu vermeiden, werden nur die Simulationsergebnisse derjenigen Stationen ausgewertet, die sich in der Mitte des Simulationsfeldes befinden, innerhalb der Interferenzreichweite einer Referenzstation S (schwarz markierte Knoten in Abb. 4.15). Unterschiedliche Werte für m_I werden dargestellt, indem die Gesamtzahl der Stationen zwischen 40 und 150 variiert wird. Eine höhere Gesamtzahl führt bei gleichem Simulationsfeld zu einer höheren Knotendichte, und entsprechend befinden sich dann mehr Stationen in Interferenzreichweite von S. Die Stationen sind zufällig auf dem Simulationsfeld verteilt und bewegen sich nicht. Wie im Singlehop-Szenario haben alle Stationen immer Pakete zu senden.

Im Folgenden wird nicht der Datendurchsatz (auf der Anwendungsschicht) betrachtet, sondern der MAC-Schicht-Durchsatz pro Knoten. Dieser ist in Abb. 4.16 dem MAC-Schicht-Durchsatz pro Knoten der Singlehop-Analyse gegenübergestellt. Was im Singlehop-Modell die Gesamtzahl der Knoten ist, ist jetzt m_I, die Anzahl der Knoten in Interferenzreichweite von Sender und Empfänger. Im Multihop-Szenario ist daher die kleinstmögliche Stationenzahl, die dargestellt werden kann, größer als im Singlehop-Fall: Wenn drei Stationen in Interferenzreichweite sind, bedeutet das, dass sich durchschnittlich weniger als drei Stationen zueinander in Sendereichweite befinden. Derartige Szenarien können nicht sinnvoll simuliert werden.

Außerdem sind in Abb. 4.16 Simulationsergebnisse unter Verwendung des ns-2 sowie einzelne Analyseergebnisse aus der Literatur [5, 8, 26] zum Vergleich eingezeichnet.

Man sieht, dass Analyse und Simulation sehr ähnliche Werte liefern. Beim ns-2 ist der Durchsatz, wie auch im Singlehop-Szenario, etwas niedriger (Abb. 4.16 a). Da in der Literatur oft von sehr unterschiedlichen Voraussetzungen ausgegangen wird, ist es schwierig, Ergebnisse aus verschiedenen Arbeiten in Relation zu setzen. Die in der Grafik eingezeichneten Werte sind einzelne Ergebnisse, die entsprechend den hier verwendeten MAC-Parametern umgerechnet wurden.

Wenn man also in die Formeln in Kap. 4.2 bzw. 4.3 m_I statt m einsetzt, erhält man gute Näherungswerte für den Durchsatz in Multihop-Szenarien. Die Paketverlustrate lässt sich auf diese Weise ebenfalls näherungsweise bestimmen (siehe Abb. 4.16 b).

Für die Verzögerung hingegen ist das Singlehop-Modell nicht anwendbar. Im Multihop-Szenario befinden sich wesentlich mehr Stationen, die Verzögerungswerte aus dem Singlehop-Modell sind für hohe Stationenzahlen jedoch aufgrund der hohen Paketverlustrate nicht aussagekräftig (siehe Kap. 3.2.3, Abb. 3.4). Deshalb können die Ergebnisse nicht auf das Multihop-Szenario übertragen werden.

Abb. 4.17 zeigt den Durchsatz der einzelnen Verkehrsklassen, wiederum im Vergleich zwischen Singlehop-Modell (mit entsprechend geänderter Stationenzahl), Multihop-Simulation und ns-2. Die y-Achse ist dabei logarithmisch dargestellt. Auch hier stimmen die Ergebnisse von Analyse und beiden Simulatoren gut überein.

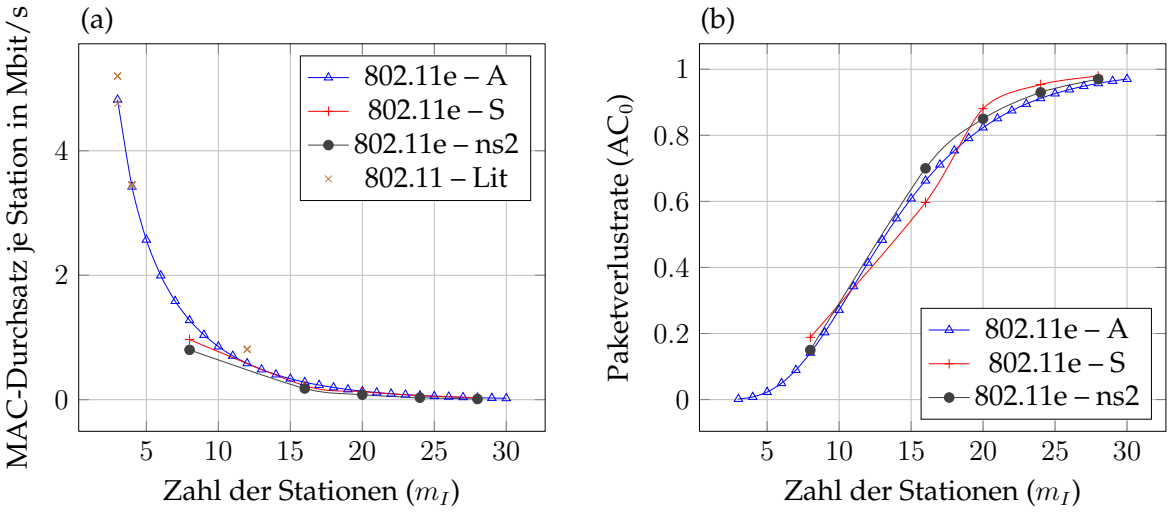


Abbildung 4.16: Vergleich zwischen Analyse und Simulation, Multihop-Szenario

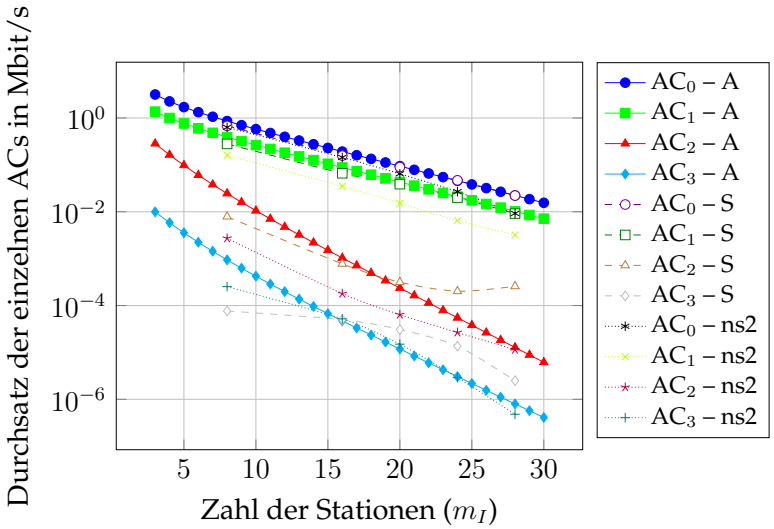


Abbildung 4.17: Vergleich zwischen Analyse und Simulation, Multihop-Szenario: Durchsatz der verschiedenen Verkehrsklassen

4.8.6 Optimierung

Äquivalent zum Singlehop-Fall kann auch für das Multihop-Szenario die optimale Fenstergröße in Abhängigkeit der Stationenzahl bestimmt werden. Die Ergebnisse hierzu sind in Abb. 4.18 dargestellt. Der angegebene Durchsatz (Abb. 4.18 a und b) ist wieder der MAC-Schicht-Durchsatz pro Station, hier allerdings aufgetragen über dem durchschnittlichen Knotengrad (Anzahl der Nachbarn eines jeweiligen Knotens). Der Knotengrad kann im laufenden Betrieb des Netzes mit geringerem Aufwand bestimmt werden als m_I (siehe Kap. 5), wodurch die Ergebnisse besser weiterverwendet werden können.

Für die Graphen in Abb. 4.18 gilt: Im Szenario mit vier Nachbarn führen zwar kleine Fenstergrößen (15 oder 31) zu den höchsten Werten für den Durchsatz, aufgrund der hohen Paketverlustrate sind diese aber nicht zweckmäßig.

Des Weiteren lässt sich beobachten, dass die Paketverlustrate (Abb. 4.18 c und d) für beide Mechanismen (IEEE 802.11e und PADCC) fast gleich ist, obwohl unterschiedlicher Durchsatz erzielt wird. Das liegt daran, dass der PADCC-Mechanismus darauf beruht, einen Teil der Pakete absichtlich zu verwerfen, um insgesamt die Kollisionswahrscheinlichkeit zu verringern.

4.9 Beiträge dieser Arbeit

Das im Zuge dieser Arbeit entwickelte Markovmodell zur Beschreibung des Medienzugriffs verbindet die Vorzüge verschiedener älterer Modelle. Details dazu sind in Kap. 4.5 aufgeführt. Neben der verbesserten Modellierung von IEEE 802.11e ist das hier vorgestellte Modell in der Lage, eDCC bzw. PADCC (siehe Kap. 3.1.3) darzustellen. Dabei können Durchsatz, Verzögerung und Paketverlustrate bestimmt werden. Zur Validierung wurden die Ergebnisse der Analyse mit Simulationsergebnissen verglichen.

Außerdem wurde gezeigt, dass mit Hilfe des Modells auch Multihop-Szenarien in guter Näherung abgebildet werden können.

Die analytische Auswertung des Modells wurde genutzt, um die Eingangsparameter des Medienzugriffsverfahrens für die Maximierung des Durchsatzes zu optimieren. So konnte abhängig vom Szenario gezeigt werden, welche Einstellungen, z.B. in Bezug auf die Fenstergröße, die besten Ergebnisse für den Durchsatz erzielen.

Wie dieses Wissen genutzt werden kann, um im laufenden Betrieb eines Netzes die Leistung zu verbessern, wird im folgenden Kapitel näher erläutert.

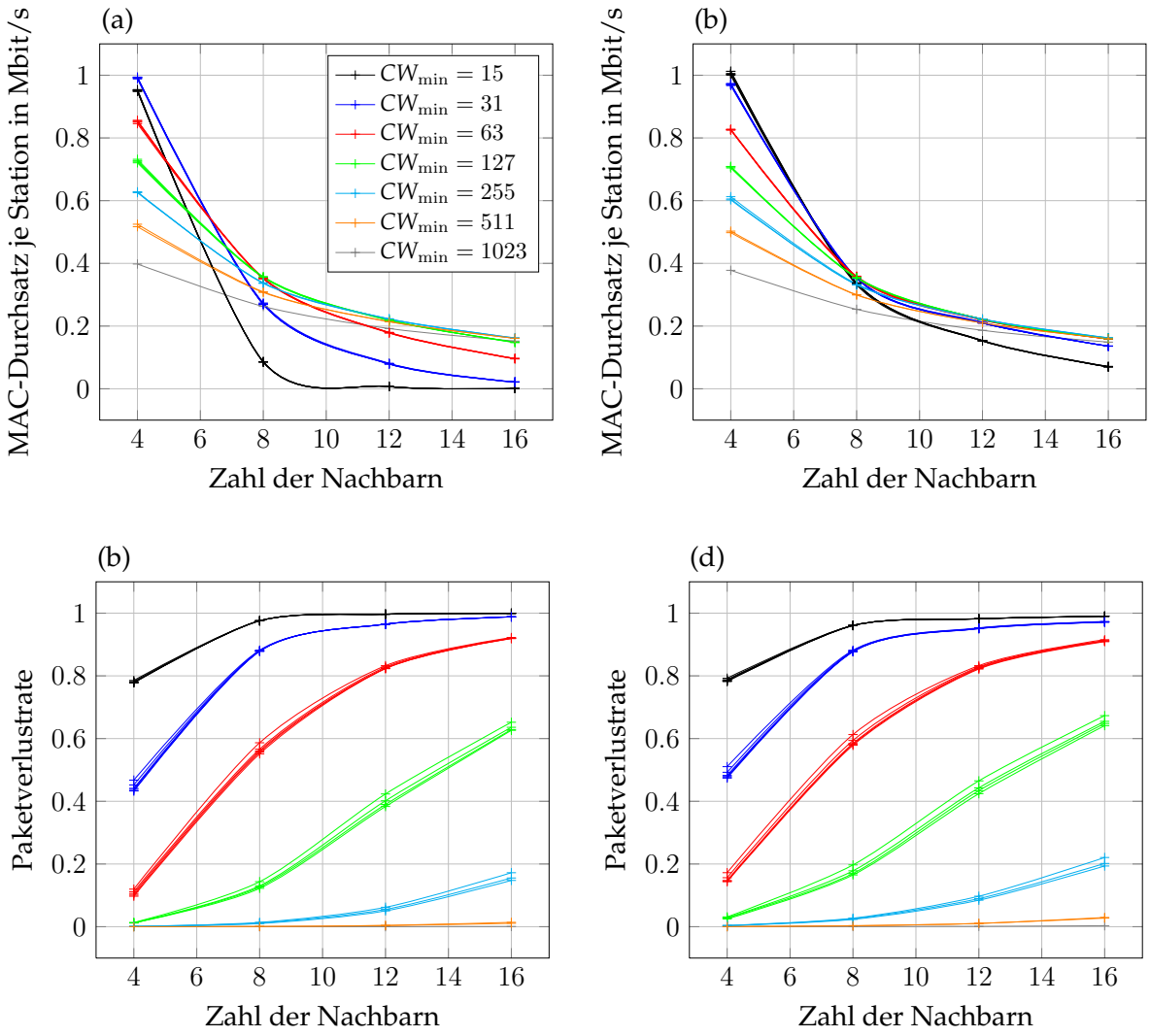


Abbildung 4.18: Optimierungsergebnisse für Multihop (links 802.11e, rechts mit PADCC)

5 Management von Wireless Mesh Networks

Wie in Kap. 2.3 bereits angedeutet, ist es auch bei selbstorganisierenden Netzen für den Betreiber interessant, Informationen über das Netz zu erhalten und in die Funktion eingreifen zu können. Die Informationen können genutzt werden, um die Performance des Netzes zu verbessern oder die Dimensionierung zu verändern, oder auch um allgemeine Statistiken aufzustellen. In Kap. 3 und 4 wurde bereits gezeigt, dass die einzelnen Dienstgütemechanismen bei der Einstellung der Parameter etwas Spielraum haben, sodass sie an die äußeren Umstände angepasst werden können. Wenn die „äußeren Umstände“, also der Zustand des Netzes, bekannt sind, kann dies ausgenutzt werden, um die Leistungsfähigkeit des Netzes zu verbessern.

Dazu sind drei wesentliche Faktoren erforderlich:

1. Der Zustand des Netzes muss erfasst werden.

2. Es muss ein Regelsatz vorhanden sein, der den aktuellen Zustand des Netzes mit adäquaten Reaktionen verknüpft.

3. Es wird ein Protokoll benötigt, welches die erforderlichen Daten ausliest und die Möglichkeit bietet, den Knoten Steuerungsinformationen für die Anpassung der Parameter zukommen zu lassen.

Abb. 5.1 zeigt den Zusammenhang zwischen Netz und Management: Die Managementeinheit liest den Zustand des Netzes ab und ändert daraufhin falls nötig die Parameter der Dienstgütemechanismen. Durch die geänderten Einstellungen wird wiederum der Netzzustand beeinflusst. Da es sich um einen Kreislauf handelt, besteht die Gefahr der Instabilität. Um dem entgegenzuwirken, sollten einerseits die Messintervalle ausreichend groß gewählt werden, andererseits empfiehlt sich der Einsatz einer Hysterese, um ständiges Hin- und Herschalten zwischen zwei Zuständen zu vermeiden.

Im Folgenden wird die in Kap. 3 beschriebene Architektur DARMA um eine Managementkomponente erweitert, welche die drei oben genannten Punkte adressiert. Die Architektur ist in Abb. 5.2 dargestellt. Die Managementkomponente übernimmt die Überwachung des Netzzustandes und erhält die entsprechenden Anweisungen dazu über eine Benutzerschnittstelle. Der Zugriff auf die drei Dienstgütemechanismen ermöglicht die Anpassung der jeweiligen Parameter.

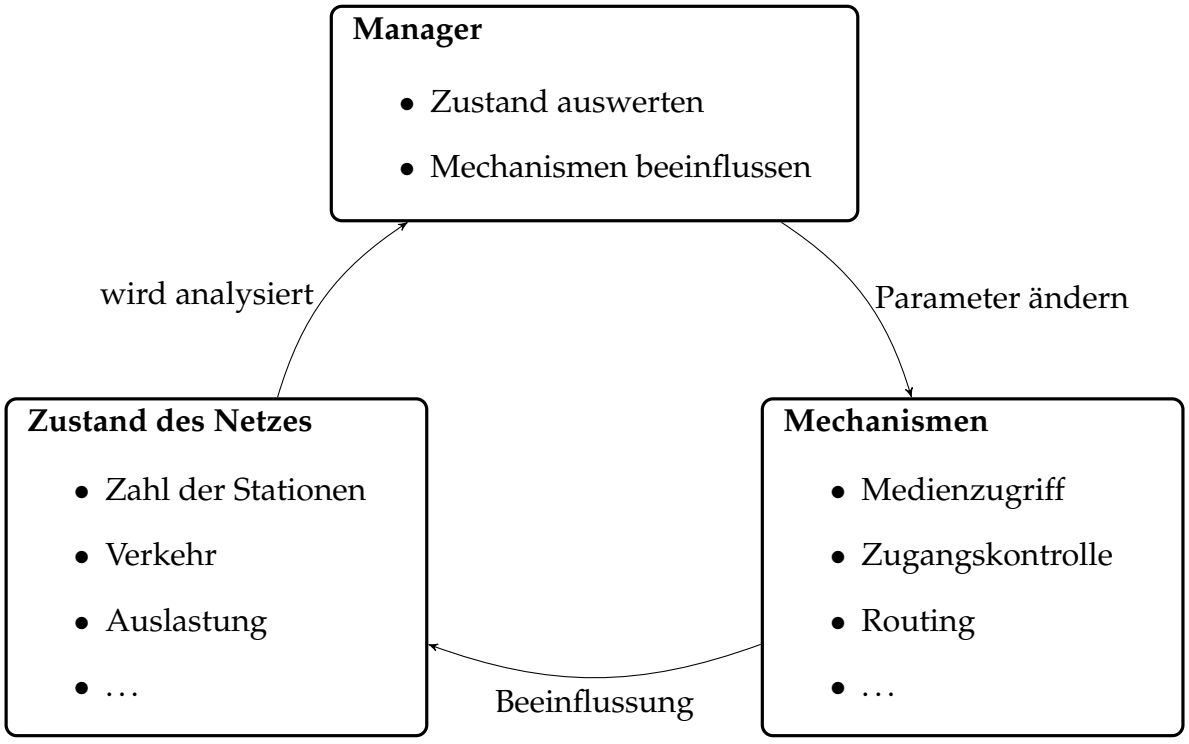


Abbildung 5.1: Zusammenhang zwischen Netz und Managementsystem

5.1 Struktur der Managementarchitektur

Wie in Kap. 2.1 bereits beschrieben, haben die betrachteten Netze in erster Linie die Aufgabe, teilnehmenden Stationen Zugang zum Internet zu bieten. Dabei steht keine zentrale Steuerungseinheit zur Verfügung. Eine nicht-hierarchische Struktur ist für das Managementsystem jedoch unvorteilhaft, da sie schlecht skaliert und somit in größeren Netzen viel Overhead bei der Kommunikation bedeutet. Deshalb ist eine Einteilung in Cluster vorteilhaft. Diese Einteilung wird hier nur für Managementaufgaben verwendet.

5.1.1 Einteilung in Cluster

Die grundlegenden Eigenschaften von Clusteringalgorithmen wurden in Kap. 2.3.1 bereits erläutert. Im Folgenden wird ein Mechanismus entworfen, der auf dem in [11] beschriebenden Distributed Clustering Algorithm (DCA) basiert und diesen den spezifischen Voraussetzungen von WMNs entsprechend erweitert.

Da ein Clusterhead zusätzliche Aufgaben zu erfüllen hat, bietet es sich in einem Mesh-Netz an, die Gateways als Clusterheads auszuwählen. Die Gateways haben eine permanente Stromversorgung und sind üblicherweise im Besitz des Netzbetreibers, weswegen es einfacher ist, die Software auf dem neuesten Stand zu halten. Aufgaben

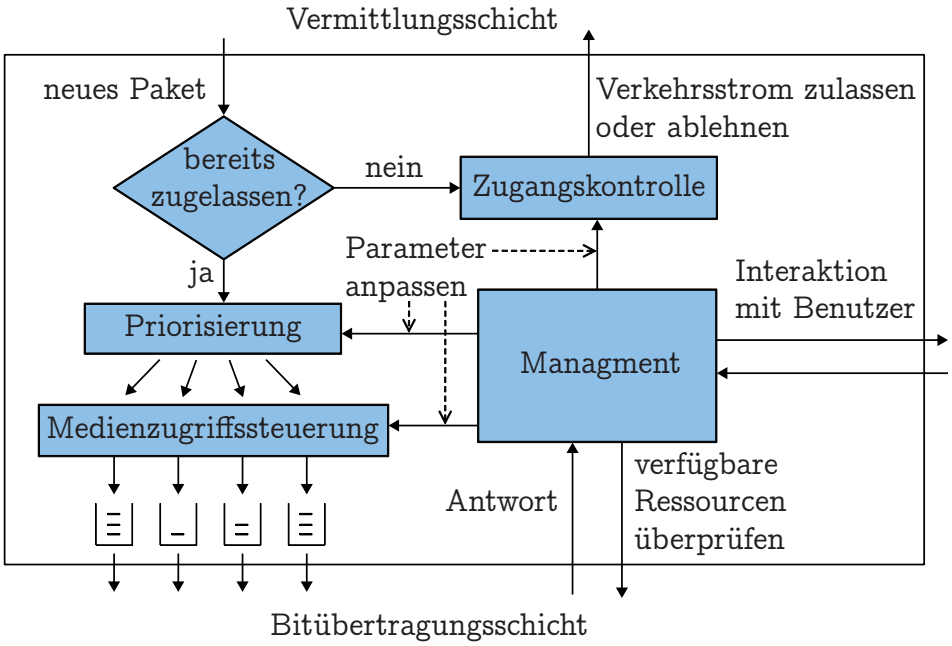


Abbildung 5.2: DARMA inklusive Managementkomponente

der Clusterheads sind:

- Speichern ausgewählter Daten aller Teilnehmer des Clusters
- Weiterleiten dieser Daten an die Managementdatenbank
- Verwaltung der Teilnehmer / Clusterbildung

Wie in Kap. 2.3.1 bereits diskutiert, sollen sich alle Teilnehmer in Sendereichweite ihres CHs befinden, um den Datenverkehr, der durch Managementnachrichten erzeugt wird, möglichst gering zu halten. Da auf diese Weise nicht zwingend die ganze Fläche des Netzes durch die Gateways abgedeckt wird, müssen zusätzliche Clusterheads definiert werden. Dazu dient der folgende Algorithmus (siehe Abb. 5.3):

Jedes Gateway ernennt sich selbst zum Clusterhead. Jeder andere Knoten überprüft, ob unter seinen Nachbarn ein Clusterhead ist. Wenn ja, schließt er sich diesem an (im Zweifelsfall dem mit der niedrigsten Kennung[1]). Sonst ernennt er sich selbst zum Clusterhead. Jeder Clusterhead pflegt eine Liste aller Clusterteilnehmer und speichert Informationen über jeden einzelnen, die in regelmäßigen Abständen aktualisiert werden (siehe auch Kap. 5.4).

[1]Der in [11] beschriebene Algorithmus stellt sicher, dass jede Station nur einen Clusterhead unter ihren Nachbarn hat. Das ist hier aufgrund der Ernennung aller Gateways zum CH nicht gegeben.

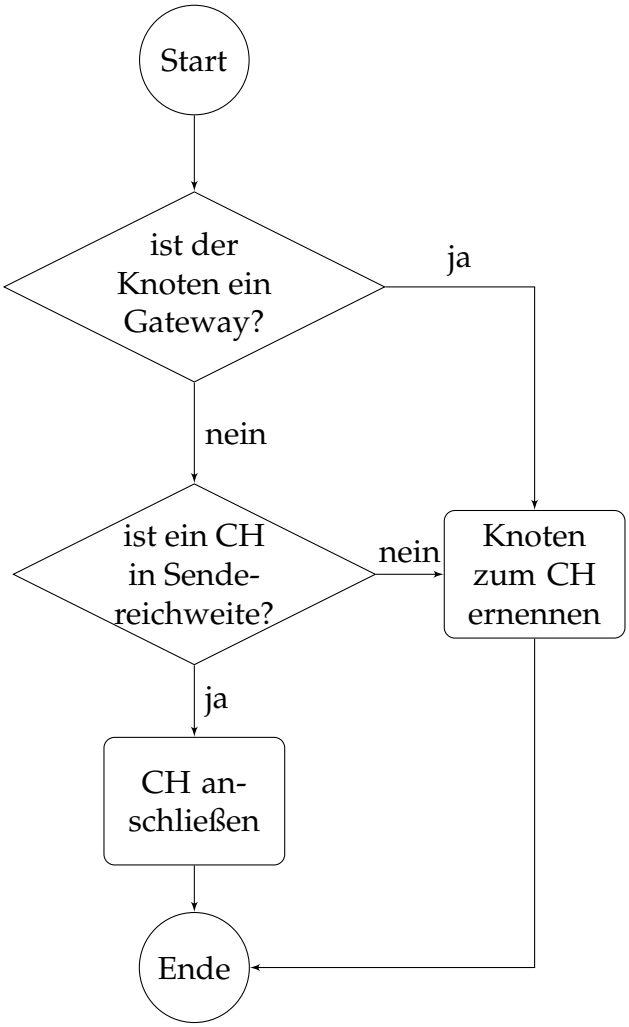


Abbildung 5.3: Clusteringalgorithmus

Anstatt der Adresse kann auch eine Metrik verwendet werden, die die Eignung eines Knotens als Clusterhead widerspiegelt. Diese wird durch einen 8-bit-Wert dargestellt, der sich aus Faktoren wie Stromversorgung, Nähe zum nächsten Gateway, Wahrscheinlichkeit mit welcher der Knoten das Netz in näherer Zukunft verlässt und gegebenfalls Anzahl der Clusterteilnehmer berechnet. Ein niedriger Wert bedeutet dabei bessere Eignung. Gateways haben prinzipiell den Wert „0“, außer wenn sich schon mehr als zehn Teilnehmer in ihrem Cluster befinden, dann steigt der Wert auf „1“. Knoten, die kein Gateway sind, haben mindestens den Wert „2“, sind also immer schlechter geeignet als Gateways. Der Wert erhöht sich jeweils um 1 falls der Knoten eine Betriebszeit von weniger als 24 Stunden hat oder falls das nächste Gateway mehr als zwei Hops entfernt ist. Er erhöht sich um 2, falls der Knoten über keine permanente Stromversorgung verfügt.

Alle Knoten berechnen ihre Eignung und schicken diesen Wert in ihrer Clusteranfrage sowie auch in der Antwort mit. So kann jede Station, die noch keinem Cluster zugeordnet ist, die Antworten verschiedener CHs auswerten, und sich den besten aussuchen. Falls sich kein CH in der Nähe befinden sollte, kann jede Station die Anfragen der benachbarten Stationen auswerten. Ein Knoten ernennt sich genau dann selbst zum Clusterhead, wenn keine Station mit einer besseren Eignung in Sendereichweite ist, oder wenn sich alle Stationen, die besser geeignet wären, einem anderen Cluster angeschlossen haben.

Falls ein Teilnehmer das Cluster verlässt, merkt der CH das bei der nächsten Aktualisierung der Daten anhand der fehlenden Statusmeldung und löscht den Eintrag aus der Liste.

5.1.2 Speicherung der Daten

Für die Speicherung der gewonnenen Daten ist eine Datenbank vorgesehen. Diese muss sich nicht zwingend innerhalb des Netzes befinden, aber sie muss von allen Knoten aus erreichbar sein. Im Folgenden wird davon ausgegangen, dass die Datenbank sich außerhalb des WMNs befindet und über das Internet darauf zugegriffen werden kann. In der Datenbank können gleichzeitig auch die Reaktionen auf bestimmte Ereignisse abgespeichert sein, falls diese automatisch ausgeführt werden sollen. Für das Managementsystem macht es keinen Unterschied, ob eine Änderung automatisiert oder von Hand durch einen Administrator ausgelöst wird.

Die Clusterheads speichern lokal Informationen über ihre Clusterteilnehmer und leiten diese an die Datenbank weiter. Der genaue Ablauf und die Nachrichten sind in Kap. 5.4 definiert.

Prinzipiell sind zwei verschiedene Möglichkeiten denkbar: Die Clusterheads können einerseits die Daten vorverarbeiten und bündeln, sodass weniger Verkehr entsteht. Dadurch haben sie aber zusätzliche Arbeit und Verantwortung. In dieser Architektur wird die andere Variante gewählt: Da die Knoten im Netz mit möglichst wenig

zusätzlichen Aufgaben belastet werden sollen, wird ihnen hier keine Entscheidungsgewalt zugesprochen. Die Daten werden nur geringfügig vorverarbeitet und dann in regelmäßigen Abständen direkt an die Datenbank weitergeleitet. So muss lokal immer nur der aktuelle Datensatz von jedem Teilnehmer gespeichert werden, sowie drei zusätzliche Werte, die direkt daraus abgelesen werden können (Anzahl der Teilnehmer, Knotengrad und Auslastung; siehe Kap. 5.4). Der Manager verfügt über die Daten aller Netzteilnehmer und kann auf dieser Basis globale Entscheidungen treffen, was für die meisten der betrachteten Parameter sinnvoll ist (siehe Kap. 5.2 bzw. 5.5). Ohne Bündelung der Daten ist zwar der Verkehr zur Datenbank etwas höher, dafür ist so keine Kommunikation der CHs untereinander notwendig und die Komplexität wird insgesamt geringer.

Die beiden Hierarchieebenen des Netzes sind in Abb. 5.4 dargestellt:

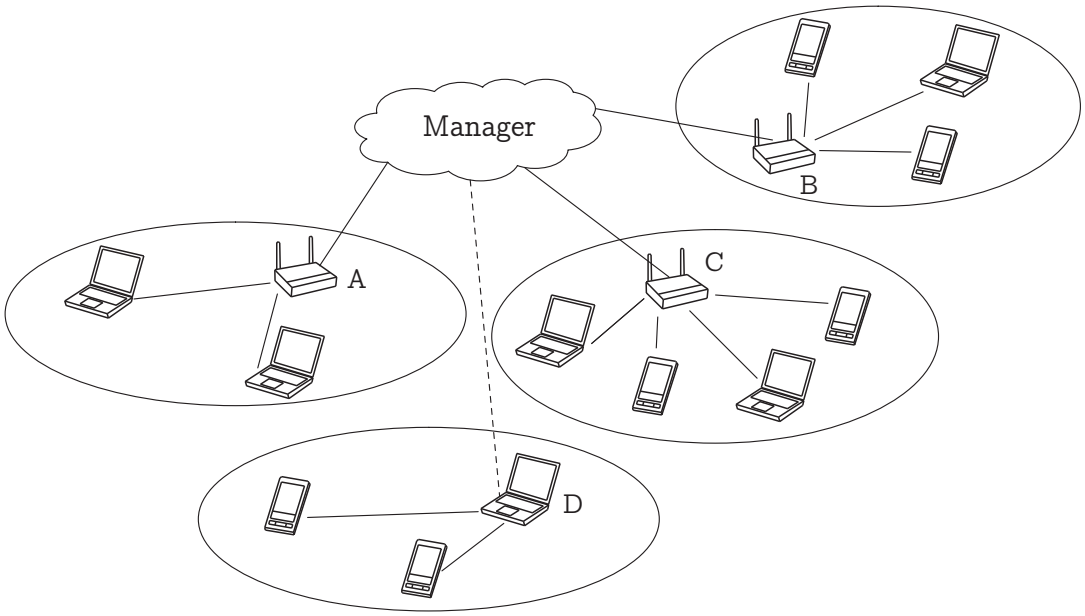


Abbildung 5.4: Einteilung des Netzes in Cluster

Die CHs sind durch Buchstaben gekennzeichnet. Hierbei ist zu beachten, dass die Linien zwischen den einzelnen Knoten keine Kommunikationsverbindungen darstellen, sondern logische Abhängigkeiten. Insbesondere besteht keine direkte (Kabel- oder Funk-)Verbindung zwischen dem Manager und Knoten D. Da kein Gateway in Funkreichweite ist, bildet D ein eigenes Cluster und ist damit als Clusterhead direkt dem Manager unterstellt.

5.2 Identifizierung der relevanten Parameter

Zunächst müssen die Parameter identifiziert werden, die den Zustand des Netzes beschreiben. Hier sind in erster Linie diejenigen Parameter interessant, die eine Auswirkung auf die Dienstgütemechanismen haben. Diese sind in Tab. 5.1 zusammengefasst. Weitere, rein statistische Informationen für den Betreiber können zusätzlich erfasst werden.

Zusätzlich zu den in Kap. 3 und 4 behandelten Mechanismen sind hier der Vollständigkeit halber noch weitere aufgeführt.

Tabelle 5.1: Managementparameter

Mechanismus	Eingangsparameter	Auswirkung auf	abhängig von
Zugangs-kontrolle	– Schwellenwert – ECN-Kriterium – Priorisierung	– Blockierung	– Auslastung – Kapazität – Szenario
Priorisierung	– Zahl der Verkehrsklassen – Fenstergröße – AIFS	– Fairness – Durchsatz	– Auslastung – Stationenzahl – Szenario
Medienzugriff	– PADCC an / aus – Sendewahrscheinlichkeit	– Kanalbelegung – Durchsatz	– Auslastung – Knotendichte – Stationenzahl
Beamforming	– je Paket / Verkehrsstrom	– Overhead	– Stationenzahl – Szenario
Routing	– Metrik – proaktiv / reaktiv	– Stabilität – Linkbruchrate	– Auslastung – Kapazität – Knotendichte – Stationenzahl – Szenario
Security	– Sicherheitsstufe(n)	– Verzögerung	– Szenario

Die Parameter in der rechten Spalte von Tab. 5.1 beschreiben den (aktuellen) Zustand des Netzes. Wenn diese Parameter bekannt sind, können die Eingangsvariablen der Dienstgütemechanismen so eingestellt werden, dass sie die für diesen Betriebsfall bestmöglichen Ergebnisse liefern. In Kap. 5.5 ist der Zusammenhang zwischen Netzzustand, Eingangsparametern und Ergebnis in Bezug auf Durchsatz, Verzögerung und Paketverlustrate genauer erklärt.

Für den Betreiber eines Netzes ist unter anderem interessant, wie viele Stationen sich (durchschnittlich oder maximal) im Netz befinden, wie oft Stationen das Netz verlassen oder neu hinzukommen, wie stark die Kapazität des Netzes ausgelastet ist, welche Art von Verkehr die Nutzer erzeugen (Realzeitdaten, Hintergrundverkehr,

Kommunikation untereinander oder mit dem Internet, etc.), ob bzw. wie oft Fehler auftreten und wodurch diese verursacht werden.

Die für die Optimierung der Mechanismen benötigten Parameter werden im Folgenden näher erläutert.

5.3 Beschreibung des Netzzustandes

Die relevanten Parameter, die den Zustand des Netzes beschreiben, sind also

- Szenario
- Topologie
  - Anzahl der Stationen im Netz
  - Knotengrad
  - Knotendichte / Konnektivität
- Verkehr
  - Kapazität
  - Auslastung

Im Folgenden wird näher darauf eingegangen, wie die einzelnen Parameter erfasst werden können.

5.3.1 Szenario

Unter den Begriff *Szenario* fällt alles, was vor der Inbetriebnahme des Netzes bereits bekannt ist. Dazu ist interessant, wo das Netz eingesetzt wird (siehe auch Kap. 2.1.1), um zu wissen, welche speziellen Anforderungen es in Bezug auf die Dienstgüte gibt. Die ungefähre Größe (sowohl Fläche als auch Zahl der Teilnehmer) muss bereits in der Planungsphase des Netzes abgeschätzt werden, um das Netz dimensionieren zu können. Vom Einsatzgebiet ist auch die Mobilität der Teilnehmer abhängig. Diese Parameter dienen der grundsätzlichen Auswahl der Dienstgütemechanismen. Während des Betriebs können die Mechanismen noch genauer an die aktuelle Situation angepasst werden.

5.3.2 Topologie des Netzes

In Abhängigkeit des Szenarios kann eine grobe Abschätzung der Größe des Netzes bereits im Vorhinein angegeben werden. Um die genauen Werte (in ausreichender Näherung) zu ermitteln, gibt es während des Betriebs verschiedene Möglichkeiten.

Der Clusteringalgorithmus ermöglicht die Ermittlung der Gesamtzahl der Stationen im Netz. Jeder Clusterhead weiß die Anzahl der Knoten, die ihm zugeordnet sind. Der Manager kann daraus die Zahl aller Knoten bestimmen.

Bei Verwendung eines proaktiven Routingprotokolls, was in weitgehend statischen Netzen meistens von Vorteil ist, pflegt jeder Knoten eine Routingtabelle. In dieser Tabelle sind die Pfade zu allen potenziellen Kommunikationspartnern verzeichnet, also zu allen Stationen, die sich im Netz befinden. Die Anzahl kann also einfach dort abgelesen werden. Da die Tabelle vom Routingmechanismus aktuell gehalten wird, entsteht in diesem Fall kein zusätzlicher Overhead.

Ein reaktives Routingprotokoll speichert in der Routingtabelle nur diejenigen Stationen, mit denen in näherer Vergangenheit eine Kommunikation stattgefunden hat. Aus deren Anzahl kann nicht ohne weiteres auf die Gesamtzahl der Knoten geschlossen werden. Es ist jedoch problemlos möglich, dass jeder Knoten eine Tabelle seiner Nachbarn anlegt. Daraus kann jede Station ihren Knotengrad bestimmen. Die Liste wird aktualisiert, wenn neue Nachrichten empfangen werden. Wenn ein Nachbar längere Zeit keine Nachricht sendet, ist dies ein Indiz dafür, dass er nicht mehr da ist (beispielsweise weil er sich aus dem Funkradius hinausbewegt hat, oder weil das Gerät ausgeschaltet wurde), und der Eintrag wird aus der Liste gelöscht.

Die Knotendichte in einem Netz lässt Rückschlüsse auf die Konnektivität des Netzes zu, da die Entfernung zwischen zwei Knoten näherungsweise reziprok proportional ist zur Wahrscheinlichkeit, dass zwischen den beiden Knoten eine Funkverbindung besteht (siehe auch Kap. 4.8.2). Stationenzahl und abgedeckte Fläche hängen über die Knotendichte wie folgt zusammen:

$$Dichte = \frac{Zahl\ der\ Stationen}{abgedeckte\ Fläche}$$

Es reicht also, zwei dieser Werte zu kennen, um den dritten berechnen zu können.

Die Fläche eines Netzes kann einfach berechnet werden, wenn jede Station ihre eigene Position bestimmen kann, beispielsweise mit Hilfe von GPS [40]. Dies ist in WMNs aber üblicherweise nicht der Fall. Auf Basis des Szenarios kann eine grobe Abschätzung für die Größe angegeben werden, aber aufgrund der Eigenschaften von WMNs kann diese stark variieren, da am Rand des Netzes immer weitere Stationen dazukommen können, die damit die Fläche erweitern. In bestimmten Fällen kann die Maximalgröße angegeben werden, beispielsweise wenn sich das Netz auf einer Insel befindet oder ringsherum unwegsames Gelände ist, sodass nicht davon auszugehen ist, dass sich dort weitere Stationen befinden.

Der Knotengrad der einzelnen Stationen hängt auch mit der Dichte zusammen. Für den mittleren Knotengrad kann ein statistischer Wert angegeben werden, wenn die Knotendichte und die Verteilung der Knoten bekannt sind [40]. Umgekehrt kann aus dem Knotengrad (bei bekannter Verteilung) auf die Dichte geschlossen werden. Dabei sind jedoch immer nur durchschnittliche Angaben möglich.

Anhand der Knotengrade der einzelnen Stationen kann auch ohne Kenntnis der Verteilung die Knotendichte in einzelnen Bereichen des Netzes abgeschätzt werden. Je mehr Nachbarn die einzelnen Stationen haben, desto höher ist im Mittel die Knotendichte in diesem Bereich.

5.3.3 Kapazität und Auslastung

Die Gesamtkapazität ist in drahtlosen Netzen nicht ohne weiteres zu bestimmen. Der Funkstandard gibt zwar eine Abschätzung für die erreichbare Datenrate vor, diese wird jedoch durch äußere Störeinflüsse verringert und muss außerdem zwischen allen sendenden Stationen aufgeteilt werden.

Für die Auslastung des Netzes gilt:

$$Auslastung = \frac{genutzte\ Ressourcen}{insgesamt\ verfügbare\ Ressourcen}$$

Die genutzten Ressourcen können zwar mit Hilfe der Sendedatenrate abgeschätzt werden, aber wenn die Gesamtkapazität nicht bekannt ist, kann daraus nicht auf die Auslastung geschlossen werden.

In Kap. 3.1.3 wurde bereits eine Methode vorgestellt, um die Auslastung näherungsweise zu bestimmen. Da dies Teil des Zugangskontrollmechanismus ist, liegen die Informationen bereits vor und können vom Managementsystem verwendet werden, ohne dass zusätzlicher Overhead entsteht.

5.3.4 Zusammenfassung

In manchen Szenarien kann der Großteil der Informationen ohne zusätzlichen Aufwand gewonnen werden, weil die Werte schon vorhanden sind und nur abgelesen werden müssen.

Auch im allgemeinen Fall können die meisten Werte relativ einfach bestimmt werden. Der Knotengrad lässt sich passiv ermitteln, wobei jeder Knoten nur eine Tabelle der direkten Nachbarn speichern muss. Aufgrund der Einteilung in Cluster liegen die Stationenzahlen der verschiedenen Cluster vor, woraus die Gesamtzahl der Stationen bestimmt werden kann. Die Auslastung des Netzes ist aus dem Zugangskontrollmechanismus bekannt.

Um die Daten weiterverwenden zu können, müssen sie allerdings noch aggregiert und ausgewertet werden. Darauf wird im folgenden Kapitel näher eingegangen.

5.4 Managementprotokoll

Zum Sammeln der Daten und zur Rekonfiguration der Endgeräte wird das Simple Network Management Protokoll SNMP [72, 77] verwendet, weil es das am weitesten verbreitete Managementprotokoll ist und dadurch Kompatibilität zu anderen Netzen gewährleistet wird. Die Grundlagen von SNMP wurden in Kap. 2.3 schon genauer beschrieben.

5.4.1 Nachrichten

Durch die Clusterbildung wird das Netz in zwei Hierarchieebenen unterteilt (siehe Abb. 5.4). Alle Geräte sind bei ihrem jeweiligen Clusterhead registriert, und dieser kann Informationen der Teilnehmer auslesen und gegebenenfalls ändern. Die CHs wiederum melden sich bei der zentralen Managementeinheit an, welche die Daten ausliest, die von den Clusterheads bereitgestellt werden. Diese Daten umfassen die eigenen Informationen der Clusterheads sowie die Informationen der Clusterteilnehmer, die am CH gebündelt werden. Auf diese Weise kann die Managementeinheit die Informationen aller Netzteilnehmer erfassen. Die Datenerfassung erfolgt über die SNMP-spezifischen Nachrichten (siehe [72] und Kap. 2.3). Für die Organisation der Cluster sind eigene Nachrichten erforderlich, die im Folgenden dargestellt werden.

Hallo-Nachricht: Ein neu hinzugekommener Knoten verschickt diese Anfrage, um herauszufinden, ob sich ein Clusterhead in der Nähe befindet.

ACK: Auf eine Hallo-Nachricht antwortet ein Clusterhead mit einem ACK und bestätigt damit, dass er Clusterhead ist. In der Nachricht wird die Kennung des CH (und gegebenenfalls die Eignung entsprechend der verwendeten Metrik) mitgeschickt.

JOIN: Ein Knoten teilt einem Clusterhead mit, dass er sich dem Cluster anschließen möchte.

Abb. 5.5 und 5.6 zeigen zwei Fälle als Nachrichtenflussdiagramme: Station B ist neu hinzugekommen und sucht in der Umgebung nach einem Clusterhead. Im ersten Fall (Abb. 5.5) ist Station C bereits CH und antwortet entsprechend auf die Anfrage. B schließt sich daraufhin dem Cluster an. C forder periodisch von allen Stationen des Clusters Informationen an – dies wird mit Hilfe von SNMP erledigt und ist hier durch *Info-Req* angedeutet, woraufhin die einzelnen Stationen mit den jeweiligen Informationen antworten. Abb. 5.6 zeigt den Fall, dass noch kein Clusterhead in der Nähe ist. Wenn Knoten B keine Antwort erhält, ernennt er sich selbst zum CH und antwortet entsprechend auf die Anfrage von Knoten C, der erst später hinzukommt und sich in diesem Fall B anschließen kann.

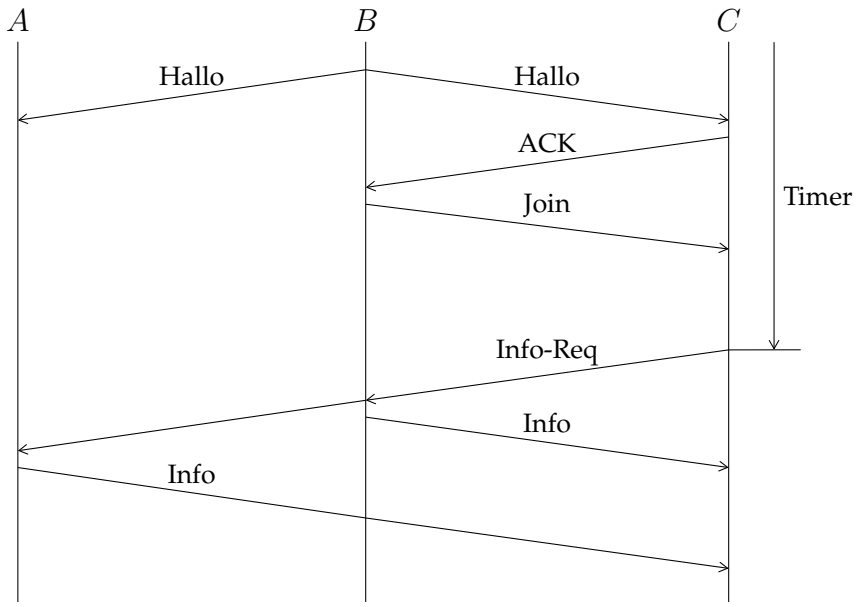


Abbildung 5.5: Clusteringalgorithmus

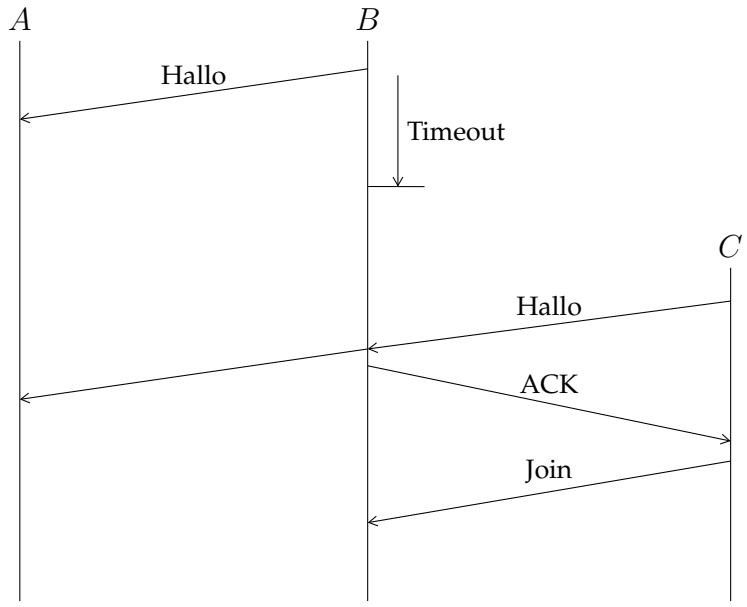


Abbildung 5.6: Clusteringalgorithmus

5.4.2 Daten

Weiter oben wurde bereits die zweistufige Hierarchie beschrieben (siehe Abb. 5.4). Knotengrad und Auslastung der einzelnen Stationen werden lokal bestimmt und abgespeichert. Die Clusterheads lesen diese Informationen aller Stationen des Clusters aus und speichern sie in einer Liste. Daraus können die Zahl der Clusterteilnehmer, der maximale Knotengrad sowie die maximale Auslastung bestimmt werden, welche vom CH ebenfalls abgespeichert werden. Zusätzlich gibt es einen Wert für das Zeitintervall, in dem der Clusterhead die Daten auslesen soll. Dieses kann vom Manager gesetzt werden. Der Manager kann außerdem sowohl die einzelnen Datensätze der Knoten aus der Liste auslesen sowie die aggregierten Daten (maximale Auslastung und Knotengrad sowie Anzahl der Clusterteilnehmer).

Die Verwendung von SNMP setzt voraus, dass die Daten strukturiert dargestellt werden, um ausgelesen werden zu können. Ähnlich der in [20] vorgeschlagenen Erweiterung von SNMP für Ad-hoc-Netze wird hier die MIB-II [73] um einige für vermaschte drahtlose Netze spezifische Einträge ergänzt (siehe Abb. 5.7). Um die Komplexität gering zu halten, werden möglichst wenige neue Objekte definiert. Es ist aber problemlos möglich, bei Bedarf noch weitere zu ergänzen. Die neu hinzugefügte Gruppe *MESH* umfasst die beiden Untergruppen *Local* und *Cluster*. Erstere ist für die lokal an jedem Knoten gespeicherten Daten gedacht, was in diesem Fall die Anzahl der Nachbarn (*numberNeighbors*) und die aktuelle Auslastung (*Load*) sind. Außerdem fallen hierunter die Parameter, die von außen geändert werden sollen, also die Fenstergröße (*WindowSize*), die Sendewahrscheinlichkeit für Medienzugriff bzw. Priorisierung (*PADCCProb*) und der Schwellenwert für die Zugangskontrolle (*CACThresh*). Diese Objekte werden in Kap. 5.4.3 genauer erläutert. Die Gruppe *Cluster* wird nur von den Clusterheads benötigt. Sie umfasst eine Liste der Daten der Clusterteilnehmer (*NodeList*) mit der jeweiligen Teilnehmerkennung (*nodeID*), sowie eine Vorauswertung der Daten in dem Sinne, dass die Anzahl der Clusterteilnehmer (*numberNodes*) und der maximale Knotengrad (*maxNodeDegree*) bzw. die maximale Auslastung (*maxLoad*) der Clusterteilnehmer in einem eigenen Datenfeld gespeichert werden, um das Auslesen durch den Manager zu vereinfachen. Daneben gibt es das Objekt *UpdateInterval*, welches vom Manager verändert werden kann und angibt, in welchen zeitlichen Abständen der Clusterhead die Informationen der Teilnehmer abrufen soll.

5.4.3 Ändern der Parameter

Ein wichtiger Aspekt der Managementarchitektur ist, dass die verwendeten Mechanismen während des Betriebs rekonfiguriert werden können. Dazu ist eine Eingriffsmöglichkeit von außen notwendig. Genau wie das Auslesen der Daten erfolgt die Änderung der Parameter mit Hilfe von SNMP. Die entsprechenden Datensätze sind in Abb. 5.7 zu sehen.

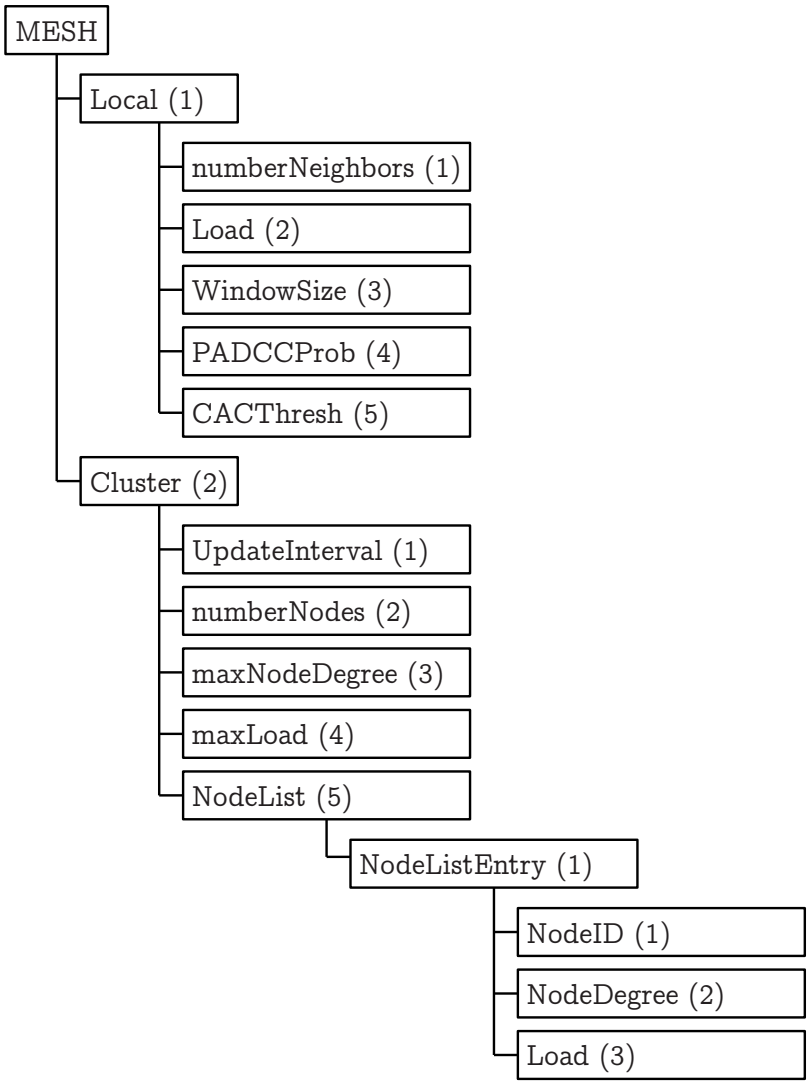


Abbildung 5.7: MIB-Erweiterung

WindowSize bezeichnet die Fenstergröße ($CW_{\min}$) für das Medienzugriffsverfahren, anhand derer nach Tab. 4.1 die Werte für die einzelnen Verkehrsklassen berechnet werden können. *PADCCProb* ist die Sendewahrscheinlichkeit für den PADCC-Mechanismus. Diese wird mit Hilfe von Formel 3.4 und 3.5 bestimmt. Durch Ändern des Parameters ist es möglich, zwischen verschiedenen weiteren Berechnungsmethoden zu wechseln, oder PADCC ganz auszuschalten (entspricht einer Sendewahrscheinlichkeit von 1). Der Schwellenwert für die Zugangskontrolle, *CACThresh*, bezeichnet den Anteil an der Gesamtkapazität, die durch Datenverkehr belegt sein darf.

Alle Dienstgütemechanismen haben Standardeinstellungen für die einzelnen Parameter, die beispielsweise nach einem Neustart verwendet werden, oder wenn eine Station neu zum Netz hinzukommt. Diese Standardwerte werden in die MIB eingetragen. Im laufenden Betrieb greift der Manager bzw. der Clusterhead auf die

Werte zu und ändert sie bei Bedarf. Das Ändern der Parameter wird also durch den Manager herbeigeführt. Die Basis für die Entscheidungen wird in Kap. 5.5 ausführlich behandelt. Hier soll kurz angesprochen werden, welche Auswirkungen der Vorgang auf das Netz hat bzw. haben kann. Wichtige Fragen hierbei sind:

- Wie lange dauert es, bis die Änderungen an das ganze Netz weitergegeben sind?
- Was passiert, wenn die Information bei manchen Knoten erst später bzw. gar nicht ankommt?

Hier ist ein Vorteil von DARMA, dass die Entscheidung über eine Parameteränderung zentral getroffen wird. Das bedeutet, dass die Entscheidung immer eindeutig ist. Bei dezentraler Steuerung könnten verschiedene Einheiten zu verschiedenen Schlüssen gelangen – das ist hier nicht der Fall. Der Manager informiert die Clusterheads, welche wiederum die Information an ihre Teilnehmer weitergeben. Es sind also zwei konsekutive Nachrichten notwendig, bis alle Knoten im Netz informiert sind. Im fehlerfreien Fall bedeutet das, dass in weniger als einer Sekunde alle Stationen informiert werden können.

Es kann natürlich passieren, dass eine solche Nachricht verloren geht, und deshalb nicht alle Stationen zeitnah von den Änderungen erfahren. In diesem Fall würden einzelne Knoten oder auch einzelne Cluster mit den alten Einstellungen weiterarbeiten. Eine Station, die mit einer anderen Fenstergröße oder Sendewahrscheinlichkeit arbeitet als ihre Nachbarn, hat (je nachdem ob der Wert größer oder kleiner ist) einen leichten Vor- oder Nachteil beim Zugriff auf das Medium. Wenn das ganze Cluster einen falschen Wert verwendet, ist die Fairness innerhalb des Clusters gegeben, weil die Teilnehmer aufgrund des Clusteringalgorithmus mit hoher Wahrscheinlichkeit benachbart sind. Der Durchsatz ist dann jedoch nicht optimal, und der Vor- oder Nachteil ergibt sich gegenüber benachbarten Clustern. Falls ein zu hoher CAC-Schwellenwert verwendet wird, kann das Auswirkungen auf das ganze Netz haben, da dann eventuell zu viel Verkehr zugelassen wird. Hierbei ist auch zu bedenken, dass ein Absenken des Wertes nicht in jedem Fall sofort umgesetzt werden kann, beispielsweise wenn der Knoten in Bezug auf den älteren, höheren Wert komplett ausgelastet ist. Die Änderung macht sich dann erst bemerkbar, wenn Datenströme beendet werden, bzw. bei der Zulassung neuen Verkehrs.

Normalerweise ändern sich die Parameter aber graduell, sodass die Unterschiede zwischen den verschiedenen Stationen nicht groß sind. Trotzdem ist es (insbesondere in Bezug auf Fairness) wichtig, dass eine Parameteränderung möglichst schnell von allen Stationen umgesetzt wird. Deshalb überprüfen der Manager bzw. die CHs nach einer Umstellung noch einmal, ob alle Stationen die richtigen Parameter verwenden.

5.4.4 Ausfall eines Clusterheads

Wenn ein Clusterhead ausfällt, sei es aufgrund eines Fehlers oder weil das Gerät ausgeschaltet wird, bemerken die Clusterteilnehmer dies daran, dass sie kein *Info-Req*

mehr erhalten. Daraufhin führen sie den in Kap. 5.1.1 vorgestellten Clusteringalgorithmus erneut aus und schließen sich (falls möglich) einem benachbarten Cluster an oder formen ein neues Cluster. Dies kann vorübergehend zu einer ungünstigeren Strukturierung führen. Insgesamt werden jedoch Gateways und andere statische Knoten in der Regel seltener ausgeschaltet als mobile Geräte und eignen sich daher besser als CH (dies spiegelt sich auch in der Metrik zur Auswahl der Clusterheads wider). Falls bei der Neubildung der Cluster ein weniger gut geeigneter Knoten CH wird, ist die Wahrscheinlichkeit, dass dieser bald wieder ausfällt, höher. Demnach wird die Clusteraufteilung mit der Zeit besser, weil Cluster mit besser geeigneten CHs insgesamt eine höhere Lebensdauer haben.

5.4.5 Timer

Eine geeignete Dauer für einen Timer zu finden, bedeutet immer einen Kompromiss einzugehen. Werden häufiger Daten abgerufen, steigt der Verkehr an, was natürlich unerwünscht ist. Gleichzeitig kann jedoch der Zustand des Netzes besser eingeschätzt werden, wenn aktuellere Daten vorliegen. Deshalb ist zunächst die Überlegung notwendig, wie schnell sich die Werte, die abgelesen werden sollen, ändern.

Topologie: Da die betrachteten Netze relativ statisch sind, entstehen Änderungen in der Topologie in erster Linie nicht durch Bewegung, sondern durch das An- und Ausschalten von Endgeräten. Deshalb ist davon auszugehen, dass die Topologie abhängig vom Szenario über mehrere Minuten bis Stunden gleich bleibt.

Auslastung: Die Auslastung der einzelnen Knoten ändert sich hingegen schneller. Im schlimmsten Fall kann das Netz sogar innerhalb weniger Sekunden bis Minuten voll ausgelastet sein, wenn beispielsweise nach einer Besprechung alle Mitarbeiter an ihren Arbeitsplatzrechner zurückkehren und dort neuen Datenverkehr generieren. Abgesehen von solchen Extremfällen sollte sich der Verkehr in großen Netzen im Durchschnitt relativ gut verteilen, weswegen auch die Auslastung über mehrere Minuten bis Stunden als konstant angenommen werden kann.

Die nächste Überlegung ist, wieviel Aufwand es bedeutet, die Parameter im Netz zu ändern, und wieviel Zeit diese Änderung in Anspruch nimmt. Wie in Kap. 5.4.3 bereits angesprochen, lassen sich die Werte einfach und innerhalb geringer Zeit umschalten. Allerdings wird durch die Signalisierung zusätzlicher Verkehr erzeugt, und nach jeder Änderung müssen die Werte aller Stationen nochmals überprüft werden. Deshalb sollten die Parameter am besten so selten wie möglich geändert werden.

SNMP bietet auch die Möglichkeit, dass Agenten sogenannte *Traps* schicken, um den Manager unaufgefordert über aufgetretene Ereignisse zu informieren. Dies kann genutzt werden, falls z.B. die Last plötzlich oder über einen festgesetzten Schwellenwert ansteigt. Darauf soll hier jedoch nicht näher eingegangen werden.

Fazit

In durchschnittlichen Netzen reicht es, wenn die Parameter im Abstand von einigen Minuten bis ca. 1–2 Stunden (je nach Szenario) ausgelesen werden. Plötzlich auftretende Ereignisse können zusätzlich mit Hilfe von Trap-Nachrichten gemeldet werden. Eine Änderung der Parameter ist im Normalfall seltener nötig, und wird durchgeführt wann immer die Voraussetzungen dazu gegeben sind (siehe auch Kap. 5.6). Um ein ständiges Hin- und Herschalten zwischen zwei Zuständen zu verhindern, ist der Einsatz einer Hysterese angebracht.

5.5 Rückkopplung zur QoS-Architektur

In den vorigen Kapiteln wurde erläutert, wie die im Netz vorhandenen Informationen durch eine Managementeinheit abgerufen und in einer zentralen Datenbank abgelegt werden. Anschließend können diese Informationen genutzt werden, um die Parameter der QoS-Architektur zu verändern. Dies kann entweder automatisiert ablaufen oder durch einen Netzadministrator angestoßen werden. In beiden Fällen ist es notwendig, dass ein Zusammenhang zwischen Netzzustand und adäquater Reaktion darauf hergestellt wird. Das kann kognitiv passieren, wenn Menschen involviert sind, ansonsten als Regel, die in einer Datenbank hinterlegt ist.

In den Kapiteln 3 und 4 wurden die Zusammenhänge zum Teil schon dargestellt. Hier folgt eine Zusammenfassung.

5.5.1 Zugangskontrolle

Beim betrachteten Zugangskontrollmechanismus gibt es mehrere Einstellungen, die verändert werden können.

Als erstes ist der Schwellenwert zu nennen. Wie in Kap. 3.1.1 genauer erläutert, gibt er an, welcher Anteil der verfügbaren Kapazität durch Datenverkehr belegt werden darf. Wenn die Schwelle erreicht ist, können keine neuen Verkehrsströme mehr zugelassen werden. Die Konsequenzen daraus sind folgende: Ein niedriger Schwellenwert führt dazu, dass mehr Verkehrsströme abgelehnt werden, die Kapazität wird dann nicht optimal genutzt. Ein hoher Schwellenwert hat andererseits zur Folge, dass wenig Reserve in Bezug auf die Kapazität vorhanden ist. Da die Entscheidungen über die Zulassung neuer Verkehrsströme dezentral vorgenommen werden, sind sie nicht immer zu 100% konsistent. Dadurch kann es zu Ressourcenengpässen kommen, wenn nicht genügend Reserve zur Verfügung steht. Es muss also abgewogen werden zwischen hoher Blockierungsrate und Verschwendung von Kapazität auf der einen Seite, bzw. Degradation der Dienstgüte auf der anderen Seite.

Welche der beiden Alternativen mehr Gewicht hat, hängt in erster Linie vom Szenario ab. So ist es in einer Büroumgebung wichtig, dass der Datenverkehr zuverlässig

transportiert wird. Hier ist also ein niedriger Schwellenwert sinnvoll. In Netzen, die unentgeltlich genutzt werden, beispielsweise Internetzugang auf einem Universitätscampus, ist hingegen eine maximale Ausnutzung der Kapazität von größerem Interesse. Hier wird der Schwellenwert hoch gewählt. Neben dem Szenario spielt auch die Gesamtkapazität des Netzes eine Rolle bei der Festsetzung des Wertes. Wenn nur in sehr begrenztem Umfang Ressourcen zur Verfügung stehen, ist es umso wichtiger, diese nicht zu veschwenden. Wenn hingegen die Ressourcenbelegung stark schwankt, ist eine niedrige Schwelle besser, um mehr Reserve zu haben.

Die Schwelle, ab der das Netz als überlastet betrachtet wird, kann ebenfalls geändert werden. Da diese eng mit dem oben angesprochenen Schwellenwert zusammenhängt, sind die dadurch entstehenden Unterschiede aber so gering, dass sich die Anpassung kaum lohnt.

Für die Zulassung von Verkehrsströmen können auch Prioritäten verwendet werden. Anders als bei der Verkehrskategorisierung sind diese unabhängig von der Art des Datenverkehrs, sondern an das jeweilige Endgerät gebunden. So kann man beispielsweise sicherstellen, dass in einem Katastrophenszenario der Einsatzleiter jederzeit auf das Netz zugreifen kann. Eine solche Priorisierung ist stark vom Szenario abhängig, sodass eine Änderung während des Betriebs normalerweise nicht notwendig ist.

Eine weitere Einstellmöglichkeit ist die Regelung, welche Verkehrsströme als erstes abgebrochen werden, falls dies wegen Überlast notwendig werden sollte. Dazu kann die eben genannte Priorität als Kriterium verwendet werden, sodass weniger wichtige Datenströme als erstes beendet werden. Daneben gibt es auch die Möglichkeit, die zuletzt zugelassenen Verkehrsströme als erstes wieder zu beenden. Hierbei handelt es sich ebenfalls um eine grundsätzliche Designfrage, die im Vorhinein festgelegt und nicht während des Betriebs geändert wird.

5.5.2 Medienzugriff und Verkehrskategorisierung

Die Auswirkungen, die Stationenzahl bzw. Auslastung auf der einen Seite und Durchsatz bzw. Verzögerung auf der anderen Seite auf das Medienzugriffsverfahren haben, wurden in Kap. 4 bereits ausführlich diskutiert. Hier sollen die wichtigsten Punkte noch einmal zusammengefasst werden.

Die Fenstergrößen ($CW_{\min}(i)$ und $CW_{\max}(i)$) der einzelnen Verkehrklassen können im Prinzip beliebig geändert werden, es gibt im Standard jedoch Vorgaben [63]. Wenn die Fenstergröße diesen Vorgaben entsprechend gewählt wird, bleibt das Verhältnis zwischen den einzelnen Prioritäten immer erhalten, da die Fenstergröße aller Verkehrsklassen gleichzeitig geändert wird. So kann die Zeit für den Kanalzugriff angepasst werden, ohne die Priorisierung zu verändern. Bei hoher Netzauslastung (das entspricht einer hohen Stationenzahl, wenn alle Stationen Daten senden) ist eine größere Fenstergröße sinnvoll, weil dann zwischen zwei konsekutiven Kanalzugriffen einer Station mehr Zeit vergeht. Bei niedriger Netzauslastung kann ein kleineres Fenster verwendet werden, um die vorhandene Kapazität voll auszunutzen.

Die Anzahl der Verkehrsklassen ist im Standard ebenfalls vorgegeben. Die vier vordefinierten Klassen (Voice, Video, Best Effort und Background) sind dabei jedoch auf typischen Internetverkehr ausgelegt. In Katastrophenszenarien kann es sinnvoll sein, nur zwei Verkehrsklassen zu verwenden (zeitkritischer Verkehr und sonstiger Verkehr). Dadurch werden die Unterschiede zwischen den Klassen größer, und die Pakete mit höherer Priorität werden demnach stärker bevorzugt.

Eine Änderung des IFS soll hier nicht näher betrachtet werden, wie in Kap. 3.1.2 auch bereits diskutiert.

Für die Berechnung der Sendewahrscheinlichkeit (PADCC) gelten Formel 3.4 und 3.5. Es ist jedoch möglich, eine andere Berechnungsvorschrift zu verwenden, und auch während des Betriebs zwischen verschiedenen Methoden umzuschalten. Abhängig vom Szenario kann eine Priorisierung (ähnlich wie beim CAC-Mechanismus) sinnvoll sein, sodass einzelne Endgeräte, die aus bestimmten Gründen wichtiger sind als andere, häufiger auf den Kanal zugreifen können. In Kap. 4.7 wurde gezeigt, dass die Verwendung von PADCC kaum Einfluss auf den Durchsatz hat, wenn über die Stationenzahl (bzw. die Auslastung) optimiert wird. PADCC ist aber schneller anpassungsfähig und deshalb bei stark schwankendem Verkehr vorzuziehen. In relativ statischen Szenarien kann hingegen darauf verzichtet werden, um die Komplexität zu verringern.

5.5.3 Zusammenfassung

Abhängig vom Zustand des Netzes kann also angegeben werden, welche Parameter zu optimalen Ergebnissen führen. Eine Zusammenfassung der Zusammenhänge zwischen Netzzustand und geeigneten Parametern ist in Tab. 5.2 dargestellt. Dort lässt sich ablesen, wie die Dienstgütemechanismen in bestimmten Szenarien und Betriebsfällen einzustellen sind.

Das Szenario ist vor der Inbetriebnahme des Netzes bekannt, die entsprechenden Werte können also im Vorhinein eingestellt werden. Die anderen Parameter (Auslastung, Stationenzahl, Schwankungen in Auslastung und Stationenzahl) ändern sich während des Betriebs. Sie werden mit Hilfe des in Kap. 5.4 vorgestellten Protokolls ausgelesen und die entsprechende Reaktion ausgeführt. Konkret bedeutet das z.B. für den CAC-Schwellenwert: Im Campus-Szenario ist der Wert generell relativ hoch, wird aber herabgesetzt, falls das Netz starken Schwankungen unterliegt. Im Office-Szenario hingegen ist der Wert grundsätzlich relativ niedrig, kann aber bei niedriger Netzauslastung oder geringen Schwankungen erhöht werden. Stationenzahl und Auslastung hängen voneinander ab, sofern alle Stationen ein ähnliches Verhalten aufweisen. Höhere Stationenzahl führt dann zu höherer Last, und beides führt wiederum zur Vergrößerung des Zeitfensters (CW). Der entscheidende Parameter ist hier allerdings die Auslastung. Bei kleiner Stationenzahl und hoher Auslastung sollte CW demnach groß gewählt werden.

Tabelle 5.2: Regeln für die Anpassung der Parameter

		Zugangskontrolle			Priorisierung / Medienzugriff				Timer
		Schwellen-wert	Priori-sierung	ECN	Verkehrs-klassen	CW	AIFS	PADCC	
Szenario	Campus	hoch	nein	neueste	vier	–	–	–	lang
	Office	niedrig	ja	prio	vier	–	–	–	kurz
	Emergency	–	ja	prio	zwei	–	–	–	kurz
Schwankungen	hoch	niedrig	–	–	–	–	–	an	kurz
	niedrig	hoch	–	–	–	–	–	aus	lang
Auslastung	hoch	mittel	–	–	–	groß	–	–	–
	niedrig	hoch	–	–	–	klein	–	–	–
Stationenzahl	niedrig	–	–	–	–	klein	–	–	–
	mittel	–	–	–	–	mittel	–	–	–
	hoch	–	–	–	–	groß	–	–	–

5.6 Aufwand/Nutzen-Abschätzung

Basierend auf den Simulationsergebnissen aus Kap. 3 und 4 soll hier ein Vergleich des Durchsatzes, der mit und ohne den Einsatz der DARMA Managementarchitektur erzielt werden kann, angegeben werden. Hierbei handelt es sich um eine theoretische Abschätzung, da für das Managementsystem keine Implementierung vorliegt.

Das Szenario umfasst ein Gateway und 15 Stationen, die sich in Sendereichweite des Gateways befinden. Zu Beginn sendet eine Station mit 1 Mbit/s Daten an das Gateway, jeweils nach 10 s beginnt eine weitere Station mit derselben Datenrate zu senden. Einmal pro Minute, also in jedem sechsten Zeitintervall, wird der Status des Netzes abgefragt und gegebenenfalls die Parameter angepasst. Es wird angenommen, dass dadurch der Durchsatz in dem entsprechenden Zeitintervall um 2% absinkt und dass im nächsten Intervall die neuen Parameter vorliegen und verwendet werden. Abb. 5.8 zeigt die durchschnittliche erzielte Gesamtdatenrate (auf der Anwendungsschicht) in den einzelnen Zeitintervallen für unterschiedliche CAC-Schwellenwerte.

Die grauen Linien (Winkelhalbierende) stellen das Verkehrsangebot dar und geben demnach die Obergrenze für den erzielbaren Durchsatz an. Dieser kann in der Realität nur dann erreicht werden, wenn keinerlei Kollisionen auftreten. Sobald mehr als eine Station Daten sendet, fällt der tatsächliche Durchsatz demnach unter diese Grenze.

Die blauen Kurven ergeben sich bei Verwendung von reinem 802.11e (Abb. 5.8 a und c) bzw. PADCC (Abb. 5.8 b und d), ohne Zugangskontrolle und/oder Management. Bei hoher Stationenzahl steigt die Kollisionswahrscheinlichkeit der gesendeten Pakete, weil die Stationen sich gegenseitig stören. Dadurch sinkt der erzielte Gesamtdurchsatz.

Der Einsatz eines Zugangskontrollverfahrens (hier DAC, grüne Kurven) begrenzt den zugelassenen Verkehr, hier auf 80% (Abb. 5.8 a und b) bzw. 60% (Abb. 5.8 c und d). Das entspricht zehn bzw. sieben Stationen, die Daten senden dürfen. Für die restliche Dauer der Simulation bleibt der Durchsatz deshalb konstant, weil keine weiteren Verkehrsströme mehr zugelassen werden.

Die roten Kurven zeigen die Abschätzung für den Durchsatz mit Verwendung der Gesamtarchitektur. Im sechsten und zwölften Zeitintervall ist jeweils der Einbruch im Durchsatz zu sehen, der den Overhead des Managementprotokolls widerspiegelt. Im siebten Intervall kommen dann die geänderten Parameter zum Einsatz: Konkret wird hier die Fenstergröße des Medienzugriffsverfahrens auf die Stationenzahl angepasst und führt dadurch zu höherem Gesamtdurchsatz. Bei zehn bzw. sieben Stationen greift der Zugangskontrollmechanismus ein und lässt keine weiteren Verkehrsströme zu. Im zwölften Zeitintervall, während der nächsten Managementphase, wird festgestellt, dass die aktuelle Stationenzahl keine weitere Änderung der Fenstergröße erfordert. In Abb. 5.8 c und d wird an dieser Stelle allerdings der CAC-Schwellenwert erhöht, weil dieser mit 60% relativ niedrig ist im Vergleich zur Auslastung des Netzes.

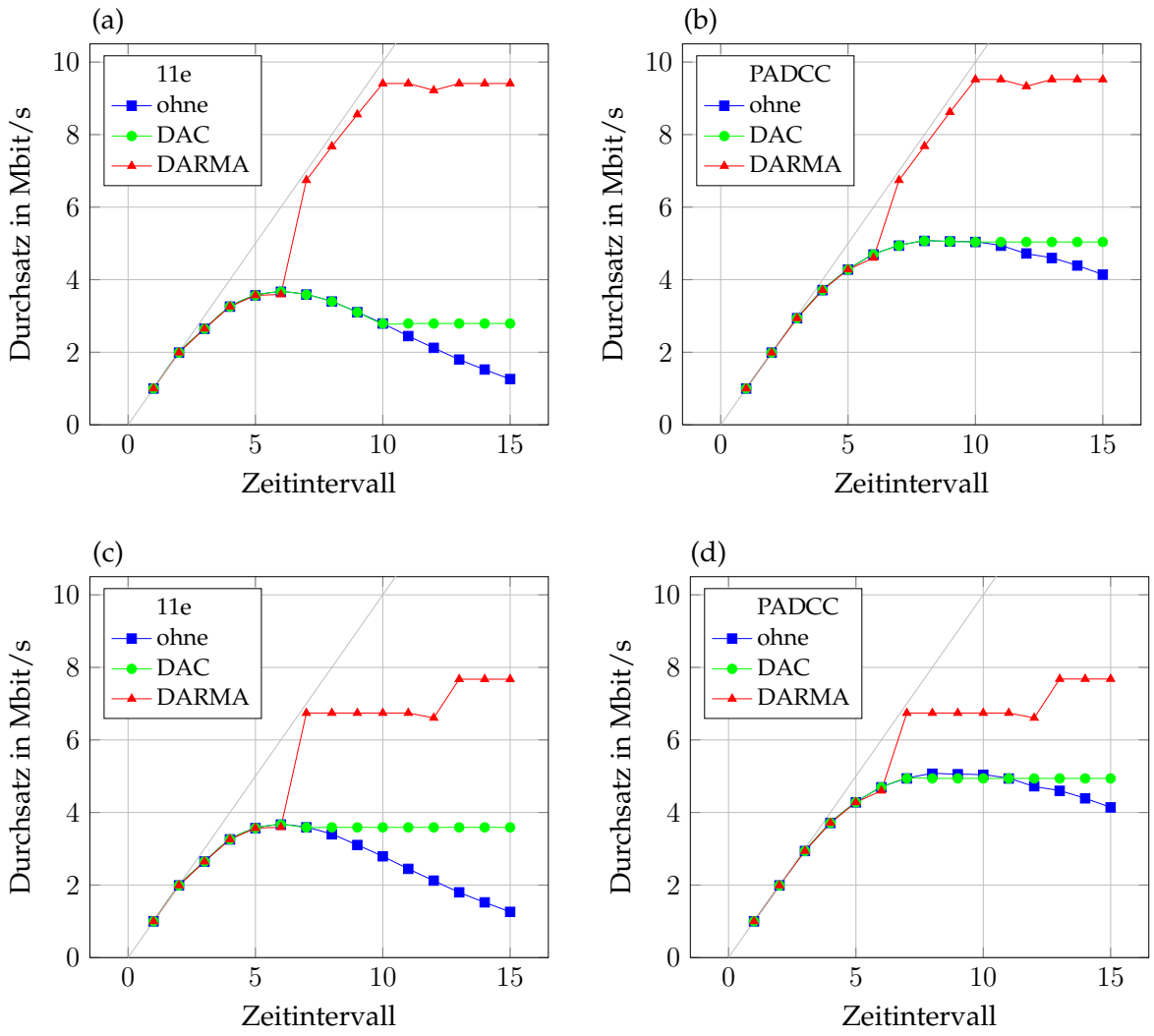


Abbildung 5.8: Durchschnittlicher Durchsatz mit und ohne Verwendung von DARMA, oben mit CAC-Schwellenwert 80%, unten 60%

Durch eine Erhöhung der Schwelle auf 65% kann ein weiterer Verkehrsstrom zugelassen werden.

Tabelle 5.3 zeigt den Gesamtdurchsatz über die ganze Simulationsdauer. Wenn keine Zugangskontrolle eingesetzt wird, hat die Wahl des CAC-Schwellenwertes dabei keine Bedeutung.

Tabelle 5.3: Gesamtdurchsatz

Mechanismus		Durchsatz	
		Schwellenwert 0,8	Schwellenwert 0,6
802.11e	ohne	2,54 Mbit/s	2,54 Mbit/s
	DAC	2,86 Mbit/s	3,23 Mbit/s
	DARMA	6,28 Mbit/s	5,24 Mbit/s
PADCC	ohne	4,10 Mbit/s	4,10 Mbit/s
	DAC	4,26 Mbit/s	4,20 Mbit/s
	DARMA	6,49 Mbit/s	5,40 Mbit/s

PADCC erzielt einen höheren Durchsatz als reines 802.11e, wobei die Unterschiede zwischen den beiden Mechanismen durch den Einsatz von DARMA geringer werden. Dies wurde in Kap. 4.7 bereits diskutiert. DARMA erreicht außerdem in jedem der betrachteten Fälle den höchsten Gesamtdurchsatz, obwohl durch das Management zusätzlicher Overhead entsteht. Dieser wird aber dadurch kompensiert, dass durch die Anpassung der Fenstergröße der Durchsatz erheblich gesteigert werden kann. Aus der Tabelle wird im Zusammenhang mit 802.11 und DAC außerdem ersichtlich, dass ein höherer Zugangskontrollschwellenwert nicht zwingend zu höherem Gesamtdurchsatz führt. Dies wird auch in Abb. 5.8 deutlich: Bei einer Netzauslastung von 80% ist die Kollisionswahrscheinlichkeit bereits so hoch, dass der erzielbare Durchsatz unter dem maximal möglichen Wert liegt. Der niedrigere Schwellenwert führt demnach hier zu besseren Ergebnissen. Bei DARMA tritt diese Problematik nicht auf, da dort die Fenstergröße entsprechend angepasst wird.

In Abb. 5.9 ist für das oben beschriebene Szenario mit Zugangskontrollschwellenwert 80% dargestellt, wie sich eine Änderung des Managementintervalls auf den Durchsatz auswirkt. Zum Vergleich sind 30, 60 und 100 Sekunden eingetragen. Bei Verwendung eines großen Intervalls kann erst spät auf die geänderten Voraussetzungen reagiert werden. Dadurch werden über lange Zeit suboptimale Parameter verwendet, was sich ungünstig auf den Durchsatz auswirkt. Bei Verwendung eines kleinen Intervalls kann immer zeitnah auf neue Parameter gewechselt werden, dafür sind aber die Verluste durch den Overhead höher.

Da es sich hier nur um eine Abschätzung handelt, sind die Graphen rein qualitativ zu betrachten und können daher nicht genutzt werden, um genaue Werte abzulesen.

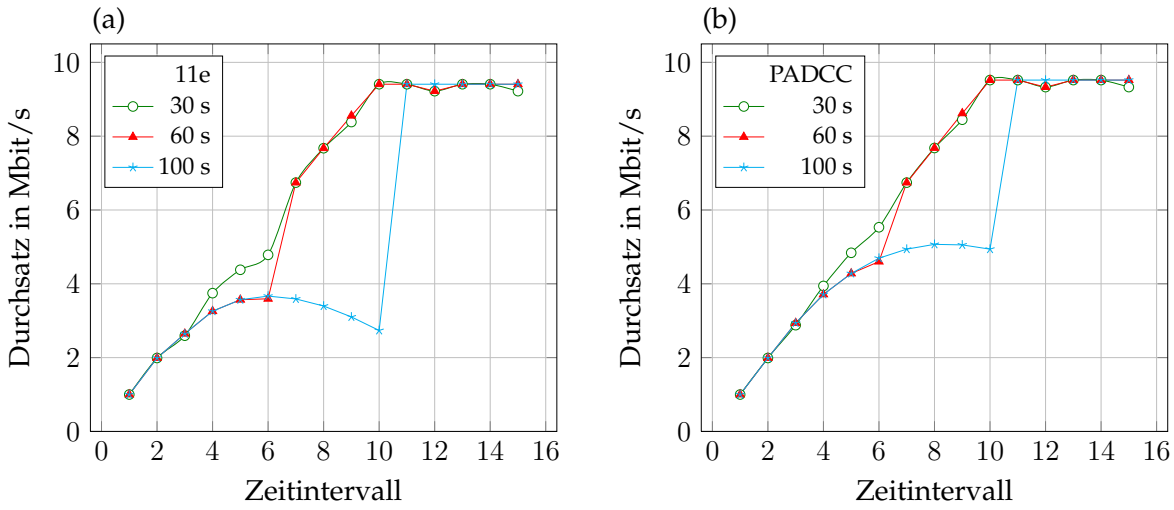


Abbildung 5.9: Durchschnittlicher Durchsatz für unterschiedliche Managementintervalle

5.7 Beiträge dieser Arbeit

Die in dieser Arbeit vorgestellte Managementarchitektur basiert auf SNMP und ist daher kompatibel zu bestehenden Systemen. Die Funktionalität von SNMP wurde dahin gehend erweitert, dass die spezifischen Anforderungen von WMNs unterstützt werden. Dabei ist neben Methoden für die Clusterbildung insbesondere die Möglichkeit, auf die Dienstgütemechanismen zuzugreifen, interessant. Die Kombination aus Überwachung des Netzzustandes und Rückkopplung zur QoS-Architektur ermöglicht die flexible Anpassung an die jeweilige Situation, sowohl in der Planungsphase als auch während des Betriebs. Dadurch ist die Architektur vielseitig einsetzbar und nicht auf bestimmte Szenarien beschränkt. Mit Hilfe einer Datenbank, welche mögliche Netzzustände mit geeigneten Parametereinstellungen verknüpft, ist sogar eine automatische Anpassung möglich.

6 Zusammenfassung und Ausblick

6.1 Beiträge dieser Arbeit

Im Rahmen dieser Arbeit wurde DARMA entwickelt, eine QoS- und Managementarchitektur für vermaschte drahtlose Netze, die das Netz überwacht und Dienstgüte bereitstellt. Die Dienstgütemechanismen lassen sich flexibel justieren und erlauben so eine optimale Anpassung an die äußeren Umstände. Dadurch ist die Architektur vielseitig einsetzbar und nicht auf spezielle Anwendungsfälle beschränkt.

Die QoS-Komponente von DARMA ist komplett auf der MAC-Schicht (Schicht 2 des OSI-Modells) angesiedelt. Dadurch ist sie nicht von speziellen Protokollen anderer Schichten abhängig, sondern mit verschiedenen Verfahren kombinierbar und damit kompatibel zu existierenden Systemen. Die Bereitstellung der Dienstgüte wird nicht anhand von Reservierung, sondern durch Zugangskontrolle und Priorisierung erzielt, was bei Nutzung eines unlizensierten Frequenzbandes vorteilhafter ist. Der Zugangskontrollmechanismus DAC sendet Testpakete entlang der Route und bedient sich dabei einer einfach zu realisierenden Abschätzung der verfügbaren Kapazität an jedem zwischenliegenden Knoten. Dadurch wird eine Degradation der Dienstgüte anderer Verkehrsströme vermieden. Die Priorisierung ist aus IEEE 802.11e übernommen und ddeshalb konform mit bestehenden Systemen. Das Medienzugriffsverfahren PADCC ist kompatibel zu dem bei IEEE 802.11e eingesetzten Verfahren, welches am weitesten verbreitet ist. Der Vorteil von PADCC ist, dass es in Situationen mit hoher Verkehrslast schneller reagieren kann. Alle Mechanismen sind frei konfigurierbar und dadurch für die zahlreichen unterschiedlichen Einsatzgebiete von WMNs geeignet, da sie an die jeweiligen spezifischen Anforderungen angepasst werden können.

Es wurde ein Markovmodell entwickelt, um den Priorisierungs- und Medienzugriffsmechanismus PADCC mathematisch zu beschreiben. Dieses kombiniert die Vorteile verschiedener bestehender Markovmodelle, darunter die Modellierung mehrerer Verkehrsklassen, sodass die Wahrscheinlichkeit für einen Kanalzugriff für jede Priorität einzeln dargestellt wird. Dabei wird berücksichtigt, dass Verkehrsklassen höherer Priorität früher auf den Kanal zugreifen können und so den Backoff von Verkehrsklassen mit niedrigerer Priorität unterbrechen können. Außerdem ist das Modell in der Lage, Post-Backoff und interne Kollisionen darzustellen. In bisherigen Modellen wurde auf diese Punkte nicht oder nur teilweise eingegangen. Mit Hilfe des Markovmodells ist die numerische Berechnung der stationären Wahrscheinlichkeiten für die einzelnen Zustände möglich. Aus diesen können wiederum Kollisionswahrscheinlichkeit, Durchsatz und Verzögerung berechnet werden. Das im Rahmen dieser Arbeit

entwickelte Markovmodell ermöglicht auch die Approximation von Multihop-Szenarien. Dazu muss die Zahl der Stationen, die eine Eingangsvariable des Modells ist, angepasst werden. Anstatt der Gesamtzahl der Knoten im Szenario werden nur noch diejenigen Stationen einbezogen, die eine Übertragung beeinflussen können.

Mit Hilfe des Markovmodells wurden die Parameter des Medienzugriffsverfahrens optimiert, um maximalen Durchsatz in Abhängigkeit der Stationenzahl zu erzielen. Dabei wurde gezeigt, dass für hohe Auslastung ein großes Zeitfenster *CW* sinnvoll ist, und umgekehrt für geringe Auslastung ein kleines Zeitfenster. Diese Ergebnisse erlauben die optimale Einstellung der Fenstergröße für ein gegebenes Szenario.

Die für DARMA konzipierte Managementkomponente umfasst einen Clusteringalgorithmus und ein Managementprotokoll. Der Clusteringalgorithmus nutzt intrinsische Eigenschaften von WMNs, indem er zusätzlich anfallende Managementaufgaben in erster Linie den Gateways zuteilt. Diese sind dafür besser geeignet als durchschnittliche Stationen, da sie eine permanente Stromversorgung haben und im Normalfall nicht ausgeschaltet werden. Falls die Gateways nicht ausreichen, können aber auch normale Teilnehmer diese Aufgaben übernehmen. Das Managementprotokoll ermöglicht das Auslesen des aktuellen Status des Netzes und die Änderung der Dienstgüteparameter während des Betriebs, um sie optimal an die Gegebenheiten anpassen zu können (entsprechend den Ergebnissen aus der Optimierung anhand des Markovmodells). Dabei ist es sinnvoll, die Parameter von Zugangskontrolle und Verkehrskategorisierung schon während der Planungsphase des Netzes geeignet einzustellen, und Medienzugriffssteuerung und Zugangskontrolle während des Betriebs weiter anzupassen. Das Managementprotokoll basiert auf SNMP und ist dadurch kompatibel zu anderen Systemen. SNMP wurde erweitert, um die speziellen Anforderungen von WMNs zu unterstützen. Mit Hilfe des Protokolls werden die Zahl der Stationen und die Auslastung ausgelesen, der Manager (entweder ein Netzadministrator oder eine Datenbank, in der entsprechende Instruktionen hintergelegt sind) veranlasst daraufhin die adäquaten Änderungen der Parameter.

6.2 Ausblick

Die in dieser Arbeit vorgestellte QoS- und Managementarchitektur DARMA dient dazu, die Überwachung des Netzes zu vereinfachen und gleichzeitig die Funktionalität zu verbessern. Endkunden profitieren dabei vom besseren Service, aber in erster Linie ist ein solches System für die Netzbetreiber interessant. Dadurch, dass der Aufwand für das Management verkleinert und die Effizienz gesteigert wird, können bei gleichbleibenden Kosten mehr Kunden bedient werden. Die vorgeschlagene Architektur ist über die vorgestellten Punkte hinaus erweiterbar. Das Management kann ausgeweitet werden, sowohl in Bezug auf die Evaluierung des Netzzustandes als auch beim Eingriff in die Funktionaliät. Bei den betrachteten Dienstgütemechanismen gibt es ebenfalls noch weitere Einstellungsmöglichkeiten. Beispielsweise ist mit Hilfe des Markovmodells auch eine Optimierung des AIFS möglich. Dies wurde hier nicht

betrachtet (siehe auch Kap. 3.1.2), könnte aber in anderen Fällen sinnvoll sein.

DARMA bietet ein holistisches Managementsystem, welches zu IEEE 802.11s kompatibel ist und dieses teilweise erweitert und verbessert. Die abgeschlossene Standardisierung von 802.11s wird demnächst vermehrt Einsatzmöglichkeiten für DARMA eröffnen: Es ist zu erwarten, dass es in näherer Zukunft zunehmend Geräte geben wird, die den Standard unterstützen. Durch die Interoperabilität von Geräten verschiedener Hersteller werden dann auch die Möglichkeit der Bereitstellung und die Nutzbarkeit von Mesh-Netzen verbessert. Dem extensiven Einsatz von WMNs steht dann nichts mehr im Wege, wodurch auch Managementsysteme erforderlich werden.

Allerdings entwickelt sich der zellulare Mobilfunk in der Zwischenzeit auch weiter, sodass im Moment noch nicht absehbar ist, welche Technologie sich durchsetzen wird, oder ob es auch langfristig mehrere Lösungen geben wird.

Anhang A

IEEE 802.11

Als Basis verwenden alle Stationen die in IEEE 802.11 definierten Mechanismen [63]. Der Standard IEEE 802.11n [65] als Erweiterung des ursprünglichen Standards definiert weitere Operationsmodi, die teilweise rückwärtskompatibel sind. Die in dieser Arbeit verwendeten Parameter werden im Folgenden dargelegt.

A.1 Physikalische Schicht

Auf physikalischer Schicht wird DSSS-OFDM (Direct Sequence Spread Spectrum Orthogonal Frequency Division Multiplexing) genutzt, welches voll kompatibel ist zu Stationen, die 802.11b oder g verwenden, aber gleichzeitig die Option beinhaltet, höhere Datenraten einzusetzen. Es verwendet als Frequenzband das ISM-Band bei $2{,}4$ GHz (ISM steht für Industrial, Scientific, and Medical, ein Frequenzband, das unlizensiert für Anwendungen in Industrie, Wissenschaft und Medizin zur Verfügung steht), mit einer Kanalbreite (channel width) von 20 MHz. Durch Einsatz unterschiedlicher Modulationsverfahren können die in Tab. A.1 dargestellten Datenraten erzielt werden. Hierbei steht R für die Coderate, N_{BPSCS} für die Anzahl der codierten Bits pro Träger, N_{CBPS} ist die Zahl der codierten Bits pro Symbol und N_{DBPS} die Zahl der Datenbits pro OFDM-Symbol. Diese Werte gelten bei Verwendung des langen Schutzintervalls (guard interval) von 800 ns. Vor einem Kanalzugriff muss die Station überprüfen, ob der Kanal frei ist. Dies ist der Fall, wenn für die Dauer eines Interframe Space (IFS) keine fremde Übertragung detektiert werden kann. Die Dauer des IFS hängt vom zu sendenen Paket ab (siehe Kap. A.2).

A.2 MAC-Schicht

Das Medienzugriffsverfahren verwendet Zeitschlitze konstanter Länge, und zwar 20 µs. Diese gelten aber nur innerhalb einer Station, verschiedene Stationen müssen sich also nicht untereinander synchronisieren. Der Zugriff auf das Medium erfolgt, wie bereits erwähnt, nach einem IFS. Wenn eine Quittung gesendet wird, muss nur für die Dauer eines kurzen IFS (Short Interframe Space, SIFS) gewartet werden. Bei Verwendung von mehreren Verkehrsklassen wird ein AIFS (Arbitrary Interframe Space) abgewartet, dessen Dauer von der jeweiligen Verkehrsklasse abhängt. Wird keine

Tabelle A.1: Modulations- und Codierungsparameter

Index	Modulation	R	N_{BPSCS}	N_{CBPS}	N_{DBPS}	Datenrate (Mbit/s)
0	BPSK	1/2	1	52	26	6,5
1	QPSK	1/2	2	104	52	13,0
2	QPSK	3/4	2	104	78	19,5
3	16-QAM	1/2	4	208	104	26,0
4	16-QAM	3/4	4	208	156	39,0
5	64-QAM	2/3	6	312	208	52,0
6	64-QAM	3/4	6	312	234	58,5
7	64-QAM	5/6	6	312	260	65,0

Priorisierung eingesetzt, so ist ein DIFS (DCF Interframe Space, DCF steht für Distributed Contention Function) abzuwarten. Für die unterschiedlichen Verkehrsklassen berechnet sich die Dauer des IFS aus den in Tab. A.2 dargestellten Werten für AIFSN (Arbitrary Interframe Space Number), der Dauer eines Zeitschlitzes und der Dauer des SIFS (hier 10 µs) nach Formel A.1.

$$t_{AIFS}(i) = AIFSN(i) \cdot t_{Slot} + t_{SIFS}, \tag{A.1}$$

wobei i die Verkehrsklasse (Access Category, AC) bezeichnet (AC_0 hat die höchste Priorität, AC_3 die niedrigste). Wenn keine Unterscheidung in Verkehrsklassen vorliegt, werden die Parameter in der letzten Zeile von Tab. A.2 verwendet.

Tabelle A.2: Verkehrsklassen

i	$AIFSN(i)$	$CW_{\min}(i)$	$CW_{\max}(i)$
0	2	7	15
1	2	15	31
2	3	31	1023
3	7	31	1023
ohne	2	15	1023

Das Medienzugriffsverfahren sieht vor, dass Kollisionen von Paketen so weit wie möglich verhindert werden. Sollte trotzdem ein Paket verloren gehen, wird dies durch Ausbleiben der Quittung bemerkt, und die Übertragung kann wiederholt werden. Bei kurzen Paketen (weniger als 3000 Byte) sind sieben Wiederholungen möglich, bei langen Paketen bis zu vier.

Weitere Parameter sind in Tab. A.3 dargestellt.

Tabelle A.3: Weitere Parameter

Paketheader (MAC-Schicht)	288 bit
Paketheader (Physikalische Schicht)	192 bit
– Präambel	144 bit
– PLCP-Header	48 bit
Quittung (PHY-Header + 112 bit)	304 bit
Dauer eines Symbols	4 µs
Übertragungsdauer eines Datenpakets	294 µs
Übertragungsdauer einer Quittung	214 µs
ACK-Timeout	222 µs

Anhang B

Simulator ns-2

B.1 Grundlagen

Der *Network Simulator 2* [81] oder kurz *ns-2* wurde an der University of California in Berkeley entwickelt. Es handelt sich dabei um einen modularen objektorientierten Simulator für diskrete Ereignisse, der für die Forschung im Bereich von Kommunikationsnetzen gedacht ist. Er modelliert die vier unteren Schichten des OSI-Modells und unterstützt dabei auf jeder Schicht mehrere verschiedene Protokolle, die frei kombinierbar sind. Drahtlose und leitungsgebundene Netze werden dabei gleichermaßen unterstützt, es stehen mehrere MAC-Mechanismen und zahlreiche Routingverfahren zur Verfügung, sowie auch Fehlermodelle und Methoden zur Auswertung der Simulationen [80].

Der ns-2 ist modular aufgebaut und kann daher problemlos erweitert werden. Der Kern des Simulators ist in C++ implementiert, als Benutzerschnittstelle dient ein OTcl-Interpreter. Die Verwendung zweier verschiedener Programmiersprachen dient der Erfüllung von zwei unterschiedlichen Aufgaben. Detaillierte Simulationen mehrerer Schichten erfordern die Verarbeitung großer Datenmengen in kurzer Zeit, dafür ist C++ gut geeignet. Wenn jedoch für mehrere aufeinanderfolgende Simulationsdurchläufe jeweils nur einzelne Parameter geändert werden sollen, ist die Verwendung einer Skriptsprache zweckmäßiger, damit nicht jedesmal das ganze Programm neu kompiliert werden muss. Deshalb wird die Übergabe der Simulationseinstellungen mit Hilfe von OTcL erledigt. Letzteres ist zwar in der Ausführung langsamer, kann aber einfacher und schneller geändert werden. Die beiden Programmteile sind über spezielle Methoden miteinander verbunden, mit deren Hilfe Objekte in beiden Sprachen erzeugt und verwendet werden können.

Jede OSI-Schicht bzw. jedes Protokoll ist im ns-2 als eigene Klasse implementiert. Das Zusammenspiel der verschiedenen Schichten ist festgelegt, aber es bleibt dem Anwender überlassen, welche Protokolle jeweils verwendet werden. Ebenso ist es möglich, dem Simulator neue Protokolle hinzuzufügen oder bestehenden Programmcode zu erweitern. Im Folgenden werden einige solcher Erweiterungen vorgestellt.

Vom ns-2 existieren zahlreiche unterschiedliche Versionen. In dieser Arbeit wurde der ns-2.29 [81] verwendet.

B.2 Erweiterungen

B.2.1 IEEE 802.11e/n

Das an der TU Berlin entwickelte Simulationsmodell zur Darstellung von 802.11e [79] ist modular, adaptiv und einfach erweiterbar. Der Code basiert auf dem im ns-2 enthaltenen IEEE 802.11 und erweitert diesen. Dabei wird, wie auch schon im ursprünglichen Modell, nur der wettbewerbsbasierte Medienzugriff betrachtet. Dieser wird auf mehrere Warteschlangen mit entsprechenden Timern umgestellt. Neu sind dabei auch die sogenannten CFBs (Contention Free Bursts) oder auch TXOPs (Transmission Opportunities), welche einer Station erlauben, bei einem Kanalzugriff gleich mehrere Pakete direkt nacheinander zu senden. Zusätzlich wurden einige Fehler in der ursprünglichen Implementierung korrigiert.

Im Rahmen dieser Arbeit wurden noch weitere Probleme des ursprünglichen Codes repariert, insbesondere in Bezug auf die Verwendung von RTS/CTS (Ready-to-Send / Clear-to-Send).

Im Zuge dieser Arbeit wurde außerdem eine Erweiterung des ns-2 zur Simulation von IEEE 802.11n entwickelt. Dabei wurde insbesondere auf die höheren Datenraten Wert gelegt, die aufgrund der Verwendung von neuen Modulationsverfahren erreicht werden können. Des Weiteren wurde Datenaggregation (Frame Aggregation, A-MPDU und A-MSDU) sowie die Verwendung des Block-ACK, welches ermöglicht, mehrere Quittungen in einem Paket zu versenden, implementiert, aber nicht näher untersucht. Beamforming, wie im Standard IEEE 802.11n auch beschrieben, wird in Anhang B.2.4 ausführlicher beschrieben.

B.2.2 eDCC/PADCC

Für eDCC und PADCC muss vor dem Senden eines Pakets die Sendewahrscheinlichkeit PT berechnet werden. Dazu ist es notwendig, die Anzahl der Wiederholungen des Pakets zu kennen, den Initialwert des Backoff-Counters sowie die Anzahl fremder Übertragungen, die während des eigenen Backoffs starten. Diese Werte müssen für jede Station bzw. jede Warteschlange, die sich im Backoff befindet, bestimmt werden.

Zu Beginn eines Backoffs wird der Initialwert des Backoff-Counters zufällig gezogen. Dieser Wert kann für die spätere Verwendung zwischengespeichert werden. Die Anzahl der Wiederholungen eines Pakets ist innerhalb der MAC-Schicht bekannt, da der ns-2 bei jedem Paket darauf achten muss, dass die maximale Zahl an Wiederholungen (retry limit) nicht überschritten wird. Wenn eine fremde Übertragung stattfindet, während eine Station sich im Backoff befindet, wird das Dekrementieren des Backoff-Counters unterbrochen. Wenn dieses Ereignis eintritt, wird dies von einer neu eingeführten Zählvariable registriert, die zu Beginn der Backoffprozedur auf 0 gesetzt wird.

Anhand dieser Werte kann mit Formel 2.3 und 2.4 die Übertragungswahrscheinlichkeit für eDCC berechnet werden. Bei Einsatz von PADCC wird PT entsprechend nach den Formeln 3.1–3.5 bestimmt.

Die Verwendung von eDCC bzw. PADCC kann über das Simulationsskript aktiviert werden.

B.2.3 City Propagation

Das *City-Propagation*-Modul (City-Prop) [23] kombiniert ein Mobilitätsmodell mit einem Ausbreitungsmodell zur Modellierung urbaner Umgebungen. Für die Simulation von Büroumgebungen wurde im Rahmen dieser Arbeit der ursprüngliche Code angepasst.

Die im ns-2 enthaltenen Ausbreitungsmodelle basieren auf der Annahme, dass der Pfadverlust proportional zur Entfernung zwischen zwei Knoten ist. Dies ist jedoch nicht korrekt, wenn sich beispielsweise eine Wand zwischen Sender und Empfänger befindet. Eine Station, die weiter entfernt ist, aber eine Sichtverbindung zum Sender hat, kann dann unter Umständen eine bessere Empfangsqualität erzielen. In City-Prop wird dies mit berücksichtigt.

Das hier verwendete Ausbreitungsmodell ist ein erweitertes Freiraummodell (siehe auch Kap. 3.2). Der Pfadverlust a im freien Raum hängt von der Entfernung d zwischen Sender und Empfänger ab [54]:

$$a = \frac{P_S}{P_E} = \frac{(4\pi)^2 \cdot d^\gamma \cdot L}{G_S \cdot G_E \cdot \lambda^2} \tag{B.1}$$

P_S und P_E sind dabei die Sende- bzw. Empfangsleistung. $G_{S/E}$ sind der Sender- bzw. Empfängergewinn und L ist der Verlust des Systems; diese drei Werte werden üblicherweise gleich 1 gesetzt. λ ist die Wellenlänge, die sich aus der Frequenz $f = \frac{c}{\lambda}$ berechnen lässt. Der Pfadverlustkoeffizient γ ist 2 im freien Raum und wird auf 4 gesetzt, falls keine Sichtverbindung besteht. Für jede Mauer, die sich zwischen Sender und Empfänger befindet, wird eine Dämpfung von 15 dB angenommen.

City-Prop berechnet für jedes Sender-Empfänger-Paar den Pfadverlust anhand beider Methoden (direkte Verbindung unter Berücksichtigung dazwischenliegender Wände, sowie indirekter Empfang des Signals über Mehrwegeausbreitung und Reflexionen mit $\gamma = 4$). Der kleinere von beiden Werten wird dann in der Simulation verwendet.

B.2.4 Beamforming

Bei Verwendung von omnidirektionalen Antennen ist der Antennengewinn (G_S bzw. G_E) in Formel B.1 gleich 1. Beamforming hingegen bewirkt, dass der Gewinn nicht in alle Richtungen konstant ist, sondern von der Abstrahlungsrichtung abhängt.

Für die Umsetzung im ns-2 wurde das bestehende Antennenmodell erweitert, um eine Berücksichtigung des jeweiligen Antennengewinns zu ermöglichen. Dieser wird aus einer vorher berechneten Tabelle abgelesen, die für jede mögliche Ausrichtung der Senderichtung die Gewinne in alle Richtungen darstellt. Die Granularität ist $1°$. Für die Berechnung des Pfadverlustes zwischen zwei Stationen wird dann der Antennengewinn in der jeweiligen Abstrahlungsrichtung verwendet.

Um die Antenne auszurichten, ist eine Funktion innerhalb des MAC-Protokolls notwendig. Hier wurde nur *Maximize Gain Beamforming* implementiert, also die Ausrichtung der Hauptabstrahlungsrichtung des Senders auf den Empfänger. Vor dem Senden eines Pakets gibt die MAC-Schicht den Befehl zum Ausrichten der Antenne. Dies kann vor jeder Übertragung geschehen, oder einmal pro Verkehrsstrom. Es ist auch möglich, die Antennen aller Knoten (zufällig oder gezielt) auszurichten und dann für die Dauer der Simulation in dieser Richtung zu belassen. Die Verwendung von Beamforming sowie die Vorschrift zur Ausrichtung können über das Simulationsskript eingestellt werden.

B.2.5 Zugangskontrolle

Die Zugangskontrolle wird über das Simulationsskript gesteuert. Im Gegensatz zu den anderen Mechanismen werden hier nicht nur die Parameter übergeben, sondern es findet während der gesamten Simulationszeit eine Interaktion zwischen C++ und Tcl-Code statt. Das ist notwendig, da das Simulationsskript die einzelnen Verkehrsströme startet.

Jeder neue Verkehrsstrom bekommt zunächst den Status *NEU*. Wenn die Antwort auf ein Testpaket erhalten wurde, wird der Zustand auf *ZUGELASSEN* oder *ABGELEHNT* geändert, abhängig vom Inhalt des Antwortpakets. Ein abgelehnter Verkehrsstrom existiert zwar nominell weiter, sendet aber keine Daten.

Ob in einer Simulation Zugangskontrolle verwendet wird oder nicht, sowie die Einstellung der einzelnen Parameter, wird über das Simulationsskript festgelegt.

Anhang C

MAC-Schicht-Simulator Simbo

C.1 Singlehop-Szenario

Der MAC-Schicht-Simulator Simbo modelliert nur den Medienzugriff. Da sich im Singlehop-Szenario alle Stationen in Sendereichweite befinden, haben alle die gleiche Sicht auf den Kanal und merken demnach gleichzeitig, wenn der Kanal frei wird. Das hat zwei Konsequenzen, die die Modellierung vereinfachen:

1. Während eine Übertragung stattfindet, müssen alle anderen Stationen warten, in dieser Zeit passiert also nichts.

2. Da alle Stationen immer Pakete zu senden haben und gleichzeitig merken, dass der Kanal frei ist, sind die Backoffs der einzelnen Stationen auf ganze Zeitschlitze synchronisiert (siehe Abb. C.1).

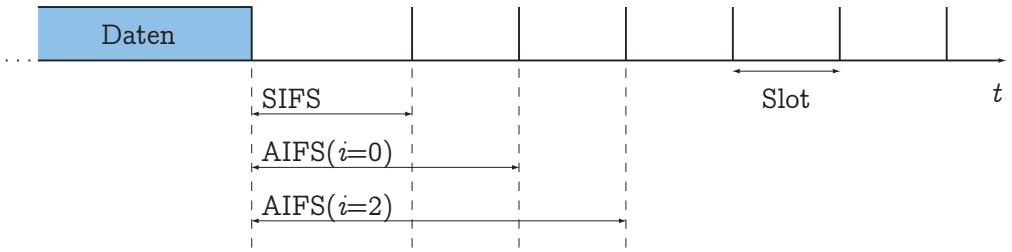


Abbildung C.1: Kanalzugriff unter CSMA/CA

Jede der m Stationen umfasst vier Verkehrsklassen, von denen wiederum jede zwei Timer unterhält, die den Backoff-Status widerspiegeln. Der AIFS-Timer hat in Abhängigkeit der Verkehrsklasse eine feste Länge, während der Backoff-Counter b zufällig aus $\{0, 1, \ldots, CW_j(i) - 1\}$ gezogen wird. Wenn der Kanal frei wird, wird zunächst der AIFS dekrementiert und sobald dieser 0 erreicht, der Backoff-Counter. Wird der Backoff unterbrochen, weil eine andere Station sendet, wird der Backoff-Counter eingefroren und der AIFS auf den ursprünglichen Wert zurückgesetzt. Nach dem Ende der nächsten Übertragung wird dann wieder zunächst der AIFS bis 0 heruntergezählt und anschließend mit dem Dekrementieren des Backoff-Counters fortgefahren.

Der Simulator ist ereignisgesteuert, die Abläufe passieren also nicht in Echtzeit, sondern nach der Verarbeitung eines Ereignisses wird zum nächsten Ereignis gesprungen. Die möglichen Ereignisse sind dabei:

1. Eine Station hat ihren Backoff beendet.
2. Mehrere Stationen haben ihren Backoff beendet.

Zu Beginn wird also überprüft, welche Station als erstes ihren Backoff beenden wird, bzw. ob es mehrere Stationen gleichzeitig sind. Daraufhin werden die Backoff-Counter aller Stationen um diesen Wert dekrementiert und der AIFS jeweils zurückgesetzt. Im Fall (1), dass nur eine Station sendet, ist die Übertragung erfolgreich. Dies wird für die Auswertung der Simulation vermerkt. Anschließend wählt die Station einen neuen Backoff-Counter, der Backoff-Level wird dabei wieder auf den ursprünglichen Wert zurückgesetzt. Im Fall (2) findet eine Kollision statt. Dies wird auch für die Auswertung vermerkt, anschließend erhöhen die beteiligen Stationen ihren Backoff-Level und ziehen einen neuen Backoff-Counter.

Diese Schritte werden ca. 10.000.000 mal wiederholt, um die gewünschte Genauigkeit zu erzielen. Im Anschluss werden die Ergebnisse (Durchsatz, Verzögerung, Paketverlustrate, Kollisionsrate der Pakete) ausgewertet.

C.2 Multihop-Szenario

Da sich nicht mehr alle Stationen gegenseitig hören können, haben sie eine unterschiedliche Sicht auf den Kanal und sind dadurch nicht mehr synchron. Deshalb muss die Einteilung in Zeitschritte, wie sie für den Singlehop-Fall eingesetzt wurde, erweitert werden, um alle möglichen Ereignisse abbilden zu können.

Jede Station unterhält einen Timer, der die Zeit bis zum nächsten Ereignis festhält (z.B. noch 20 µs bis der Backoff-Counter dekrementiert wird, oder noch 300 µs bis das Senden des Pakets beendet ist). Wenn eine Aktion abgeschlossen ist, wird bei allen Stationen der Timer dekrementiert. Sobald ein Timer (oder auch mehrere gleichzeitig) „0“ erreicht, wird die entsprechende nächste Aktion bei dieser Station durchgeführt. Am Ende der Simulationszeit werden analog zum Singlehop-Szenario die Simulationsparameter ausgewertet, um Durchsatz, Verzögerung und Paketverlustrate zu erhalten.

Da der MAC-Schicht-Durchsatz betrachtet wird, wird immer nur ein Hop ausgewertet. Die Ergebnisse sind daher unabhängig vom Routing, und Wissen über den Routingalgorithmus ist nicht erforderlich. Für die Auswertung des MAC-Schicht-Durchsatzes werden eigene Pakete und weitergeleitete Pakete gleich behandelt. Der Empfänger eines Pakets ist ein zufällig gewählter Nachbar der jeweiligen Station. Dazu ist es, im Gegensatz zum Singlehop-Szenario, notwendig, relative Positionen der Knoten zueinander zu definieren. Jede Station erhält dazu eine Liste, in der ihre

Nachbarn sowie alle Knoten in ihrer Interferenz- und CS-Reichweite notiert sind. Da von statischen Szenarien ausgegangen wird, ist diese Liste über die Dauer der Simulation konstant.

Anhang D

Analytisches Markovmodell

D.1 Zustandsübergänge

Die Wahrscheinlichkeiten für die einzelnen Zustandsübergänge des in Kap. 4 entwickelten Markovmodells lassen sich unter Verwendung der im Folgenden beschriebenen Parameter bestimmen. Aus den Übergangswahrscheinlichkeiten können die stationären Wahrscheinlichkeiten des Modells berechnet werden.

D.1.1 Parameter

- $p_i^{\text{tr}}(t)$: Die Wahrscheinlichkeit dafür, dass sich eine bestimmte AC_i in einem Zustand befindet, in dem sie im nächsten Schritt eine Übertragung initialisieren kann.
- $PT_{i,j}(t)$: Die Wahrscheinlichkeit dafür, dass eine mögliche Übertragung einer AC_i im Backoff-Level j tatsächlich initialisiert wird (bei Einsatz von PADCC).
- $\tau_i(t)$: Die Wahrscheinlichkeit dafür, dass eine bestimmte AC_i im nächsten Schritt eine Übertragung initialisieren wird ($\tau_i(t) = E_j\left[p_{i,j}^{\text{tr}}(t)\right] \cdot PT_{i,j}(t)$).
- $p_i(t)$: Kollisionswahrscheinlichkeit, welche in die folgenden Unterwahrscheinlichkeiten aufgesplittet wird:
  - $p^{\text{me}}(t)$: Die Wahrscheinlichkeit dafür, dass mindestens eine andere Station eine Übertragung initialisiert.
  - $p^{\text{ge}}(t)$: Die Wahrscheinlichkeit dafür, dass genau eine andere Station eine Übertragung initialisiert.
  - $p_i^{\text{en}}(t)$: Die Wahrscheinlichkeit dafür, dass keine andere $\text{AC}_{i'}$ der eigenen Station eine Übertragung initialisiert.
  - $p_i^{\text{kh}}(t)$: Die Wahrscheinlichkeit dafür, dass keine $\text{AC}_{i'}$ höherer Priorität der eigenen Station eine Übertragung initialisiert.

D.1.2 Zustandsübergänge

Um die Übersichtlichkeit zu verbessern, werden die Abhängigkeiten von t im Folgenden nicht mit notiert:

1. Herunterzählen des AIFS, $s > 1$:

$$(j, b, s, t) \rightarrow \begin{cases} (j, b, s-1, t+1) & (1-p^{\text{me}}) \cdot p_i^{\text{en}} \\ (j, b, -1, 0) & (p^{\text{me}} - p^{\text{ge}}) \cdot p_i^{\text{en}} \\ (j, b, -2, 0) & (p^{\text{ge}} \cdot p_i^{\text{en}}) + ((1-p^{\text{me}}) \cdot (1-p_i^{\text{en}})) \\ (j, b, -3, 0) & p^{\text{me}} \cdot (1-p_i^{\text{en}}) \end{cases} \tag{D.1}$$

2. Verlassen eines Kollisionszustandes , $s < 0$:

$$(j, b, s, t) \rightarrow (j, b, A_i, 0) \tag{D.2}$$

3. Verlassen des AIFS und dekrementieren, $s = 1$, $b > 0$:

$$(j, b, 1, t) \rightarrow \begin{cases} (j, b-1, 0, t+1) & (1-p^{\text{me}}) \cdot p_i^{\text{en}} \\ (j, b, -1, 0) & (p^{\text{me}} - p^{\text{ge}}) \cdot p_i^{\text{en}} \\ (j, b, -2, 0) & (p^{\text{ge}} \cdot p_i^{\text{en}}) + ((1-p^{\text{me}}) \cdot (1-p_i^{\text{en}})) \\ (j, b, -3, 0) & p^{\text{me}} \cdot (1-p_i^{\text{en}}) \end{cases} \tag{D.3}$$

4. Dekrementieren des Backoff, $s = 0$, $b > 0$:

$$(j, b, 0, t) \rightarrow \begin{cases} (j, b-1, 0, t+1) & (1-p^{\text{me}}) \cdot p_i^{\text{en}} \\ (j, b, -1, 0) & (p^{\text{me}} - p^{\text{ge}}) \cdot p_i^{\text{en}} \\ (j, b, -2, 0) & (p^{\text{ge}} \cdot p_i^{\text{en}}) + ((1-p^{\text{me}}) \cdot (1-p_i^{\text{en}})) \\ (j, b, -3, 0) & p^{\text{me}} \cdot (1-p_i^{\text{en}}) \end{cases} \tag{D.4}$$

Beim Übergang in einen neuen Backoff, wegen Zurückstellens der Übertragung, Kollision oder Initialisierung eines neuen Datenpakets, muss beachtet werden, dass alle möglichen Werte von b im nächsten Backoff-Level gleichverteilt gezogen werden. Dabei entspricht b_{init} einer zufällig gezogenen Zahl aus $\{0, 1, \ldots, CW_j(i) - 1\}$, wobei j der Backoff-Level ist, in den übergegangen wird.

5. Backoffinitialisierung nach erfolgreicher Übertragung, $b = -2$:

$$(j, -2, 0, t) \rightarrow (-1, b_{\text{init}}, A_i, 0) \tag{D.5}$$

6. Backoffinitialisierung nach einem Paketverlust, $b = -1$ und $j = j_{\max}(i)$:

$$(j_{\max}(i), -1, 0, 0) \rightarrow (-1, b_{\text{init}}, A_i, 0) \tag{D.6}$$

7. Backoffinitialisierung nach eigener Kollision, $b = -1$ und $j < j_{\max}(i)$:

$$(j, -1, 0, 0) \rightarrow (j+1, b_{\text{init}}, A_i, 0) \tag{D.7}$$

8. Sendeentscheidung treffen, $b = 0$, $s \in \{0, 1\}$, $j < j_{\max}(i)$:
$(j, 0, 0 \text{ bzw. } 1, t) \rightarrow$

$$\begin{cases} (j, -2, 0, 0) & PT_i \cdot (1 - p^{\text{me}}) \cdot p_i^{\text{kh}} \\ (j, -1, 0, 0) & PT_i \cdot ((p^{\text{me}} \cdot p_i^{\text{kh}}) + (1 - p_i^{\text{kh}})) \\ (j+1, b_{\text{init}}, 0, t+1) & \dfrac{(1 - PT_i) \cdot (1 - p^{\text{me}}) \cdot p_i^{\text{en}}}{CW_{j+1}(i)} \\ (j+1, b_{\text{init}}, -1, 0) & \dfrac{(1 - PT_i) \cdot (p^{\text{me}} - p^{\text{ge}}) \cdot p_i^{\text{en}}}{CW_{j+1}(i)} \\ (j+1, b_{\text{init}}, -2, 0) & \dfrac{(1 - PT_i) \cdot (p^{\text{ge}} \cdot p_i^{\text{en}}) + ((1 - p^{\text{me}}) \cdot (1 - p_i^{\text{en}}))}{CW_{j+1}(i))} \\ (j+1, b_{\text{init}}, -3, 0) & \dfrac{(1 - PT_i) \cdot p^{\text{me}} \cdot (1 - p_i^{\text{en}})}{CW_{j+1}(i)} \end{cases} \tag{D.8}$$

9. Wenn sich die AC_i im letzten Backoff-Level befindet, ergibt sich bei der Sendeentscheidung eine Sondersituation. In diesem Fall entspricht ein nicht gesendetes Paket einem Paketverlust, und der Post-Backoff wird gestartet, bevor das nächste Paket gesendet wird. $b = 0$, $s \in \{0, 1\}$, $j = j_{\max}(i)$:

$(j_{\max}(i), 0, 0 \text{ bzw. } 1, t) \rightarrow$

$$\begin{cases} (j_{\max}(i), -2, 0, 0) & PT_i \cdot (1 - p^{\text{me}}) \cdot p_i^{\text{kh}} \\ (j_{\max}(i), -1, 0, 0) & PT_i \cdot ((p^{\text{me}} \cdot p_i^{\text{kh}}) + (1 - p_i^{\text{kh}})) \\ (-1, b_{\text{init}}, 0, t+1) & \dfrac{(1 - PT_i) \cdot (1 - p^{\text{me}}) \cdot p_i^{\text{en}}}{CW_0(i) + 1} \\ (-1, b_{\text{init}}, -1, 0) & \dfrac{(1 - PT_i) \cdot (p^{\text{me}} - p^{\text{ge}}) \cdot p_i^{\text{en}}}{CW_0(i) + 1} \\ (-1, b_{\text{init}}, -2, 0) & \dfrac{(1 - PT_i) \cdot (p^{\text{ge}} \cdot p_i^{\text{en}}) + ((1 - p^{\text{me}}) \cdot (1 - p_i^{\text{en}}))}{CW_0(i) + 1} \\ (-1, b_{\text{init}}, -3, 0) & \dfrac{(1 - PT_{i,j_{\max}}) \cdot p^{\text{me}} \cdot (1 - p_i^{\text{en}})}{CW_0(i) + 1} \end{cases} \tag{D.9}$$

D.2 Parameterberechnung

- Die Wahrscheinlichkeit dafür, dass mindestens eine fremde Station im nächsten Zeitschlitz sendet

$$p^{\text{me}} = 1 - (1 - \tau)^{n-1} \tag{D.10}$$

- Die Wahrscheinlichkeit dafür, dass genau eine fremde Station im nächsten Zeitschlitz sendet

$$p^{\text{ge}} = \tau \cdot (1-\tau)^{n-2} \cdot (n-1) \tag{D.11}$$

- Die Wahrscheinlichkeit dafür, dass von der eigenen Station keine (andere) $AC_{i'}$ sendet

$$p_i^{\text{en}} = \prod_{i' \neq i} (1 - \tau_{i'}) \tag{D.12}$$

Für $b = 0$ ergibt sich noch der Sonderfall, dass die eigene Station einen Sendeversuch der betrachteten AC_i nur dann vereitelt, wenn eine $AC_{i'}$ höherer Priorität sendet und die AC_i somit virtuell kollidiert. Für diesen Fall ergibt sich die folgende Wahrscheinlichkeit:

- Die Wahrscheinlichkeit dafür, dass keine höhere $AC_{i'}$ der eigenen Station sendet

$$p_i^{\text{kh}} = \prod_{i' > i} (1 - \tau_{i'}) \tag{D.13}$$

- n ist die Anzahl der Stationen, die im betrachteten Zeitschlitz die Möglichkeit haben, auf den Kanal zuzugreifen. Sie hängt von den zuvor eingetretenen Ereignissen ab. Nach einer erfolgreichen Übertragung sind alle Stationen sendebereit, nach einer Kollision sind jedoch die beteiligten Stationen länger gesperrt. Ist der Kanal also zu einer beliebigen Zeit mit $t = T$ frei, die Anzahl an sendefähigen Stationen betrage n_0 und es tritt im nächsten Schritt eine Übertragung oder Kollision auf, dann beträgt der Erwartungswert für die Zahl der nach der Übertragung sendefähigen Stationen N_1:

$$E_t[N_1 \mid N_0 = n_0] = \frac{p_e(t)}{p_b(t)} \cdot m + \sum_{l=2}^{n_0} \binom{n_0}{l} \cdot \frac{\tau(t)^l \cdot (1-\tau(t))^{n_0-l}}{p_b(t)} \cdot (m-l) \tag{D.14}$$

- Der Erwartungswert von T_v (siehe Kap. 4.2) ergibt sich wie folgt:

$$\begin{aligned} E[T_v] &= E_t\left[t_{Daten} + t_{AIFS}(i=0) \cdot t_{Slot} + T_f + \frac{p_e}{p_b} \cdot (t_{Daten} + t_{SIFS} + t_{ACK}) + \frac{p_k}{p_b} \cdot t_{Daten}\right] \\ &= 2 \cdot t_{Daten} + t_{AIFS}(i=0) \cdot t_{Slot} + E_t\left[n_{frei}\right] \cdot t_{Slot} + E_t\left[\frac{p_e}{p_b}\right] \cdot (t_{SIFS} + t_{ACK}) \end{aligned} \tag{D.15}$$

- Berechnung der Verzögerungszeit D_i:

$$D_i^l = \left(D_i^k \cdot \sum_{j=0}^{j_{\max}} E[PT_i(j)]\right) + \left(\sum_{j=-1}^{j_{\max}} \frac{CW_j(i)}{2} \cdot E_i\left[D_i^d\right]\right), \tag{D.16}$$

wobei D_i^k die Dauer einer Kollision bezeichnet. Die benötigten Dichten sind bereits bekannt. Für $E_i[D_i^d]$ ergibt sich dementsprechend:

$$E_i[D_i^d] = \frac{\Delta_i - k_1 \cdot D_i^k}{k_2}, \tag{D.17}$$

wobei k_1 und k_2 berechenbare Erwartungswerte sind. $E_i[D_i^d]$ kann in die Formel 4.22 eingesetzt und so D_i berechnet werden.

D.3 Iterative numerische Lösung

Das Markovmodell lässt sich anhand einiger Gleichungen beschreiben. Eine direkte Lösung dieser Gleichungen ist nicht möglich, da alle Parameter voneinander abhängen. Deshalb wird ein iteratives Lösungsverfahren eingesetzt.

D.3.1 Definition von Hilfsvariablen

Zunächst sei

$$\Theta_i(J+1, t+1) = \frac{\tau_i(t \mid j = J)}{PT_i(j = J, t \mid j = J)} \tag{D.18}$$

eine Matrix der Größe $(j_{\max}(i)+1) \times 12$, welche für gegebenes t und j die Wahrscheinlichkeit dafür angibt, dass im nächsten Schritt eine Übertragung gestartet werden kann. Die Zeilen der Matrix entsprechen dabei den einzelnen Backoff-Leveln, die Spalten dem Wert von t.

Um die Verwendung von PADCC zu beschreiben, sei

$$\Psi_i(J+1, t+1) = PT_i(t \mid j = J) \tag{D.19}$$

ebenfalls eine Matrix der Größe $(j_{\max}(i)+1) \times 12$, welche die Werte von PT angibt. Falls PADCC nicht verwendet wird, haben alle Einträge der Matrix den Wert 1.

Des Weiteren sei

$$\vartheta(k) = P(t = k-1), k \in \{1, \ldots, 12\} \tag{D.20}$$

ein Spaltenvektor der Länge 12, der die Dichte der Werte, die t annehmen kann, bezeichnet. Dann ist

$$\vartheta_i(t) = \vartheta(t \mid \tau_i(t) > 0) \tag{D.21}$$

die Dichte von t bedingt auf die Werte, in denen die AC_i eine Übertragung starten kann. Das bedeutet, für die Verkehrsklasse mit höchster Priorität gilt $\vartheta_i = \vartheta$, für die niedrigeren Prioritäten beginnt der Vektor mit Einträgen vom Wert 0. Analog dazu sei

$$\beta_I(l) = P(j = l - 1 \mid i = I), l \in \{1, \ldots, j_{\max} + 1\} \tag{D.22}$$

ein Spaltenvektor der Länge $j_{\max}+1$, der die Dichte von j angibt, also die Wahrscheinlichkeit dafür, dass für eine bestimmte AC_i in einem beliebigen Zeitschlitz j den Wert l annimmt.

D.3.2 Iterative Lösung

Die iterative Lösung setzt sich dann aus den folgenden Schritten zusammen:

1. Aus Ψ_i und β_i ergeben sich die $\tau(t)$.
2. Sind alle $\tau_i(t)$, Ψ_i und n bekannt, so lässt sich daraus $p_b(t)$ berechnen.
3. Sind $p_b(t)$ und ϑ bekannt, so lässt sich n berechnen.
4. Ist $p_b(t)$ bekannt, so lässt sich ϑ berechnen.
5. Sind $p_b(t)$ und ϑ bekannt, so lässt sich Ψ_i berechnen.
6. Sind $\tau_{i'}(t)$, $i' > i$, p_b, ϑ und Ψ_i bekannt, so lässt sich β_i berechnen.

D.3.3 Berechnung der Parameter

Die einzelnen Parameter hängen dabei wie folgt zusammen:

- Θ_i hängt nur von Fenstergröße und AIFS ab und lässt sich daher einfach angeben:

$$\Theta_i(J+1, t+1) = \begin{cases} 1 & \text{für} \quad t - A_i \geq CW_j(i) + 1 \\ \frac{2}{CW_j(i) + A_i - t + 2} & \text{für} \quad 1 \leq t - A_i < CW_j(i) + 1 \\ 0 & \text{für} \quad t - A_i < 1 \end{cases} \tag{D.23}$$

- $\tau_i(t)$ lässt sich aus Θ_i, Ψ_i und β_i bestimmen ($A \otimes B$ bezeichnet hier die elementweise Multiplikation der Matrizen):

$$\tau_i(t) = (\Theta_i \otimes \Psi_i)^T \cdot \beta_i \tag{D.24}$$

- Daraus lassen sich die einzelnen τ_i berechnen, wenn ϑ bekannt ist:

$$E_t[\tau_i] = \langle \tau_i(t), \vartheta \rangle \tag{D.25}$$

- Mit Hilfe von τ_i folgt τ aus Formel 4.4.
- Daraus lassen sich gemäß Formel 4.8 und D.14 p_b, p_e, p_k sowie n bestimmen.
- Für $k, l > 0$ gilt:
$$\vartheta(k) = \vartheta(k-1) \cdot (1 - p_b(k-1)) \tag{D.26}$$
und
$$\beta_i(l) = \beta_i(l-1) \cdot \left(1 - \left\langle \left(\Psi_i(l-1,:) \cdot (1-\tau)^n \cdot \prod_{i'>i}(1-\tau_{i'})\right)^T, \vartheta_i \right\rangle\right) \tag{D.27}$$
Da es sich hierbei um Dichten handelt, lassen sich ϑ und β_i durch Normierung ermitteln. Für die Bestimmung von β_i ist außerdem noch Ψ_i notwendig.
- Ψ_i berechnet sich zu
$$\Psi_i(j+1, t+1) = PT_j(t) \tag{D.28}$$
PT wiederum ergibt sich aus Formel 2.4 bzw. 3.4 und 3.5. PT hängt von SU ab, zu dessen Berechnung ϑ notwendig ist.

D.3.4 Initialisierung der Variablen

Θ_i ist durch die Startparameter schon vollständig definiert.

Alle Einträge von Ψ_i können mit dem Wert 1 initialisiert werden, da dies dem Fall entspricht, dass kein PADCC verwendet wird, und somit zu einer Lösung führen muss.

Über n ist bekannt, dass $0 \leq n \leq m$. Deshalb kann $n = a \cdot m, a \in]0, 1[$ gewählt werden, mit beispielsweise $a = 0{,}9$.

Aufgrund der Verteilung von j gilt $\beta(l+1) \leq \beta(l)$. Unter der Annahme, dass β sich mit wachsendem m immer mehr einer Gleichverteilung annähert, kann folgende Näherung verwendet werden: $\beta_i(l+1) = \beta_i(l) \cdot (1 - \frac{1}{m})$

Aus diesen Startwerten können alle anderen Parameter wie im vorigen Abschnitt beschrieben berechnet werden.

Fachbegriffe

Access Category	Verkehrsklasse
Access Point	Access Point
Acknowledgement	Quittung
Ad hoc network	Ad-hoc-Netz
Backoff	Backoff
Best Effort Traffic	Best-Effort-Verkehr
Connection Admission Control	Zugangskontrolle
Capture Effect	Capture-Effekt
Carrier Sensing	Carrier Sensing
Cluster	Cluster
Contention Window	Zeitfenster bzw. Fenstergröße
Control Packet	Signalisierungsnachricht
Free Space Propagation Model	Freiraumausbreitungsmodell
Gateway	Gateway
Header	Header
Hidden node, hidden station	Hidden Node
Hop	Hop
Interframe Space	Interframe Space
Internet Protocol	Internetprotokoll
Line of Sight	Sichtverbindung

Link Break	Unterbrechung der Funkverbindung
Medium Access Control	Medienzugriffssteuerung
Overhead	Overhead
Probing Packet	Testpaket
Quality of Service	Dienstgüte
Rate Control	Regelung der Datenrate
Routing	Routing, Verkehrslenkung
Signal to Interference and Noise Ratio	Signal-zu-Interferenz-und-Rauschabstand
Slot, Time Slot	Zeitschlitz
stateful	zustandsbehaftet
stateless	zustandslos
Smart Antenna	Intelligente Antenne
Timer	Timer
Traffic Differentiation	Verkehrskategorisierung, Priorisierung, Einteilung in Verkehrsklassen unterschiedlicher Priorität
Wireless Mesh Network	Vermaschtes drahtloses Netz, Mesh-Netz

Abkürzungen

AC	Access Category
ACK	Acknowledgement
AIFS	Arbitrary Interframe Space
AODV	Ad hoc On-demand Distance Vector Routing (Routingmechanismus)
AP	Access Point
BS	Basisstation
CAC	Admission Control / Connection Admission Control
CH	Clusterhead
CITR	Channel Idle Time Ratio (Anteil der Zeit, in der der Kanal frei ist)
CS	Carrier Sensing (Abhören des Kanals)
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance (Medienzugriffsverfahren)
CW	Contention Window (Fenstergröße)
DAC	DARMA Admission Control (Zugangskontrollmechanismus)
DARMA	Distributed Adaptive Resource Management Architecture
DCA	Distributed Clustering Algorithm
DCC	Distributed Contention Control (Medienzugriffsverfahren)
DCF	Distributed Contention Function (Medienzugriffssteuerung unter IEEE 802.11)
DIFS	DCF Interframe Space
DSDV	Destination Sequenced Distance Vector Routing (Routingmechanismus)

ECN	Explicit Congestion Notification (Teil von bestimmten CAC-Verfahren)
EDCA	Enhanced Distributed Channel Access (Medienzugriffssteuerung unter IEEE 802.11e)
eDCC	EDCA Distributed Contention Control (Erweiterung von DCC)
EY-NPMA	Elimination Yield Non Preemptive Multiple Access (Medienzugriffsverfahren)
GPRS	General Packet Radio Service (Dienst zur Datenübertragung in GSM-Netzen)
GPS	Global Positioning System
GSM	Global System for Mobile Communications (Mobilfunkstandard)
GW	Gateway
IFS	Interframe Space
IP	Internetprotokoll
LTE	Long Term Evolution (Mobilfunkstandard)
MAC	Medium Access Control (Medienzugriffssteuerung)
MIB	Management Information Base (Managementdatenbank)
ns-2	Network Simulator, Version 2 (Programm zur Simulation von Kommunikationsnetzen)
OSI	Open Systems Interconnection (OSI-Referenzmodell)
PADCC	Priority-Aware Distributed Contention Control (Erweiterung von DCC)
QoS	Quality of Service (Dienstgüte)
RTS/CTS	Ready-to-Send / Clear-to-Send (Optionaler Zusatz zu CSMA/CA)
SIFS	Short Interframe Space
SINR	Signal-zu-Interferenz-und-Rauschabstand (Signal to Interference and Noise Ratio)
SNMP	Simple Network Management Protocol (Managementprotokoll)

SWAN	Service Differentiation for Stateless Wireless Ad hoc Networks (CAC-Mechanismus / QoS-Architektur)
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network (Mesh-Netz, vermaschtes drahtloses Netz)

Formelzeichen

a	Pfadverlust, Dämpfung
A_i	Unterschied zwischen der Dauer des AIFS der betrachteten Verkehrsklasse i und dem kürzesten AIFS
c	Lichtgeschwindigkeit
CW	Contention Window (Fenstergröße)
CW_j	Fenstergröße in Abhängigkeit des Backoff-Levels j
$CW_{\max}$	Maximale Fenstergröße
$CW_{\max}(i)$	Maximale Fenstergröße in Abhängigkeit der Priorität i
$CW_{\min}$	Minimale Fenstergröße
$CW_{\min}(i)$	Minimale Fenstergröße in Abhängigkeit der Priorität i
d	Abstand
D_i	Durchschnittliche Verzögerung eines Paketes der Verkehrsklasse i
f	Frequenz
G_E	Empfängergewinn
G_S	Sendergewinn
i	Priorität
L	Systemdämpfung
m	Gesamtzahl der Stationen im Szenario
m_I	Zahl der Stationen in Interferenzreichweite von Sender und Empfänger
n	Zahl der Stationen, die im betrachteten Zeitschritt auf den Kanal zugreifen können

p^{ge}	Wahrscheinlichkeit dafür, dass genau eine andere Station eine Übertragung initialisiert
p^{me}	Wahrscheinlichkeit dafür, dass mindestens eine andere Station eine Übertragung initialisiert
P_E	Empfangsleistung
P_S	Sendeleistung
p_b	Wahrscheinlichkeit dafür, dass der Kanal im betrachteten Zeitschlitz belegt ist
p_e	Wahrscheinlichkeit dafür, dass der Kanal im betrachteten Zeitschlitz durch eine erfolgreiche Übertragung belegt ist
p_i	Kollisionswahrscheinlichkeit für die Verkehrsklasse i
p_i^{dekr}	Wahrscheinlichkeit dafür, dass der Backoff unterbrochen wird (in Abhängigkeit der betrachteten Verkehrsklasse i)
p_i^{en}	Wahrscheinlichkeit dafür, dass keine andere Verkehrsklasse der eigenen Station eine Übertragung initialisiert
p_i^{kh}	Wahrscheinlichkeit dafür, dass keine Verkehrsklasse der eigenen Station, die eine höhere Priorität als i hat, eine Übertragung initialisiert
p_i^{tr}	Wahrscheinlichkeit dafür, dass sich eine bestimmte Verkehrsklasse i in einem Zustand befindet, in dem sie im nächsten Schritt eine Übertragung initialisieren kann
p_k	Wahrscheinlichkeit dafür, dass der Kanal im betrachteten Zeitschlitz durch eine Kollision belegt ist
PT	Sendewahrscheinlichkeit (eDCC-Mechanismus)
R_{CS}	Carrier-Sensing-Reichweite
R_I	Interferenzreichweite
R_{Tx}	Sendereichweite
S	Durchsatz
S_g	Gesamtdurchsatz
S_i	Durchsatz der Verkehrsklasse i

S_m	Durchsatz pro Station
SU	Slot Utilization, Nutzungsrate der Zeitschlitze (eDCC-Mechanismus)
T_c	Dauer einer Kollision ohne Beteiligung der betrachteten Station
T_f	Zeit, in der der Kanal frei ist
T_s	Dauer einer erfolgreichen Übertragung
T_v	Dauer einer Kollision, wenn eine AC der betrachteten Station beteiligt ist
t_{ACK}	Sendedauer einer Quittung
t_{AIFS}	Dauer eines AIFS
$t_{AIFS}(i)$	Dauer eines AIFS in Abhängigkeit der Prioriät i
$t_{AIFS}(i=0)$	Dauer des minimalen AIFS (entspricht dem AIFS der höchsten Priorität)
t_{Daten}	Sendedauer eines Pakets
t_{IFS}	Dauer eines Interframe Space
t_{SIFS}	Dauer eines SIFS
t_{Slot}	Dauer eines Zeitschlitzes
β_i	Vektor, der die Dichte von j angibt
γ	Ausbreitungskoeffizient
Δ_i	Zeit, die zwischen zwei erfolgreichen Übertragungen der Verkehrsklasse i vergeht
$\Theta_i(j,t)$	Matrix, welche für gegebenes j und t die Wahrscheinlichkeit dafür angibt, dass im nächsten Schritt eine Übertragung gestartet werden kann
ϑ	Vektor, der die Dichte von t angibt
κ_i	Wahrscheinlichkeit dafür, dass eine stattfindende Übertragung von Verkehrsklasse i stammt
λ	Wellenlänge

λ_i	Paketverlustrate der Verkehrsklasse i
τ	Wahrscheinlichkeit dafür, dass eine Station im nächsten Zeitschritt eine Übertragung startet
τ_i	Wahrscheinlichkeit dafür, dass eine AC im nächsten Zeitschritt eine Übertragung startet
τ_i^{net}	Wahrscheinlichkeit dafür, dass eine AC im nächsten Zeitschritt eine Übertragung startet, ohne dass eine AC mit höherer Priorität gleichzeitig eine Übertragung beginnt
Ψ_i	Matrix, welche die Werte von PT angibt

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Publikationen der Autorin

[1] Jörg Eberspächer, Stephan Eichler, Christian Hartmann, Silke Meister, Robert Nagel, Robert Vilzmann und Hans-Martin Zimmermann. Wireless Multi-hop Networks: Classification, Paradigms and Constraints. Technical Report, Lehrstuhl für Kommunikationsnetze, Technische Universität München, LKN-TR-4, 2007.

[2] Silke Meister und Michael Bahr. Verfahren zur Priorisierung von Medienzugriffen in Kommunikationsnetzen unter Berücksichtigung der Lastsituation. Patent, DE102009004918A1, 22.07.2010.

[3] Silke Meister und Christian Hartmann. A Quality of Service (QoS) Resource Management Architecture for Wireless Mesh Networks. In *EUNICE 2008: Proceedings of the 14th EUNICE open European Summer School*, S. 1–6, 2008.

[4] Silke Meister und Christian Hartmann. A Realistic Beamforming Model for ns-2. In *MESH 2010: Proceedings of the 3rd International Conference on Advances in Mesh Networks*, S. 48–52, 2010. (Auszeichnung für die beste Veröffentlichung)

Allgemeine Publikationen

[5] Ahmad Ali Abdullah, Fayez Gebali und Lin Cai. Modeling the throughput and Delay in Wireless Multihop Ad Hoc Networks. In *GLOBECOM 2009: Proceedings of the 2009 IEEE Global Telecommunications Conference*, S. 1–6, 2009.

[6] Gahng-Seop Ahn, Andrew T. Campbell, Andras Veres und Li-Hsiang Sun. SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks. In *INFOCOM 2002: Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, Band 2, S. 457–466, 2002.

[7] Ian Akyildiz und Xudong Wang. A survey on wireless mesh networks. *IEEE Communications Magazine*, 43(9):S23–S30, 2005.

[8] Farshid Alizadeh-Shabdiz und Suresh Subramaniam. Analytical models for single-hop and multi-hop ad hoc networks. In *BroadNets 2004: Proceedings of the First International Conference on Broadband Networks*, S. 449–458, 2004.

[9] James M. Anderson, Mohammad Ilyas und Sam Hsu. Distributed network management in an Internet environment. In *GLOBECOM '97: Proceedings of the 1997 IEEE Global Telecommunications Conference*, Band 1, S. 180–184, 1997.

[10] Vivek Aseeja und Rong Zheng. MeshMan: A management framework for wireless mesh networks. In *IM '09: Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management*, S. 226–233, 2009.

[11] Stefano Basagni. Distributed clustering for ad hoc networks. In *I-SPAN '99: Proceedings of the 4th InternationalSymposium on Parallel Architectures, Algorithms, and Networks*, S. 310–315, 1999.

[12] Bernhard Beyer. Modellierung und Analyse des Medienzugriffs des WLAN-Protokolls IEEE 802.11e. Diplomarbeit, Technische Universität München, 2010.

[13] Giuseppe Bianchi. Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, 2000.

[14] Giuseppe Bianchi, Ilenia Tinnirello und Luca Scalia. Understanding 802.11e Contention-Based Prioritization Mechanisms and Their Coexistence with Legacy 802.11 Stations. *IEEE Network*, 19(4):28–34, 2005.

[15] Luciano Bononi, Marco Conti und Lorenzo Donatiello. Design and performance evaluation of a distributed contention control (DCC) mechanism for IEEE 802.11 wireless local area networks. In *WOWMOM '98: Proceedings of the 1st ACM international workshop on Wireless Mobile Multimedia*, S. 59–67, 1998.

[16] Noureddine Boudriga, Mourad Baghdadi und Mohammad S. Obaidat. A new scheme for mobility, sensing, and security management in wireless ad hoc sensor networks. In *Proceedings of the 39th Annual Simulation Symposium*, S. 7–13, 2006.

[17] Raffaele Bruno, Marco Conti und Enrico Gregori. Mesh networks: commodity multihop ad hoc networks. *IEEE Communications Magazine*, 43(3):123–131, 2005.

[18] Carlos T. Calafate, Juan-Carlos Cano, Pietro Manzoni und Manuel P. Malumbres. A QoS architecture for MANETs supporting real-time peer-to-peer multimedia applications. In *Proceedings of the Seventh IEEE International Symposium on Multimedia*, S. 8–15, 2005.

[19] Ritu Chadha, Hong Chen, Yuu-Heng Cheng, Jason Chiang, Andrei Ghetie, Gary Levin und Harshad Tanna. Policy-based mobile ad hoc network management. In *POLICY 2004: Proceedings of the Fifth IEEE International Workshop on Policies for Distributed Systems and Networks*, S. 35–44, 2004.

[20] Wenli Chen, Nitin Jain und Suresh Singh. ANMP: ad hoc network management protocol. *IEEE Journal on Selected Areas in Communications*, 17(8):1506–1531, 1999.

[21] José R. Gallardo, Paúl Medina und Weihua Zhuang. QoS mechanisms for the MAC protocol of IEEE 802.11 WLANs. *Wireless Networks*, 13(3):335–349, 2007.

[22] Thomas Gehrsitz. Untersuchung des Medienzugriffs nach IEEE 802.11 mit QoS-Erweiterung anhand von Markov-Modellen. Diplomarbeit, Technische Universität München, 2009.

[23] Ingo Gruber. Path Lifetimes and Fair Medium Access in Wireless Multihop Networks. Doktorarbeit, Technische Universität München, 2005.

[24] Dhruv Gupta, Daniel Wu, Chao C. Chen, Chen-Nee Chuah, Prasant Mohapatra und Sanjay Rungta. Experimental Study of Measurement-based Admission Control for Wireless Mesh Networks. In *MASS 2007: Proceedings of the 2007 IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems*, S. 1–9, 2007.

[25] Lajos Hanzo II. und Rahim Tafazolli. Admission control schemes for 802.11-based multi-hop mobile ad hoc networks: a survey. *IEEE Communications Surveys and Tutorials*, 11(4):78–108, 2009.

[26] Jun He und Hung Keng Pung. Performance modeling and evaluation of IEEE 802.11 distributed coordination function in multihop wireless networks. In *ICON 2004: Proceedings of the 12th IEEE International Conference on Networks*, S. 73–79, 2004.

[27] Wendi B. Heinzelmann, Anantha P. Chandrakasan und Hari Balakrishan. An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*, 1(4):660–670, 2002.

[28] Lianxing Jia, Wei Zhu, Chenggong Zhai und Yi Du. Research on an Integrated Network Management System. In *SNPD 2007: Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, Band 2, S. 311–316, 2007.

[29] Zhen-ning Kong, Danny H. K. Tsang, Brahim Bensaou und Deyun Gao. Performance analysis of IEEE 802.11e contention-based channel access. *IEEE Journal on Selected Areas in Communications*, 22(10):2095–2106, 2004.

[30] Hyunmin Kyung, Sangho Seo und Sin-Chong Park. QoS (quality-of-service) improvement in IEEE 802.11e enhanced distributed channel access (EDCA). In *ISCIT 2004: Proceedings of the 2004 IEEE International Symposium on Communications and Information Technology.*, Band 1, S. 302–307, 2004.

[31] Ming-Yi Lee, Jiann-Liang Chen und Shinfeng Lin. A Java-based wireless network management system. In *ICPWC 97: Proceedings of the 1997 IEEE International Conference on Personal Wireless Communications*, S. 353–356, 1997.

[32] Seoung bum Lee, Gahng-Seop Ahn, Xiaowei Zhang und Andrew T. Campbell. INSIGNIA: An IP-Based Quality of Service Framework for Mobile ad Hoc Networks. *Journal of Parallel and Distributed Computing*, 60:374–406, 2000.

[33] Hwa-Chun Lin und Chien-Hsing Wang. Distributed network management by HTTP-based remote invocation. In *GLOBECOM '99: Proceedings of the 1999 IEEE Global Telecommunications Conference*, Band 3, S. 1889–1893, 1999.

[34] Chi Harold Liu, Athanasios Gkelias und Kin K. Leung. Connection admission control and grade of service for QoS routing in mesh networks. In *PIMRC 2008: Proceedings of the 19th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, S. 1–5, 2008.

[35] Matthias Lott. Improved Quality of Service Support for IEEE 802.11 DCF. In *EWC 2005: Proceedings of the 11th European Wireless Conference 2005 – Next Generation Wireless and Mobile Communications and Services*, S. 1–7, 2005.

[36] C. John McCann, George F. Elmasry, Brian Russell und Bob Welsh. A measurement-based approach for multilevel admission of heterogeneous traffic in wireless ad-hoc networks. In *MILCOM 2004: Proceedings of the 2004 IEEE Military Communications Conference*, Band 3, S. 1562–1565, 2004.

[37] Edgar Piacentini, Mauro Fonseca und Anelise Munaretto. VoIP call admission control for last mile Wireless Mesh Networks. In *WD '08: Proceedings of the 1st IFIP Wireless Days*, S. 1–5, 2008.

[38] Ramya Raghavendra, Prashanth Aravinda Kumar Acharya, Elizabeth M. Belding und Kevin C. Almeroth. Antler: A multi-tiered approach to automated wireless network management. In *INFOCOM '08: Proceedings of the 2008 IEEE INFOCOM Workshops*, S. 1–6, 2008.

[39] Lakshmi Raman. OSI systems and network management. *IEEE Communications Magazine*, 36(3):46–53, 1998.

[40] Muhammad Hassan Raza und Larry Hughes. Determining Density in Ad hoc Networks. In *CCECE '06: Proceeding s of the 2006 Canadian Conference on Electrical and Computer Engineering*, S. 2160–2163, 2006.

[41] Francoise Sailhan, Liam Fallon, Karl Quinn, Paddy Farrell, Sandra Collins, Daryl Parker, Samir Ghamri-Doudane und Yangcheng Huang. Wireless Mesh Network Monitoring: Design, Implementation and Experiments. In *2007 IEEE Globecom Workshops*, S. 1–6, 2007.

[42] Nuno Salvador, Vitor Filipe, Carlos Rabadao und Antonio Pereira. Management Model for Wireless Broadband Networks. In *ICSNC '08: Proceedings of the Third International Conference on Systems and Networks Communications*, S. 38–43, 2008.

[43] Thomas Schwabe. IP-Netze mit Interdomain-BGP-Routing. Doktorarbeit, Technische Universität München, 2006.

[44] Joao L. Sobrinho und Anjur S. Krishnakumar. Quality-of-service in ad hoc carrier sense multiple access wireless networks. *IEEE Journal on Selected Areas in Communications*, 17(8):1353–1368, 1999.

[45] Mineo Takai, Jay Martin, Rajive Bagrodia und Aifeng Ren. Directional virtual carrier sensing for directional antennas in mobile ad hoc networks. In *MobiHoc '02: Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc Networking & Computing*, S. 183–193, 2002.

[46] Juki Wirawan Tantra, Chuan Heng Foh und Adel Ben Mnaouer. Throughput and delay analysis of the IEEE 802.11e EDCA saturation. In *ICC 2005: Proceedings of the 2005 IEEE International Conference on Communications*, S. 3450–3454, 2005.

[47] Zhifeng Tao und Shivendra Panwar. Throughput and delay analysis for the IEEE 802.11e enhanced distributed channel access. *IEEE Transactions on Communications*, 54(4):596–603, 2006.

[48] Ilenia Tinnirello und Giuseppe Bianchi. Rethinking the IEEE 802.11e EDCA Performance Modeling Methodology. *IEEE/ACM Transactions on Networking*, 18(2):540–553, 2010.

[49] Gilman Tolle und David Culler. Design of an application-cooperative management system for wireless sensor networks. In *Proceeedings of the Second European Workshop on Wireless Sensor Networks*, S. 121–132, 2005.

[50] Tzu-Chieh Tsai und Ming-Ju Wu. An analytical model for IEEE 802.11e EDCA. In *ICC 2005: Proceedings of the 2005 IEEE International Conference on Communications*, Band 5, S. 3474–3478, 2005.

[51] Robert Vilzmann. Wireless Multi-Hop Networks with Beamforming Antennas and Multi-User Detection. Doktorarbeit, Technische Universität München, 2009.

[52] Robert Vilzmann, Christian Bettstetter, Daniel Medina und Christian Hartmann. Hop distances and flooding in wireless multihop networks with randomized beamforming. In *MSWiM '05: Proceedings of the 8th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, S. 20–27, 2005.

[53] Ram R. Voruganti. A global network management framework for the '90s. *IEEE Communications Magazine*, 32(8):74–83, 1994.

[54] Bernhard Walke. *Mobilfunknetze und ihre Protokolle. 1. Grundlagen, GSM, UMTS und andere zellulare Mobilfunknetze*. Mobilfunknetze und ihre Protokolle. Teubner, 2001.

[55] Dongxia Xu, Taka Sakurai und Hai L. Vu. An Access Delay Model for IEEE 802.11e EDCA. *IEEE Transactions on Mobile Computing*, 8(2):261–275, 2009.

[56] Kaixin Xu, Mario Gerla und Sang Bae. Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks. *Elsevier Ad hoc Networks*, 1(1):107–123, 2003.

[57] Yaling Yang und Robin Kravets. Distributed QoS guarantees for realtime traffic in ad hoc networks. In *SECON 2004: Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, S. 118–127, 2004.

[58] Yaling Yang und Robin Kravets. Throughput guarantees for multi-priority traffic in ad hoc networks. In *IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, S. 379–388, 2004.

[59] Wei Zhang, Jun Sun, Jing Liu und Haibin Zhang. Performance Analysis of IEEE 802.11e EDCA. *Transactions on Communications*, e-90 B:180–183, 2007.

[60] Dongmei Zhao, Jun Zou und Terence D. Todd. Admission control with load balancing in IEEE 802.11-based ESS mesh networks. *Wireless Networks*, 13(3):351–359, 2007.

[61] Hans-Martin Zimmermann. Efficient Data Transport in Cellular Multi-Hop Networks. Doktorarbeit, Technische Universität München, 2009.

Zitierte Standards

[62] Broadband Radio Access Networks (BRAN); HIgh PErformance Radio Local Area Network (HIPERLAN) Type 1; Functional specification. ETSI/BRAN EN 300-652, 1998.

[63] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2007, 2007.

[64] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. IEEE Std 802.11e-2005, 2005.

[65] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 5: Enhancements for Higher Throughput. IEEE Std 802.11n-2009, 2009.

[66] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 10: Mesh Networking. IEEE Std 802.11s-2011, 2011.

[67] IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Broadband Wireless Access Systems. IEEE Std 802.16-2009, 2009.

[68] IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Broadband Wireless Access Systems – Amendment 1: Multiple Relay Specification. IEEE Std 802.16j-2009, 2009.

[69] Information Technology – Open Systems Interconnection – Common management information protocol – Part 1: Specification. ISO 9596, 1998.

[70] Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. ITU-T X.200, 1994.

[71] Information Technology – Open Systems Interconnection – Common management information protocol: Specification. ITU-T X.711, 1997.

[72] Simple Network Management Protocol (SNMP). RFC 1157 (Historic), 1990.

[73] Management Information Base for Network Management of TCP/IP-based internets: MIB-II. RFC 1213 (Standard), 1991.

[74] Integrated Services in the Internet Architecture: an Overview. RFC 1633 (Informational), 1994.

[75] Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474 (Proposed Standard), 1998. Updated by RFCs 3168, 3260.

[76] An Architecture for Differentiated Service. RFC 2475 (Informational), 1998. Updated by RFC 3260.

[77] Introduction and Applicability Statements for Internet-Standard Management Framework. RFC 3410 (Informational), 2002.

[78] IPv6 Flow Label Specification. RFC 3697 (Proposed Standard), 2004.

Zitierte Webseiten

[79] TU Berlin. A IEEE 802.11e EDCA and CFB Simulation Model for ns-2. http://www.tkn.tu-berlin.de/research/802.11e_ns2, 2006.

[80] Kevin Fall, Kannan Varadhan und das VINT-Projekt. The ns manual. http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf, 2005.

[81] Steven McCanne und Sally Floyd. ns Network Simulator, Version 2.29. http://www.isi.edu/nsnam/ns/, 2005.