Inhaltsverzeichnis

IEEE 802.11-Netzwerke haben sich mittlerweile etabliert. Das Problem hierbei ist, dass die Anzahl der Geräte, die IEEE 802.11 -Netzwerke für die drahtlose Datenkommunikation verwenden, permanent steigt. Dadurch nimmt die Auslastung des drahtlosen Mediums zu und die Anzahl der Kollisionen erhöhen sich. Dadurch nimmt der Durchsatz für jedes einzelne Gerät ab. Aus diesem Grund wird der Backoff-Algorithmus für Szenarien betrachtet, in denen *inrange* Kollisionen stattfinden. Zudem wird der Backoff-Algorithmus mit dem Geburtstagspradoxon verglichen, um eine geschlossen Formel für die Kollisionsberechnung in Abhängigkeit der sendewilligen Geräte zu erhalten. Weiterhin werden RTS/CTS und Fragmentierung für *inrange* Kollisionsszenarien betrachtet.

1. Einleitung

Mittlerweile haben sich IEEE 802.11 Netzwerke, die umgangssprachlich auch WLAN oder Wifi genannt werden, in z. B. Haushalten, Hotels, Flughäfen, Cafes, Unternehmen, Bibliotheken, Verwaltungen und somit in privaten als auch in öffentlichen Gebäuden etabliert (vgl. MIT Roofnet Projekt und Frankfurt, 2012). Der Grund hierfür ist, dass der vorhandene Hausanschluss zum Internet problemlos erweitert und zusätzlich von verschiedenen Benutzern verwendet werden kann. Somit erhalten z. B. in Haushalten Familienmitglieder und Freunde, in Cafes und in Hotels Kunden mit ihren Smartphones, Netbooks, Touchpads oder Desktop-Computern einen Zugang über eine IEEE 802.11-Verbindung zum Internet. Allerdings ist ein Zugang zum Internet für einen oder mehrere Benutzer mit ihren Geräten nicht immer erforderlich, da z. B. eine Arbeitsgruppe ihre jeweiligen Geräte spontan miteinander verbinden möchte, um Daten miteinander auszutauschen und somit keinen Zugang zum Internet benötigt.
Aber nicht nur innerhalb von Gebäuden entstehen IEEE 802.11 Netze, sondern auch im Freien, um sowohl Städte, Bezirke und Länder (vgl. Freifunk Deutschland; Freifunk Östereich und Freifunk Schweiz) miteinander zu vernetzen als auch IEEE 802.11 Netze für Frühwarnsysteme im Falle von Naturkatastrophen zu ver-

wenden (vgl. Metrik).

Dadurch stehen IEEE 802.11 Netze zwar auf der einen Seite in Konkurrenz zu Mobilfunknetzen, wie z. B. UMTS, GPRS oder LTE, auf der anderen Seite können IEEE 802.11 Netze aber Mobilfunknetze erweitern, sofern die von Mobilfunkunternehmen betriebenen Netze zugänglich sind (vgl. Gast, 2005, Seite 8).

Eine Gemeinsamkeit der Funknetze ist, dass die Datenübertragung zwischen den einzelnen Stationen im jeweiligen Funknetz über ein gemeinsames, drahtloses Medium erfolgt, wobei der wesentliche Unterschied darin besteht, welche Frequenzbereiche für die jeweilige Datenübertragung verwendet werden. Das Problem hierbei ist, dass Frequenzbereiche von nationalen Regulierungsbehörden verwaltet werden (vgl. Gast, 2005, Seiten 2-5). Dementsprechend werden die jeweiligen Frequenzbereiche in Frequenzbänder unterteilt. Zur Nutzung der Frequenzbänder werden von den Regulierungsbehörden Lizenzen vergeben (mit Ausnahme der lizenzfreien ISM-Bänder, deren Frequenzen unter bestimmten Einschränkungen nach Belieben verwendet werden können (vgl. Gast, 2005, Seite 5 und Schiller, 2003, Seite 30). Aus diesem Grund verwenden IEEE 802.11-Stationen das freizugängliche ISM-Band für die Datenübertragung; wobei Mobilfunknetze lizenzpflichtige Frequenzbänder verwenden. Allerdings verwenden nicht nur IEEE 802.11-Stationen das freie ISM-Band zur Datenübertragung, sondern dieses wird auch von Stationen genutzt, die nicht zum IEEE 802.11-Standard kompatibel sind.
Dadurch kommt es zu Interferenzen zwischen den IEEE 802.11-kompatiblen Stationen untereinander wie auch zwischen den IEEE 802.11-kompatiblen Stationen und den nicht IEEE 802.11-kompatiblen Stationen, wobei dies zu Paketfehlern oder Paketverlusten in IEEE 802.11 Netzen führen kann. Paketverluste und Paketfehler treten jedoch nicht ausschließlich durch Interferenzen auf, sondern können auch andere Ursachen, wie z. B. Kanalfading, haben. Das Problem bei Paketverlusten und Paketfehlern in IEEE 802.11 Netzen ist, dass diese den Durchsatz zwischen einer sendenden und einer empfangenden IEEE 802.11-Stationen verringern. Dies hat zur Folge, dass sich der Durchsatz des gesamten IEEE 802.11 Netzes verringert.

Damit IEEE 802.11-Stationen auf die unterschiedlichen Arten von Paketverlus-

ten und Paketfehlern reagieren können, um den eigenen Durchsatz und somit den Durchsatz des gesamten Netzes zu erhöhen, werden durch den IEEE 802.11-Standard bestimmte Mechanismen zur Verfügung gestellt, die den Paketverlusten und Paketfehlern entgegenwirken. Das Problem hierbei ist, dass jeder Mechanismus von einer bestimmten Ursache für den Paketverlust ausgeht und dementsprechend adaptiert jeder Mechanismus unabhängig voneinander bestimmte IEEE 802.11-Übertragungsparameter, um auftretende Paketverluste oder Paketfehler zu verringern. Falls nun die Annahmen des jeweiligen Models über die Ursache oder Ursachen des Paketverlustes nicht zutreffen, kann eine Adaption von bestimmten IEEE 802.11-Übertragungsparametern den Paketverlust erhöhen oder die Auslieferung der Daten verzögern (Latenz) und somit den Durchsatz verringern. Deshalb ist es interessant zu untersuchen, welche Strategie für die Adaption von IEEE 802.11-Übertragungsparametern und Mechanismen notwendig ist, damit Paketverluste verringert und dadurch der Durchsatz zwischen den sendenden und empfangenden IEEE 802.11-Stationen maximiert wird.

1.1. Ziel der Arbeit

Das Ziel dieser Arbeit ist es, den Durchsatz zwischen einer sendenden und einer empfangenden 802.11-Station zu erhöhen, um dadurch den Durchsatz des gesamten Netzwerkes zu erhöhen.
Damit dieses Ziel erreicht werden kann, soll die MAC-Schicht des IEEE 802.11-Standards modifiziert werden. Aus diesem Grund ist es notwendig, die einzelnen Mechanismen der MAC-Schicht des IEEE 802.11-Standards zu untersuchen, um geeignete Strategien zu finden, de den Paketverlust oder die Paketfehler reduzieren. Deshalb soll die Anzahl der Kollisionen zwischen den sendewilligen 802.11-Stationen reduziert werden, um Neuübertragungen der fehlerhaften und verloren gegangenen Pakete zu vermeiden und den Durchsatz zwischen einer sendenden und einer empfangenden 802.11-Station zu erhöhen.

1.2. Aufbau der Arbeit

Zunächst wird im Kapitel 2 auf die Grundlagen und Terminologie des IEEE 802.11-Standard eingegangen. Anschließend werden in Kapitel 3 die Ursachen für Paketfehler und Paketverluste näher erläutert, um diese den im IEEE 802.11-Standard spezifizierten Schichten zuzuordnen. Dies ist notwendig, damit eine Schnittstelle zwischen den Ursachen für Paketfehler und Paketverluste und den Mechanismen der MAC-Schicht, die bestimmten Ursachen entgegenwirken, zu bestimmen. Die Mechanismen der MAC-Schicht, die Übertragungsparameter adaptieren, um bestimmte Ursachen für Paketfehler und Paketverluste zu reduzieren, werden im Kapitel 4 beschrieben. Dann wird im Kapitel 5 auf die Implementierung eingegangen und im Kapitel 6 werden dann die Ergebnisse der Implementierung beschrieben. Schließlich wird in Kapitel 7 eine Zusammenfassung und ein Ausblick gegeben.

2. IEEE 802.11 Grundlagen

Der IEEE 802.11-Standard ist 1997 (vgl. IEEE Standard 802.11, 1997) vom *Institute of Electrical and Electronics Engineers* (IEEE) veröffentlicht worden. Dieser Standard ist ein offener Standard und spezifiziert für jede 802.11-Station die MAC-Teilschicht und die Bitübertragungsschicht. Die MAC-Teilschicht, die auch MAC-Schicht genannt wird, ist ein Teil der Sicherungsschicht (Schicht 2), die für eine Punkt-zu-Multipunkt-Verbindung oder zuverlässige Punkt-zu-Punkt-Verbindung zuständig ist. Die Bitübertragungsschicht (Schicht 1) ist für die physikalische Übertragung der Daten verantwortlich (vgl. Schiller, 2003, Seite 19). Diese beiden Schichten werden zusammen mit dem Hybridmodell[1)] in Abbildung 1 dargestellt. Hierbei soll das Hybridmodell als Referenzmodell dienen. Dies ist notwendig, um die Aufgaben der MAC-Schicht und der Bitübertragungsschicht einzugrenzen, da diese beiden Schichten im IEEE 802.11-Standard spezifiziert worden sind, damit eine sendende mit einer oder mehreren empfangenden 802.11-Stationen kommu-

[1)] Für eine ausführliche Diskussion über das Hybridmodell sei auf (Tannenbaum, 2003, Seiten 66-67) verwiesen.

nizieren kann. Hierbei ist der Unterschied zwischen dem Hybridmodell und dem OSI-Modell, dass beim Hybridmodell die Sitzungs- (Schicht 5) und die Darstellungsschicht (Schicht 6) des OSI-Modells fehlen (vgl. Tannenbaum, 2003, Seiten 66-67).

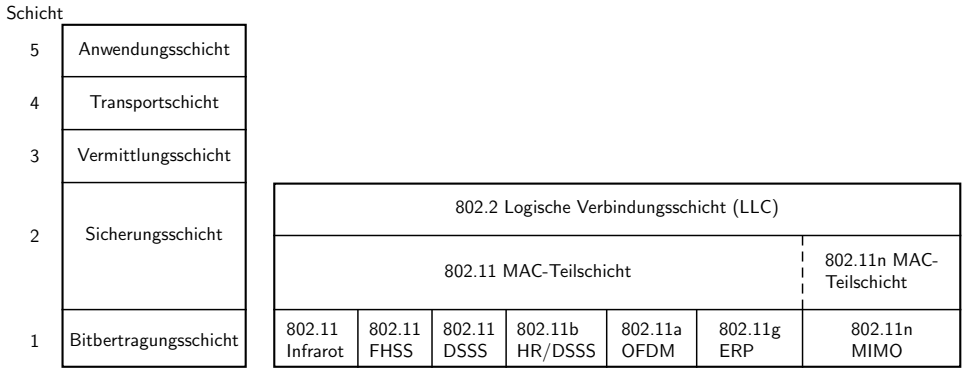


Abbildung 1: *Hybridmodell (links) und IEEE 802.11-Standard mit IEEE 802.2-Standard(rechts)*

Zudem erfolgt der Datenaustausch zwischen den Schichten im Protokollstapel des Hybridmodells bei der sendenden 802.11-Station von oben nach unten und bei der empfangenden 802.11-Station in entgegengesetzter Richtung. Somit erhält bei der sendenden 802.11-Station jede Schicht Daten von der darüber liegenden Schicht und gibt dementsprechend Daten an die darunter liegende Schicht weiter. Damit nun jede Schicht ihre speziellen Aufgaben erfüllen kann, kapselt jede Schicht die zu sendenden Daten, die die jeweilige Schicht von der darüber liegenden Schicht erhalten hat, mit zusätzlichen Informationen (engl. Overhead), wobei die gekapselten Daten in der Transportschicht als Nachrichten, in der Vermittlungsschicht als Pakete und in der Sicherungsschicht als Rahmen bezeichnet werden (vgl. Tannenbaum, 2003, Seite 231).

Wie man in Abbildung 1 sehen kann, wird die Sicherungsschicht in zwei Teile unterteilt. Der obere Teil der Sicherungsschicht beginnt meistens mit dem Protokoll der logischen Verbindungssteuerung (engl. logical link control; LLC). Das LLC-Protokoll ist im IEEE 802.2-Standard (vgl. IEEE Standard 802.2, 1998) durch die IEEE veröffentlich worden, um eine einheitliche Schnittstelle zwischen der Vermittlungsschicht und der Sicherungsschicht zu spezifizieren, da nicht nur der IEEE 802.11-Standard, sondern auch die gesamte IEEE 802-Familie unterstützt werden soll (vgl. Walke et al., 2006). Daher ist das LLC-Protokoll für die Fehler- und Flusskontrolle verantwortlich (vgl. IEEE Standard 802.2, 1998). Der untere Teil der Sicherungsschicht, ist die MAC-Schicht, die, wie schon oben erwähnt, im IEEE 802.11-Standard zusammen mit der Bitübertragungsschicht spezifiziert wird. Hauptaufgabe der MAC-Schicht ist, den Zugriff der sendenden 802.11-Stationen auf das drahtlose Übertragungsmedium zu regeln, wobei das drahtlose Übertragungsmedium von allen 802.11-Stationen gemeinsam genutzt wird und ein Broadcast-Medium ist. Außerdem nehmen die höheren Schichten, die sich über der MAC-Schicht befinden, ein drahtgebundenes Netzwerk an, deswegen muss die MAC-Schicht zusätzliche Funktionalitäten integrieren, um den höheren Schichten ein drahtgebundenes Netzwerk zu suggerieren (vgl. IEEE Standard 802.11, 2012, Seite 45).

Aus diesem Grund sind im IEEE 802.11-Standard zwei verschiedene Zugriffsverfahren für das drahtlose Übertragungsmedium spezifiziert worden, nämlich die kollisi-

onsfreie Punktkoordinationsfunktion (engl. point coordination function; PCF) und die verteilte Koordinationsfunktion (engl. distributed coordination function; DCF), die kollisionsbehaftet ist. Hierbei sei angemerkt, dass die Punktkoordinationsfunktion optional ist, wohingegen die Koordinationsfunktion obligatorisch ist (vgl. IEEE Standard 802.11, 2012, Seite 818). Weiterhin ist im IEEE 802.11e-Standard die hybride Koordinationsfunktion (engl. hybrid coordination function; HCF) spezifiziert worden, die eine Kombination aus der PCF und DCF ist und zudem die Dienstgüte (engl. Quality-of-Service; QoS) hinsichtlich des Zugriffes auf das drahtlose Übertragungsmedium unterstützt (vgl. IEEE Standard 802.11e, 2005 und IEEE Standard 802.11, 2012, Seite 12). Im Folgenden verwendet jede 802.11-Station die DCF, die dem CSMA/CA-Protokoll entspricht (vgl. Walke et al., 2006, Seite 41). Deshalb findet eine direkte Kommunikation zwischen einer sendenden und einer oder mehreren empfangenden 802.11-Stationen in der MAC-Schicht statt, indem unterschiedliche MAC-Adressen verwendet werden.

Deshalb wird bei einer Punkt-zu-Punkt-Verbindung zwischen einer sendenden und einer empfangenden 802.11-Station die MAC-Adresse der empfangenden 802.11-Station verwendet, wobei bei der Broadcast-Verbindung und bei dessen Spezialfall der Multicast-Verbindung eine allgemeine MAC-Adresse verwendet wird. Außerdem garantieren 802.11-Stationen lediglich bei einer Punkt-zu-Punkt-Verbindung einen zuverlässigen Rahmenaustausch zwischen einer sendenden und einer empfangenden 802.11-Station, die sich in gegenseitiger Kommunikationsreichweite befinden. Die zuverlässige Punkt-zu-Punkt-Verbindung in der MAC-Schicht wird gewährleistet, indem bei einer erfolgreichen Rahmenübertragung von der sendenden zur empfangenden 802.11-Station, die empfangende 802.11-Station die erfolgreiche Rahmenübertragung mit der Hilfe eines Bestätigungsrahmens (engl. Acknowledgement; ACK) quittiert. Dieser Mechanismus wird auch als positve Bestätigung (engl. positive Acknowledgement) bezeichnet, da die empfangende 802.11-Stationen lediglich erfolgreiche Rahmenübertragungen zwischen sendender und empfangender 802.11-Station quitiert (vgl. IEEE Standard 802.11, 2012, Seite 818-824). Diese Bestätigung sind jedoch für Broadcast- und Multicast-Verbindungen nicht im IEEE 802.11-Standard definiert worden und finden deshalb für diese Verbindungen nicht statt. Somit kann die sendende 802.11-Station nur bei einer Punkt-zu-Punkt-Verbindung erkennen, ob ein Paketfehler oder Paketverlust statt-

gefunden hat, da nach einer bestimmten Zeit kein Bestätigungsrahmen von der empfangenden zur sendenden 802.11-Station gesendet worden ist.
Aus diesem Grund nimmt die sendende 802.11-Station einen Paketfehler oder Paketverlust an und übertragt daraufhin den unbestätigten Rahmen erneut zur empfangenden 802.11-Station.

Folglich bildet eine sendende und eine empfangende 802.11-Station ein minimales Kommunikationssystem, wobei das Kommunikationssystem eine Zelle bildet (vgl. Labiod et al., 2007, Seite 16). Für die 802.11-Stationen, die innerhalb dieser Zelle miteinander kommunizieren, spezifziert der IEEE 802.11-Standard verschiedene Basisdienste (vgl. IEEE Standard 802.11, 2012, Seite 69). Aus diesem Grund bezeichnet der IEEE 802.11-Standard die 802.11-Stationen, die innerhalb einer Zelle miteinander kommunizieren, als Basisdienstmenge (engl. basic service set; BSS) (vgl. IEEE Standard 802.11, 2012). Die einzige Voraussetzung für eine direkte Kommunikation zwischen sendender und empfangender 802.11-Station ist, dass sich die sendende und empfangende 802.11-Station innerhalb der jeweiligen Kommunikationsreichweite befinden und miteinander assoziert sind, wobei die miteinander assozierten 802.11-Stationen in Abbildung 2 durch gestrichelte Linien dargestellt sind. Deshalb ist für die direkte Kommunikation zwischen der sendenden und der empfangenden 802.11-Station die Vermittlungsschicht nicht notwendig, da die Vermittlung der Rahmen zwischen der sendenden und der empfangenden 802.11-Station in der MAC-Schicht stattfindet. Die direkte Kommunikation zwischen der sendenden und der empfangenden 802.11-Station innerhalb der Kommunikationsreichweite wird als ad-hoc Netzwerk oder in der Terminologie des IEEE 802.11-Standards unabhängiges BSS (engl. independent BSS; IBSS) bezeichnet. Das bedeutet, dass das IBSS auf ein bestimmtes Kommunikationsgebiet eingeschränkt wird, welches abhängig von der Kommunikationsreichweite der 802.11-Stationen ist, wobei das Kommunikationsgebiet der 802.11-Stationen im IEEE 802.11-Standard als BSS-Gebiet bezeichnet wird. Neben dem IBSS ist im IEEE 802.11-Standard das Infrastruktur-Netzwerk und dessen Erweiterung spezifiziert worden, wobei das Infrastruktur-Netzwerk im IEEE 802.11-Standard Infrastruktur-BSS und dessen Erweiterung „erweiterte Dienstmenge“ (engl. extended service set; ESS) bezeichnet wird. Das Infrastruktur-BSS ist in Abbildung 2 (a) dargestellt. Wie aus dieser Abbildung ersichtlich ist, besteht ein Infrastruktur-

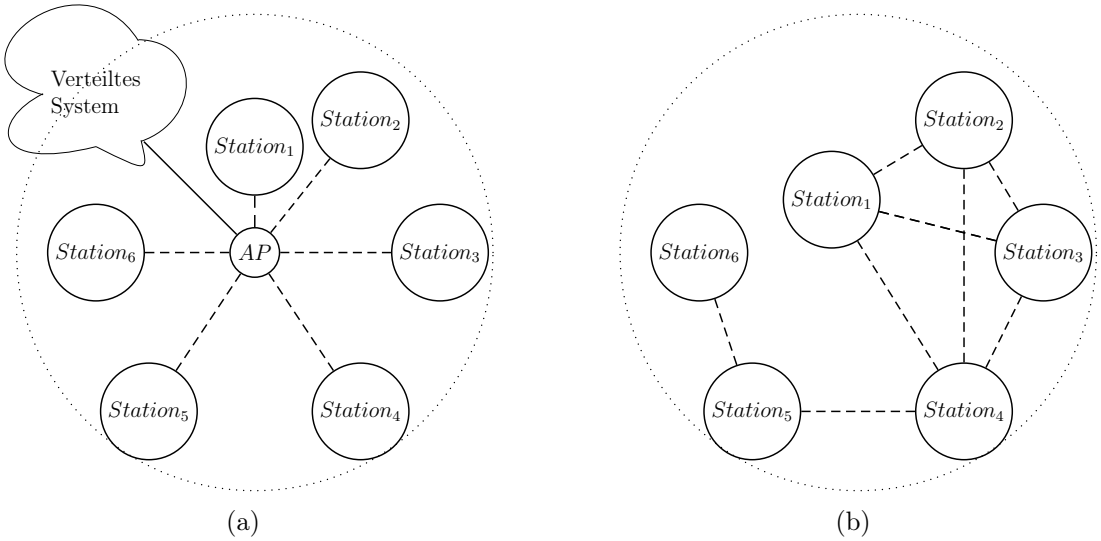


Abbildung 2: *Infrastruktur- (a) und ad-hoc Netzwerk (b)*

BSS aus 802.11-Stationen, mindestens einem verteilten System und mindestens einem Zugriffspunkt (engl. Access Point; AP) zum verteilten System, wobei das verteilte System im IEEE 802.11-Standard nicht näher spezifiziert worden ist (vgl. IEEE Standard 802.11, 2012). Ein AP erhält somit sowohl die Eigenschaft einer Basisstation als auch zusätzliche Eigenschaften, die abhängig vom verteilten System sind, wie z. B. die zusätzlichen Eigenschaften eines Gateways oder Portals oder zu mindestens einer Bridge.

Eine Basisstation muss jedoch nicht unbedingt mit einem oder mehreren verteilten Systemen verbunden sein, wohingegen dies beim AP vorausgesetzt wird (vgl. IEEE Standard 802.11, 2012, Seite 5 und Labiod et al., 2007, Seite 296).

Weiterhin ist aus Abbildung 2 (a) ersichtlich, dass ein AP zusammen mit den 802.11-Stationen, die mit dem AP assoziert sind, eine sternförmige Netzwerktopologie bildet, wie dies in Netzwerken der Fall ist, die auf dem IEEE 802.3-Standard basieren. Somit ist es die Aufgabe des APs, Rahmen sowohl zwischen der sendenden und der empfangenden 802.11-Station weiterzuleiten als auch Rahmen mit dem verteilten System auszutauschen. Dies setzt voraus, dass sich alle 802.11-Stationen, die miteinander Rahmen austauschen, sich innerhalb der Kommuni-

kationsreichweite des APs befinden müssen, wobei die Kommunikationsreichweite des APs das BSS-Gebiet festlegt, wohingegen die Kommunikationsreichweiten der einzelnen 802.11-Stationen das BSS-Gebiet des IBSS bestimmen. Wenn das BSS-Gebiet und somit das Abdeckungsgebiet eines Infrastruktur-BSS nicht ausreichend ist, werden verschiedene Infrastruktur-BSS-Netzwerke mit der Hilfe des verteilten Systems miteinander zu einem ESS verbunden. Dabei sollten sich die einzelnen BSS-Gebiete der verschiedenen APs überlappen, damit eine vollständige Abdeckung im vergrößteren BSS-Gebiet erreicht wird und somit sich eine oder mehrere 802.11-Stationen innerhalb des vergrößerten BSS-Gebietes bewegen können, ohne dass die Kommunikation zwischen den sich bewegenden 802.11-Stationen zu einem der APs im vergrößerten BSS-Gebiet abreißt. Dabei erfolgt die Kommunikation zwischen den APs über das verteilte System und somit ist der Vorgang für die LLC-Schichten der 802.11-Stationen transparent (vgl. IEEE Standard 802.11, 2012, Seite 47).

In Abbildung 1(b) ist ebenso ersichtlich, dass die MAC-Schicht nochmals durch eine horizontale, gestrichelte Linie abgegrenzt ist, wobei zwischen der 802.11- und der 802.11n-MAC-Teilschicht unterschieden wird. Dies ist notwendig, da der IEEE 802.11-Standard sukzessiv auf der Bitübertragungsschicht durch die Standards IEEE 802.11a (siehe IEEE Standard 802.11a, 1999), IEEE 802.11b (siehe IEEE Standard 802.11b, 1999), IEEE 802.11g (siehe IEEE Standard 802.11g, 2003) und IEEE 802.11n (siehe IEEE Standard 802.11n, 2009) weiterentwickelt worden ist, um die Datenrate auf der Bitübertragungsschicht zu erhöhen und um die vorhandene 802.11-MAC-Teilschicht weiterhin zu verwenden. Jedoch ist bei hohen Datenraten das Problem aufgetreten, dass der *Overhead* der 802.11-MAC-Schicht nicht vernachlässigt werden darf, da die hohen Datenraten von 802.11n nicht mehr mit der 802.11-MAC-Schicht erreicht werden und somit die 802.11-MAC-Schicht entsprechend modifiziert worden ist (vgl. Perahia und Stacey, 2008, Seiten 206 - 207). Die Modifizierung der 802.11-MAC-Schicht wird im Folgenden als 802.11n-MAC-Schicht bezeichnet.

Die Bitübertragungsschicht ist für die physikalische Übertragung der MAC-Rahmen zwischen der sendenden und der empfangenden 802.11-Station zuständig, wobei die Rahmen der MAC-Schicht von der Bitübertragunsschicht lediglich als Bitströ-

me wahrgenommen werden. Es ist daher die Aufgabe der Bitübertragungsschicht die einzelnen Bits zu kodieren, zu modulieren und schließlich über das drahtlose Medium zu übertragen; die kodierten Bits werden dabei als Symbole bezeichnet.

Für die Übertragung der Symbole über das drahtlose Medium ist die Entfernung zwischen der sendenden und der empfangenden 802.11-Station entscheidend, da die Reichweite der sendenden und der empfangenden 802.11-Station von der verwendeten Frequenz, deren Modulation und der Kodierung abhängig ist (vgl. Gast, 2005, Seite 6). Aus diesem Grund spezifiziert der IEEE 802.11-Standard für die Bitübertragungsschicht neben den Kodierungs- und Modulationsverfahren auch den Frequenzbereich für die drahtlose Kommunikation zwischen den 802.11-Stationen, wobei der IEEE 802.11-Standard sowohl den Infrarot- als auch den Funkbereich spezifiziert. In der Praxis konnte sich die Kommunikation zwischen den 802.11-Stationen im Funkbereich gegenüber der Kommunikation zwischen den 802.11-Stationen im Infrarotbereich durchsetzen (siehe Kapitel 3.2). Weiterhin hat der IEEE 802.11-Standard zwei Verfahren auf der Bitübertragungsschicht spezifiziert, nämlich das Frequenzsprungverfahren und das Spreizbandverfahren (engl. direct sequence spread spectrum; DSSS)(vgl. Tannenbaum, 2003, Seite 123). Hierbei hat sich das DSSS-Verfahren gegenüber dem Frequenzsprungverfahren durchgesetzt, da mit der Spezifizierung des IEEE 802.11b-Standards das DSSS-Verfahren um das HR/DSSS-Verfahren des IEEE 802.11b-Standards erweitert worden ist und somit beim HR/DSSS-Verfahren höhere Datenraten als beim Frequenzsprungverfahren des IEEE 802.11-Standards erreicht werden. Die Gemeinsamkeit zwischen dem IEEE 802.11-Standard und dem IEEE 802.11b-Standard ist, dass alle Verfahren für das 2,4-GHz-ISM-Band spezifiziert worden sind.

Ein weiteres Modulationsverfahren ist das OFDM-Verfahren, das im IEEE 802.11a-Standard für das 5-GHz-Band spezifiziert worden ist. Damit das OFDM-Verfahren des IEEE 802.11a-Standards auch im 2, 4 GHz-ISM-Band verwendet werden kann, um höhere Datenraten als das HR/DSSS-Verfahren zu erreichen, spezifiziert der IEEE 802.11g-Standard das OFDM-Verfahren für das 2,4-GHz-ISM-Band. Außerdem verwendet der IEEE 802.11n-Standard genauso wie der IEEE 802.11a- und der IEEE 802.11g-Standard das OFDM-Verfahren, wobei der IEEE 802.11n-Standard

mehrere Antennen für die sendende und die empfangende 802.11n-Station spezifiziert (engl. Multiple Input Multiple Output; MIMO). Bei 802.11a- und 802.11g-Stationen wird lediglich eine Antenne für die sendenden und die empfangende 802.11-Station verwendet. Durch die Verwendung von mehreren Antennen erzielen 802.11n-Stationen höhere Datenraten als 802.11a- oder 802.11g-Stationen. Außerdem spezifiziert der 802.11n-Standard die Rahmenübertragung zwischen der sendenden und der empfangenden 802.11n-Station sowohl für das 2,4-GHz- als auch für das 5-GHz-ISM-Band. Dies erfordert jedoch zwei Transceiver für jede 802.11n-Station, da für jedes der beiden ISM-Bänder für die Rahmenübertragung zwischen der sendenden und der empfangenden 802.11n-Station jeweils ein Transceiver notwendig ist (vgl. Perahia und Stacey, 2008, Seite XX).

3. Ursachen für Paketfehler und Paketverluste

3.1. In der Mediumzugriffssteuerungsschicht (MAC)

Die MAC-Schicht regelt für jede 802.11-Station den Zugriff auf das drahtlose Medium (siehe Kapitel 2). Dabei wird davon ausgegangen, dass jede 802.11-Station und jeder AP für den Mediumzugriff die DCF verwendet, die dem CSMA/CA-Protokoll entspricht (siehe Kapitel 2). Aus diesem Grund müssen sowohl 802.11-Stationen als auch APs um die Nutzung des gemeinsamen, drahtlosen Mediums miteinander konkurrieren, falls diese Rahmen versenden möchten.
Weiterhin wird vorausgesetzt, dass eine zuverlässige Punkt-zu-Punkt-Verbindung zwischen den sendenden und empfangenden 802.11-Stationen existiert (siehe Kapitel 2), wobei die Punkt-zu-Punkt-Übertragung zwischen sendender und empfangender 802.11-Station im Allgemeinen als Unicasting bezeichnet wird (vgl. Tannenbaum, 2003, Seite 30). Außerdem sei angemerkt, dass es keinen Unterschied hinsichtlich des Mediumzugriffes zwischen 802.11-Stationen und APs gibt, deshalb werden APs nicht weiter erwähnt.
Der Zugriff der sendenden 802.11-Stationen auf das gemeinsame, drahtlose Medium ist jedoch problematisch, da lediglich eine sendende 802.11-Station das gemeinsame, drahtlose Medium verwenden kann, um Rahmen zu einer empfangenden 802.11-Station über das gemeinsame, drahtlose Medium zu übertragen. Somit führen parallele Paketübertragungen von mehreren 802.11-Stationen, die sich in Kommunikationsreichweite befinden, im Allgemeinen zu Paketverlusten. Dies liegt an dem im IEEE 802.11-Standard spezifizierte Modulationsverfahren der Bitübertragungsschicht, da diese kein Code Division Multiplexing-Verfahren unterstützen (siehe Schiller, 2003, Seite 45). Deshalb finden gleichzeitige Übertragungen von verschiedenen sendenden 802.11-Stationen im gemeinsamen, drahtlosen Medium nur statt, wenn jede sendende 802.11-Station zu jeweils einer anderen empfangenden 802.11-Station Rahmen überträgt und sich die jeweiligen empfangenden 802.11-Stationen außerhalb der Kommunikationsreichweiten der anderen befinden (vgl. Tannenbaum, 2003, Seite 302). Das heißt, es muss eine räumliche Distanz zwischen den sendenden und empfangenden 802.11-Stationen existieren.

Falls nun zwei oder mehrere sendende 802.11-Stationen ihre Rahmen zu unterschiedlichen empfangenden 802.11-Stationen übertragen, wobei die unterschiedlichen empfangenden 802.11-Stationen sich im selben BSS-Gebiet befinden und sich dadurch innerhalb gegenseitiger Kommunikationsreichweite befinden, werden die obigen Bedingungen für eine gleichzeitige Rahmenübertragung zwischen sendender und empfangender 802.11-Station verletzt, d. h. die Rahmen kollidieren miteinander. In diesem Fall kommt es zu Paketfehlern oder Paketverlusten, wobei Paketfehler oder Paketverluste beim Unicasting von der sendenden 802.11-Station nur erkannt werden, wenn nach dem Ablauf einer bestimmten Zeit kein Bestätigungsrahmen von der empfangenden 802.11-Station an die sendende 802.11-Station übertragen worden ist. Aus diesem Grund geht die sendende 802.11-Station von einem Rahmenfehler oder Rahmenverlust bei der empfangenden 802.11-Station aus und übertragt diesen Rahmen erneut zur empfangenden 802.11-Station, bis die empfangende 802.11-Station die erfolgreiche Rahmenübertragung durch einen Bestätigungsrahmen bei der sendenden 802.11-Station quittiert.

Damit jede 802.11-Station bei der Rahmenübertragung Kollisionen vermeidet, detektiert jede 802.11-Station mit der Hilfe der physikalischen Trägerprüfung (engl. „Carrier Sense“), die zur Bitübertragungsschicht gehört, ob das Medium entweder von einer bereits sendenden 802.11-Station belegt ist oder das Medium frei für die Rahmenübertragung ist. Hierbei treten bei der physikalischen Trägerprüfung zwei Probleme auf, die einen Paketfehler oder Paketverlust zur Folge haben.

Das erste Problem wird als verstecktes Knotenproblem (engl. hidden node problem) und das zweite Problem als *inrange* Kollision bezeichnet (vgl. Schiller, 2003, Seite 70ff).

Das versteckte Knotenproblem ist in Abbildung 3(a) dargestellt, wobei die gepunkteten Kreise die Reichweite der physikalischen Trägerprüfung der jeweiligen sendenden 802.11-Station skizzieren. Zum versteckten Knotenproblem kommt es, wenn zwei sendende 802.11-Stationen zur gleichen empfangenden 802.11-Station Rahmen übertragen und sich die beiden sendenden 802.11-Stationen außerhalb der Reichweite der jeweiligen physikalischen Trägerprüfung befinden. Daher ist

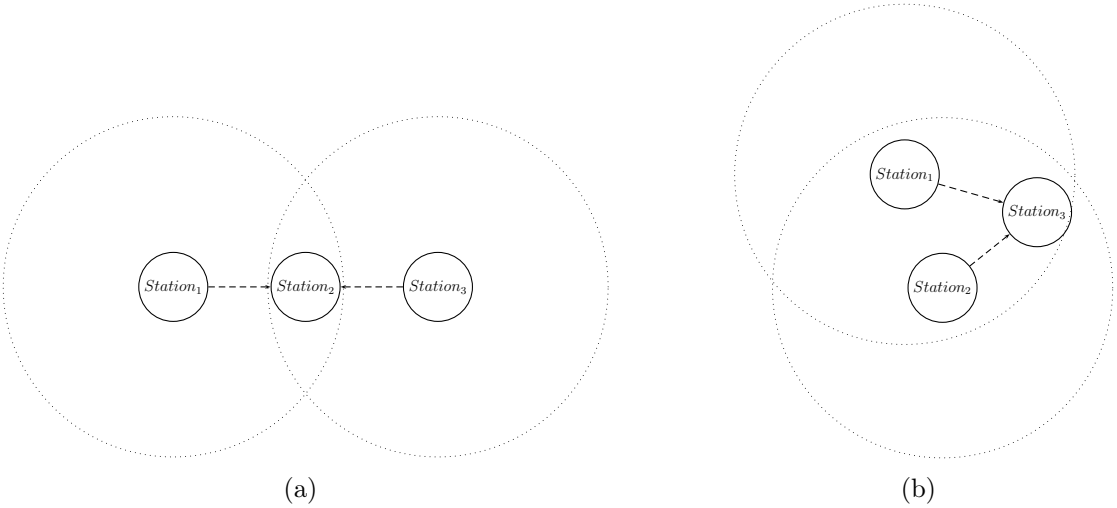


Abbildung 3: *Verstecktes Knotenproblem (a) und inrange Kollision (b)*

wegen der begrenzten Reichweite der physikalischen Trägerprüfung von beiden sendenden 802.11-Stationen eine gegenseitige Detektion nicht möglich. Deshalb kommt es bei der Rahmenübertragung der beiden sendenden 802.11-Stationen zu Kollisionen an der gleichen empfangenden 802.11-Station, obwohl die Trägerprüfungen von jeder sendenden 802.11-Station das Übertragungsmedium als frei detektiert hat. Somit setzen beide 802.11-Stationen ein freies, drahtloses Medium voraus und übertragen ihre jeweiligen Rahmen zur gleichen empfangenden 802.11-Station. Folglich kommt es bei der empfangenden 802.11-Station zu Paketfehlern oder sogar zu Paketverlusten, so dass die kollidierten Pakete von beiden sendenden 802.11-Stationen zur empfangenden 802.11-Station neu übertragen werden müssen.

Das zweite Problem wird als *inrange* Kollision bezeichnet (siehe Abbildung 3(b)) und ereignet sich, wenn mindestens zwei oder mehrere 802.11-Stationen mit der Hilfe ihrer jeweiligen Trägerprüfung das Übertragungsmedium als frei detektieren. Dadurch werden ihre Rahmen fast zeitgleich übertragen, wobei der Unterschied zwischen der *inrange* Kollision und des versteckten Knotenproblems darin besteht, dass sich bei der *inrange* Kollision alle 802.11-Stationen innerhalb des physikalischen Trägerprüfungsbreiches befinden und sich deshalb mit Hilfe der Trägerprüfung gegenseitig detektieren (siehe die gepunkteten Kreise in Abbildung 3(b)).

Dies bedeutet, dass die Reichweite der Trägerprüfung von jeder sendenden 802.11-Station ausreichend ist. Die fast zeitgleiche Rahmenübertragung von mindestens zwei oder mehreren 802.11-Stationen verursacht allerdings eine Kollision (siehe Tannenbaum, 2003, Seite 283). Dadurch kommt es zu Paketfehlern oder Paketverlusten und deshalb müssen auch hier alle sendenden 802.11-Stationen, deren Rahmen kollidiert sind, ihren kollidierten Rahmen erneut zur jeweiligen empfangenden 802.11-Station übertragen.

Dabei tritt bei den sendenden 802.11-Stationen ein weiteres Problem auf: Da diese nicht fähig sind, gleichzeitig das Übertragungsmedium mit der Hilfe der physikalischen Trägerprüfung abzuhören und Rahmen zu senden, wie dies bei drahtgebundenen Stationen der Fall ist, die konform zum IEEE 802.3-Standard (Ethernet-Standard) sind. Daher ist es für eine sendende 802.11-Station nicht möglich, wenn es zu Kollisionen gekommen ist, die Rahmenübertragung vorzeitig abzubrechen, um mit der erneuten Rahmenübertragung zu beginnen. Dieser Nachteil ist vorallem nicht mehr vernachlässigbar, wenn lange Rahmen miteinander kollidieren, da kollidierte Rahmen erst detektiert werden, wenn der komplette Rahmen übertragen worden ist und nachdem eine bestimmte Zeit verstrichen ist, in der kein Bestätigungsrahmen die sendende 802.11-Station erreicht hat. Durch diesen Vorgang entsteht Latenz, die bei einem vorzeitigen Abbruch der Rahmenübertragung für einen erneuten Übertragungsversuch des kollidierten Rahmens verwendet werden kann.

3.2. In der Bitübertragungsschicht

Die sendende 802.11-Station verwendet die Bitübertragungsschicht, um Rahmen von der MAC-Schicht in Signale zu konvertieren, wobei die Bitübertragungschicht die Rahmen der MAC-Schicht lediglich als Bitströme betrachtet (vgl. Schiller, 2003, Seite 19). Diese Signale werden dann durch die Bitübertragungsschicht der sendenden 802.11-Station über das drahtlose Medium zur Bitübertragungsschicht der empfangenden 802.11-Station übertragen. Das drahtlose Medium für die physikalische Übertragung zwischen sendender und empfangender 802.11-Station ist sowohl für das 2,4 GHz- als auch für das 5 GHz-ISM-Band im IEEE 802.11-Standard

und dessen Erweiterungen spezifiziert worden. Zudem ist eine Unterteilung der beiden ISM-Bänder in verschiedene Kanäle durch den IEEE 802.11-Standard und dessen Erweiterungen festgelegt worden (vgl. IEEE Standard 802.11, 2012, 1504ff). Hierbei wird zwischen überlappenden und nicht überlappenden Kanälen unterschieden, da eine parallele Signalübertragung von mehreren sendenden 802.11-Stationen, die sich in gegenseitiger Kommunikationsreichweite befinden, nur möglich ist, wenn jede der sendenden 802.11-Stationen einen disjunkten Kanal verwendet und sich die disjunkten Kanäle nicht gegenseitig überlappen (vgl. IEEE Standard 802.11, 2012, Seite 1572ff).

Diese Bedingungen sind notwendig, wenn sich die sendenden 802.11-Stationen innerhalb gegenseitiger Kommunikationreichweite befinden und im selben Kanal senden, da die im IEEE 802.11-Standard spezifzierten Modulationsverfahren bei einer gleichzeitigen Signalübertragung von mehreren sendenden 802.11-Stationen Paketfehler oder Paketverluste generieren. Außerdem müssen zwei oder mehrere sendende 802.11-Stationen Kanäle verwenden, die sich nicht überlappen, da ansonsten die Signale der sendenden 802.11-Stationen miteinander interferieren. Die verwendeten Kanäle dürfen deshalb nicht benachbart sein (vgl. Garcia Villegas et al., 2007).

Im Folgenden wird davon ausgegangen, dass die Signalübertragung zwischen der sendenden und der empfangenden 802.11-Station im selben Kanal stattfindet. Damit nun Signale, die von der gesendeten 802.11-Station übertragen werden, wieder von der empfangenden 802.11-Station in einen fehlerfreien Bitstrom dekodiert werden (vgl. Schiller, 2003, Seite 19), muss das Signal-Rausch-Verhältnis (engl. Signal-to-Noise-Ratio; SNR), das vom verwendeten Modulationsverfahren abhängig ist, für die Signaldekodierung ausreichend sein (vgl. Walke et al., 2006, Seite 18 und Bicket, 2005, Seite 11). Das bedeutet wiederum, dass die verwendete Kodierung und Modulation abhängig von den Mindestanforderungen an das Signal-Rausch-Verhältnis ist, wobei die Signalstärke der sendenden 802.11-Station durch die jeweilige Umgebung beeinflusst wird. Dadurch kann es zum Signalschwund, das auch *Fading* genannt wird, kommen (vgl. Walke et al., 2006, Seite 11-12 und Wysocki und Zepernick, 2000).

Das Signalschwundresultiert aus verschiedenen Ursachen, da Signale Objekte durchdringen, von diesen gebrochen, blockiert oder an diesen reflektiert werden (vgl. Schiller, 2003, Seite 37-38). Aus diesem Grund ist die Ausbreitung von Signalen nicht vorhersagbar. Deshalb kann sich der drahtlose Kanal mit der Zeit verändern, wobei sich die Veränderungen des Kanals wiederum auf die Anforderungen an die Signaldekodierung bei der empfangenden 802.11-Station auswirken.

Wenn Signale Objekte durchdringen, werden die Signale entsprechend gedämpft; die Dämpfung der Signale durch Objekte wird als Abschattung (engl. Shadowing) bezeichnet. Falls die Abschattung des Signals durch ein oder mehrere Objekte zu stark ist, wird das Signal blockiert (vgl. Schiller, 2003, Seite 37-38). Dieses Phänomen ist ein wesentlicher Grund, warum sich die Kommunikation zwischen den 802.11-Stationen im Funkbereich gegenüber der Kommunikation zwischen den 802.11-Stationen im Infrarotbereich in der Praxis durchgesetzt hat. Vorausgesetzt, dass die sendenden 802.11-Stationen sich sowohl für die Infrarot- als auch für die Funkübertragung an die maximale Sendeleistung halten, die im IEEE 802.11-Standard definierte worden ist.

Deshalb durchdringen Funksignale trotz Abschattung und eingeschränkter maximaler Sendeleistung bestimmte Objekte, wie z. B. Wände, wohingegen Infrarotsignale von diesen Objekten blockiert werden (vgl. Valadas et al., 1998).

Ein weiteres Phänomen ist die Mehrfachausbreitung, die auch Selektivschwund (engl. *Multipath-Fading*) genannt wird (vgl. Tannenbaum, 2003, Seite 88). Bei der Mehrfachausbreitung werden Signale, die auf bestimmte Objekte treffen, von diesen Objekten in verschiedene Richtungen reflektiert. Somit erreichen die verschiedenden Signale aufgrund verschiedener Weglängen zu unterschiedlichen Zeitpunkten die empfangende 802.11-Station. Folglich überlagern sich die reflektieren Signale bei der empfangenden 802.11-Station. Durch die Überlagerungen von verschiedenen Signalen wird das daraus resultierende Signal nach dem Superpositionsprinzip verstärkt, gedämpft oder ausgelöscht. Somit kommt es durch die Mehrfachausbreitung zum Paketverlust an der empfangenden 802.11-Station, wenn ein Signal durch die Mehrfachausbreitung ausgelöscht wird. Zum Paketfehler kommt

es, wenn das Signal durch die Mehrfachausbreitung so verändert wird, dass es bei der empfangende 802.11-Station zur Intersymbolinterferenz kommt und somit das Signal von der empfangenden 802.11-Station fehlerhaft dekodiert wird (vgl. Schiller, 2003, Seite 40).

Signalschwundwird aber nicht nur durch Abschattung oder Mehrfachausbreitung verursacht, sondern auch durch Mobilität (vgl. Kim et al., 1996). Hierbei kann sowohl die sendende als auch die empfangende 802.11-Station mobil sein. Wenn sich mobile 802.11-Stationen voneinander entfernen, erhöht sich die Distanz zwischen sendender und empfangender 802.11-Station und somit ist wegen des Pfadverlustes die verwendete Kodierung und Modulation für die Signalübertragung nicht mehr ausreichend, damit die empfangende 802.11-Station das Signal fehlerfrei dekodieren kann (vgl. Schiller, 2003, Seite 36 - 37).

Aber nicht nur mobile 802.11-Stationen verringern unter bestimmten Bedingungen die Signalstärke an der empfangenden 802.11-Station, sondern auch sich bewegende Personen oder Objekte, die sich in der Nähe der empfangenden 802.11-Station befinden (vgl. Hashemi, 1993).

Hinzu kommt, dass aufgrund der Weiterentwicklung von Modulationsverfahren es für 802.11b-Stationen nicht möglich ist, 802.11g-Stationen mit Hilfe der physikalischen Trägerprüfung zu detektieren. Aus diesem Grund nehmen 802.11b-Station einen freien Kanal an, obwohl eine 802.11g-Station bereits Signale sendet; somit kommt es zwischen den Signalen der beiden 802.11-Stationen zu Interferenzen. Dieses Problem wird im Folgenden als „g vs. b“ -Problem bezeichnet (siehe Abbildung 4). Außerdem erzeugen nicht nur 802.11-Stationen untereinander Interferenzen, sondern 802.11-Stationen interferieren ebenso mit Stationen, die nicht kompatibel zum IEEE 802.11-Standard sind, wie z. B. Bluetooth- und ZigBee-Stationen, Mikrowellen, schnurlose Telefone, etc. (vgl. Rayanchu et al., 2011). Hierbei wird unterschieden, ob die Stationen, die nicht kompatibel zum IEEE 802.11-Standard sind, schmalbandig oder breitbandig mit den sendenden 802.11-Stationen interferieren. Ferner wird unterschieden, ob die Stationen, die nicht zum IEEE 802.11-Standard kompatibel sind, sich koopertiv gegenüber den sendenden 802.11-Stationen verhalten.

3.3. Zusammenfassung

In den beiden vorrangegangenen Unterkapiteln sind die Ursachen für Paketfehler und Paketverluste erläutert worden. Damit die verschiedenen Ursachen für Paketfehler und Paketverluste der MAC- und der Bitübertragungsschicht zugeordnet werden können, geht Unterkapitel 3.1 auf die Ursachen für Paketfehler und Paketverluste in der MAC-Schicht und Unterkapitel 3.2 auf die Ursachen in der Bitübertragungsschicht näher ein. Die verschiedenen Ursachen für Paketfehler und Paketverluste werden in Abbildung 4 dargestellt und entsprechend klassifiziert.

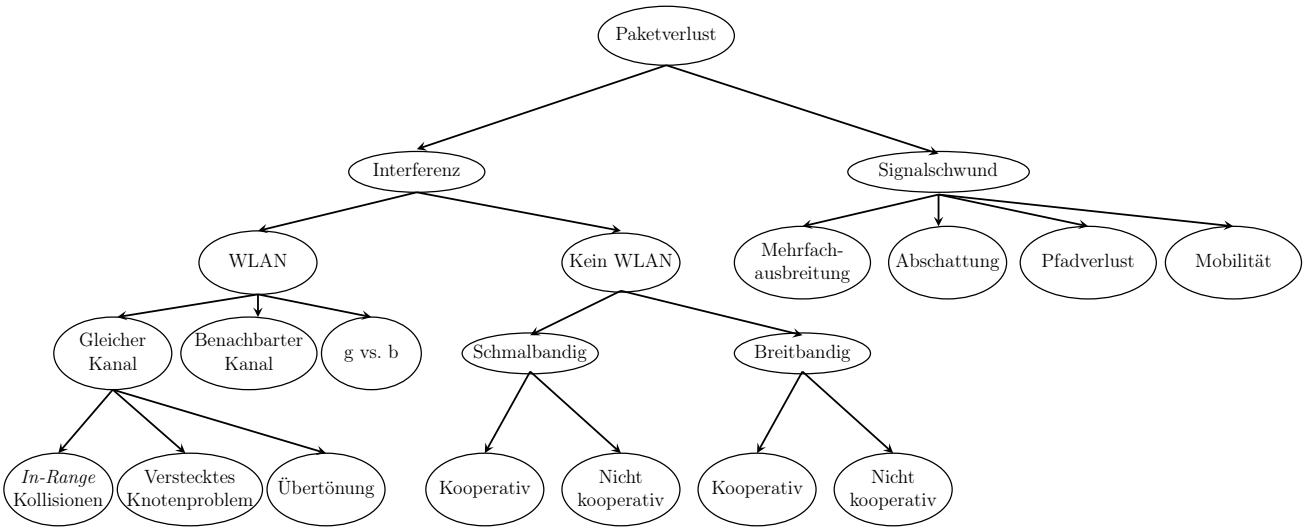


Abbildung 4: *Baumstruktur zur Klassifizierung von Paketverlusten*

4. Mechanismen gegen Paketfehler und Paketverluste

In diesem Kapitel wird näher auf die Mechanismen der MAC-Schicht eingegangen, die bestimmten Ursachen für Paketfehler und Paketverluste entgegenwirken. Die Ursachen für Paketfehler und Paketverluste sind bereits im Kapitel 3 erläutert worden. Zudem liefert Abbildung 4 im Unterkapitel 3.3 einen Überblick über mögliche Ursachen für Paketfehler und Paketverluste.

4.1. Backoff-Algorithmus und Geburtstagsparadoxon

Damit eine sendewillige 802.11-Station Pakete zu einer empfangenden 802.11-Station übertragen kann, verwendet diese für den Zugriff auf das gemeinsame, drahtlose Medium das CSMA/CA-Verfahren (vgl. IEEE Standard 802.11, 2012, Seite 824). Durch das CSMA/CA-Verfahren konkurrieren alle sendewilligen 802.11-Stationen um den Zugriff auf das gemeinsame, drahtlose Medium. Befindet sich eine sendewillige 802.11-Station in der Konkurrenzphase, verwendet diese den binären Backoff-Algorithmus (vgl. IEEE Standard 802.11, 2012, Seite 818). Der binäre Backoff-Algorithmus wird in Abbildung 5 als Aktivitätsdiagramm dargestellt (vgl. Seemann und von Gudenberg, 2006, Seite 27).

Wie man anhand von Abbildung 5 sehen kann, beginnen sendewillige 802.11-Stationen nicht wie beim ALOHA-Verfahren sofort mit der Paketübertragung (vgl. Tannenbaum, 2003, Seite 283ff), sondern jede sendewillige 802.11-Station verzögert ihre Paketübertragung um eine zufällige Wartezeit, den Backoff. Dieser wird durch den Backoff-Algorithmus aus einem vorgegebenen Zeitintervall ermittelt, das auch als Backoff-Fenster oder Konkurrenzfenster (engl. Contention window; CW) bezeichnet wird (vgl. IEEE Standard 802.11, 2012, Seite 836ff). Die Größe des Backoff-Fensters ist im IEEE 802.11-Standard und dessen Erweiterungen IEEE 802.11a/b/g/n spezifiziert worden (vgl. IEEE Standard 802.11, 2012, Seite 1442-1780; IEEE Standard 802.11a, 1999, Seite 40; IEEE Standard 802.11b, 1999, Seite 29; IEEE Standard 802.11g, 2003, Seite 47 und IEEE Standard 802.11n, 2009, Seite 336).

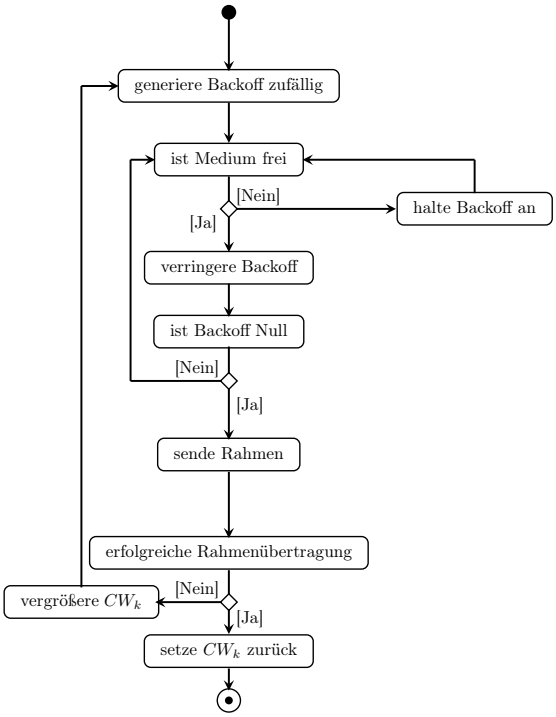


Abbildung 5: *Backoff-Algorithmus in der MAC-Schicht*

Außerdem ist die aktuelle Backoff-Fenstergröße CW_k von den Übertragungsversuchen abhängig, die eine sendewillige 802.11-Station zur Übertragung des aktuellen Rahmens tätigen muss, da der Backoff-Algorithmus als Ursache für jeden fehlgeschlagenen Übertragungsversuch von einer *inrange* Kollision k ausgeht (siehe Kapitel 3.1).

Damit *inrange* Kollisionen zwischen den sendewilligen 802.11-Stationen verringert werden (siehe Abbildung 5), vergrößert der Backoff-Algorithmus bei jeder *inrange* Kollision CW_k bis die maximale Backoff-Fenstergröße CW_{max} erreicht worden ist oder der Rahmen nach einer maximalen Anzahl von Übertragungsversuchen verworfen wird. Dabei geht der Backoff-Algorithmus, der im IEEE 802.11-Standard spezifiziert worden ist, von einer minimalen Backoff-Fenstergröße CW_{min} aus und verdoppelt CW_k nach jeder *inrange* Kollision , um der aufgetretenen *inrange* Kollision entgegenzuwirken. Daher kommt es zur Kollisionsvermeidung zwischen den sendewilligen 802.11-Stationen.

Nach erfolgreicher Paketübertragung beginnt der Backoff-Algorithmus mit minimalem Backoff CW_{min} für die nächste Paketübertragung von vorne.

Somit kann CW_k in Abhängigkeit von CW_{min}, CW_{max} und den aufgetretenen *in-range* Kollisionen k für eine sendewillige 802.11-Station nach der folgenden Gleichung berechnet werden (vgl. Walke et al., 2006, Seite 99):

$$CW_k = min((2^k \cdot (CW_{min} + 1)) - 1, CW_{max}) \tag{4.1}$$

Die minimale und maximale Backoff-Fenstergröße, CW_{min} und CW_{max}, werden im IEEE 802.11-Standard und dessen Erweiterungen IEEE 802.11a/b/g/n spezifiziert. Hierbei wird das Backoff-Fenster in Zeitschlitze (engl. Slots) aufgeteilt, wobei alle Zeitschlitze die selbe Dauer haben (vgl. IEEE Standard 802.11, 2012, Seite 836). Die Dauer eines Zeitschlitzes ist jedoch abhängig, ob der IEEE 802.11-Standard oder einer seiner Erweiterungen IEEE 802.11a/b/g/n verwendet wird, da Unterschiede zwischen diesen Standards existieren (vgl. IEEE Standard 802.11, 2012; IEEE Standard 802.11a, 1999; IEEE Standard 802.11b, 1999; IEEE Standard 802.11g, 2003 und IEEE Standard 802.11n, 2009). Aus diesem Grund werden für CW_{max} 1023 Zeitschlitze sowohl für den IEEE 802.11-Standard als auch für dessen Erweiterungen IEEE 802.11a/b/g/n spezifiziert. Wohingegen die Anzahl der Zeitschlitze für CW_{min} vom jeweiligem IEEE 802.11-Standard und dessen Erweiterungen IEEE 802.11a/b/g/n abhängt (vgl. IEEE Standard 802.11, 2012, Seite 1442-1780; IEEE Standard 802.11b, 1999, Seite 29; IEEE Standard 802.11a, 1999, Seite 40; IEEE Standard 802.11g, 2003, Seite 47 und IEEE Standard 802.11n, 2009, Seite 336).
Daher ist CW_{min} 31 Zeitschlitze, falls die sendewilligen 802.11-Stationen kompatibel zum IEEE 802.11- oder zum IEEE 802.11b-Standard sind oder sich im BSS-Gebiet sowohl sendewillige 802.11g/n-Stationen als auch sendewillige 802.11b-Stationen befinden. Ansonsten ist CW_{min} 15 Zeitschlitze, falls die sendewilligen 802.11-Stationen zum IEEE 802.11a- oder IEEE 802.11g/n-Standard kompatibel sind.

Hat die sendewillige 802.11-Station ihre aktuelle Backoff-Fenstergröße CW_k ermittelt, bestimmt dann der Backoff-Algorithmus zufällig für den Backoff B einen Zeitschlitz aus dem Intervall des Backoff-Fensters $[0, CW_k]$, um den die Rahmen-

übertragung verzögert wird; somit gilt: $B \in [0, CW_k]$ (vgl. IEEE Standard 802.11, 2012, Seite 836 - 837). Anschließend überprüft der Backoff-Algorithmus mit der Hilfe der Trägerprüfung, ob das drahtlose Medium frei ist.[2)]

Detektiert die Trägerprüfung das Medium als frei, beginnt für die sendewillige 802.11-Station die Konkurrenzphase um das drahtlose Medium. In der Konkurrenzphase verringert dann jede sendewillige 802.11-Station sukzessiv ihren Backoff B. Dieser Vorgang findet solange statt, bis entweder der Backoff abgelaufen (B $= 0$) ist oder die Trägerprüfung das Medium als belegt detektiert.[3)]

Detektiert die Trägerprüfung der sendewilligen 802.11-Station das Medium als belegt, verringert der Backoff-Algorithmus den Backoff nicht weiter, sondern hält diesen an. Mit der Verringerung des Backoffs fährt der Backoff-Algorithmus erst weiter fort, wenn die Trägerprüfung der sendewilligen 802.11-Station das Medium wieder als frei detektiert. Dieser Vorgang wird solange wiederholt bis der Backoff der sendewilligen 802.11-Station abgelaufen ist.[4)]
Nachdem der Backoff der sendewilligen 802.11-Station abgelaufen ist, wird der zu sendende Rahmen von der MAC-Schicht an die Bitübertragungsschicht weitergegeben. Daraufhin überträgt die Bitübertragungsschicht der sendewilligen 802.11-Station den Rahmen zur empfangenden 802.11-Station (siehe Abbildung 1).

Wenn nun mindestens zwei oder mehrere sendewillige 802.11-Stationen den gleichen Backoff B haben, kommt es zur *inrange* Kollision (siehe Kapitel 3.1), da der positive Bestätigungsrahmen (ACK) von der empfangenden an die sendende 802.11-Station ausbleibt. Deshalb ist die Rahmenübertragung zwischen sendender und empfangender 802.11-Station fehlgeschlagen und jede sendewillige 802.11-Station, die an der *inrange* Kollision beteiligt gewesen ist, muss einen erneuten Übertragungsversuch für ihren aktuellen Rahmen unternehmen.
Ist die Übertragung des Rahmens zwischen sendender und empfangender 802.11-Station erfolgreich, wird die Backoff-Fenstergröße CW_k auf seinen minimalen Startwert CW_{min} zurückgesetzt. Nachdem das Backoff-Fenster auf CW_{min} zurückgesetzt worden ist, beginnt der Backoff-Algorithmus einen neuen Rahmen nach dem oben

[2)] siehe Abbildung 5
[3)] siehe Abbildung 5
[4)] siehe Abbildung 5

beschriebenen Verfahren zu übertragen.

Das Zurücksetzen des Backoff-Fensters auf CW_{min} ist notwendig, damit zwischen den sendewilligen 802.11-Stationen, die um das gemeinsame, drahtlose Medium konkurrieren, Fairness hinsichtlich des Zugriffes auf das Medium erreicht wird (vgl. Bharghavan et al., 1994). Dadurch finden zwar mehr Kollisionen zwischen den sendewilligen 802.11-Stationen statt. Aber jede sendewillige 802.11-Stationen erhält die selben Startbedingungen, da Fairness nur erreicht werden kann, wenn alle sendewilligen 802.11-Stationen die selbe Backoff-Fenstergröße zur Rahmenübertragung verwenden (vgl. Bharghavan et al., 1994).

Sei nun zusätzlich zur sendewilligen 802.11-Station eine endliche Anzahl von sendewilligen 802.11-Nachbarstationen n im BSS-Gebiet der sendewilligen 802.11-Station vorhanden. Weiterhin stehen sowohl der sendewilligen 802.11-Station als auch deren 802.11-Nachbarstationen permanent Rahmen zur Übertragung zur Verfügung und deshalb operieren alle sendewilligen 802.11-Stationen unter gesättigten Bedingungen (vgl. Bianchi, 2000). Außerdem werden für das drahtlose Medium ideale Bedingungen vorausgesetzt und somit werden Paketfehler oder Paketverluste lediglich durch Kollisionen verursacht.

Unter diesen Voraussetzungen hat Bianchi (2000) das Verhalten des Backoff-Algorithmus (siehe Gleichung (4.1)) mit der Hilfe einer zwei-dimensionalen Markov-Kette modelliert. Dabei hat Bianchi (2000) die Abhängigkeit zwischen der Backoff-Fenstergröße und der Anzahl der sendewilligen 802.11-Stationen festgestellt, da sich bei konstanter Backoff-Fenstergröße und steigender Anzahl von sendewilligen 802.11-Stationen die Kollisionswahrscheinlichkeit p_c für eine *inrange* Kollision erhöht.

Allerdings berücksichtigt der Backoff-Algorithmus des IEEE 802.11-Standards die Anzahl der vorhandenen 802.11-Nachbarstationen und die Kollisionswahrscheinlichkeit der vorangegangenen Rahmenübertragung nicht unmittelbar, da nach jeder erfolgreichen Rahmenübertragung der Backoff-Algorithmus der sendewilligen 802.11-Station die Backoff-Fenstergröße CW_k wieder auf CW_{min} zurücksetzt. Aus diesem Grund werden zu Beginn jeder neuen Rahmenübertragung unnötige Kollisionen verursacht, bis die Backoff-Fenstergröße für eine erfolgreiche Rahmen-

übertragung zwischen sendewilliger und empfangender 802.11-Station erfolgt ist, die maximale Backoff-Fenstergröße erreicht worden ist oder der Rahmen von der sendewilligen 802.11-Station verworfen wird. Deshalb wird im Modell von Bianchi (2000) eine konstante und unabhängige Kollisionswahrscheinlichkeit vorausgesetzt.

Um nun unnötige Kollisionen zu vermeiden und um dadurch den Durchsatz zu erhöhen (vgl. Bianchi, 2000), sollte der Backoff-Algorithmus der sendewilligen 802.11-Station die Backoff-Fenstergröße entsprechend der Anzahl seiner sendewilligen 802.11-Nachbarstationen adaptieren. Damit eine Adaption der Backoff-Fenstergröße erreicht wird, berücksichtigt Kovar und Vít (2008) bei der Bestimmung der aktuellen Backoff-Fenstergröße CW_k die Anzahl der sendewilligen 802.11-Stationen n in einem BSS-Gebiet mit Hilfe des „klassischen“ Geburtstagsparadoxons (vgl. Treiber; Rohm; Unterrainer und Rohm).
Das „klassische“ Geburtstagsparadoxon geht auf die folgende Fragestellung ein:

- „Gesucht ist die Wahrscheinlichkeit p(n), dass von n Personen mindestens 2 am selben Tag geboren sind (das Jahr nicht berücksichtigt)“ (Rohm)

Übertragt man die obige Fragestellungen auf die Anzahl der Kollisionen in einem BSS-Gebiet, ergibt sich die folgende Fragestellung:

- Gesucht wird die Kollisionswahrscheinlichkeit p_c, dass von n Stationen mindestens 2 miteinander kollidieren.

Dadurch ergibt sich nach dem „klassischem Geburtstagsparadoxon“ die folgende geschlossene Gleichung zur Berechnung der Kollisionswahrscheinlichkeit p_c im Falle von *inrange* Kollisionen (vgl. Kovar und Vít, 2008):

$$p_c(n, CW_k) = 1 - \prod_{i=0}^{n} \frac{CW_k - i}{CW_k} \tag{4.2}$$

Somit kann mit der Hilfe von Gleichung (4.2) für eine bestimmte Kollisionswahrscheinlichkeit p_c und einer bestimmten Anzahl von 802.11-Nachbarstationen n, die Backoff-Fenstergröße CW_k für die sendewillige 802.11-Station unter gesättig-

ten Bedingungen berechnet werden.

Das Problem von Gleichung (4.2) ist, dass die Backoff-Fenstergröße CW_k für eine bestimmte Anzahl von 802.11-Nachbarstationen n und einer bestimmten Kollisionswahrscheinlichkeit p_c im Voraus berechnet werden muss und anschließend jede sendewillige 802.11-Station eine statische Tabelle zum Nachschlagen der jeweiligen Backoff-Fenstergröße mitführen muss. Um dies zu vermeiden, wird die Gleichung (4.2) durch

$$1 - x \approx e^{-x} \tag{4.3}$$

approximiert (siehe Treiber). Die Approximation (4.3) ist für $x = \frac{n}{CW_k}$ erfüllt, wenn x klein ist (vgl. Treiber). Aus diesem Grund erhält man durch Gleichung (4.2) unter Verwendung der Approximation (4.3) und der Gaußschen Summenformel:

$$p_c(n, CW_k) \geq 1 - e^{-\frac{n \cdot (n+1)}{2 \cdot CW_k}} \tag{4.4}$$

Durch Auflösen der Ungleichung (4.4) nach der Backoff-Fenstergröße (CW_k) erhält man schließlich:

$$CW_k \geq (-1) \cdot \frac{n \cdot (n+1)}{2 \cdot ln(1 - p_c(n, CW_k))} \tag{4.5}$$

Daher kann man anstatt einer statischen Tabelle die Gleichung (4.5) für die Berechnung der aktuellen Backoff-Fenstergröße CW_k für das „klassische“ Geburtstagsparadoxon verwenden.
Außerdem existiert neben dem „klassischen“ Geburtstagsparadoxon noch das „intuitive“ Geburtstagsparadoxon (vgl. Rohm; Unterrainer und Rohm).
Dabei geht das „intuitive“ Geburtstagsparadoxon auf die folgende Fragestellung ein:

- „Wie groß ist die Wahrscheinlichkeit, dass von n Personen mindestens eine denselben Geburtstag wie „ich“ (bzw. eine bestimmte Person) hat?“ (Rohm)

Übertragt man die obige Fragestellung für das „intuitive“ Geburtstagsparadoxon auf die Kollisionen innerhalb eines BSS-Gebietes, ergibt sich folgende Fragestellung:

- Wie groß ist die Kollisionswahrscheinlichkeit p_c, dass von n Stationen min-

destens eine einmal mit mir kollidiert?

Somit ergibt sich die folgende geschlossene Gleichung zur Berechnung der Kollisionswahrscheinlichkeit p_c im Falle des „intuitiven“ Geburtstagsparadoxons für *in-range* Kollisionen (vgl. Rohm und Unterrainer und Rohm):

$$p_c(n, CW_k) = 1 - \left(\frac{CW_k - 1}{CW_k}\right)^n \tag{4.6}$$

Hierbei gilt für die Gleichung (4.6) $CW_k > 0$.
Stellt man nun Gleichung (4.6) nach CW_k um, erhält man für die Backoff-Fenstergröße folgende geschlossene Gleichung:

$$CW_k = \frac{1}{1 - \sqrt[n]{1 - p_c(n, CW_k)}} \tag{4.7}$$

Hierbei gilt für Gleichung (4.7) $p_c(n, CW_k) > 0$. Außerdem wird CW_k im Folgenden für die beiden Approximationsgleichungen (4.5) und (4.7) aufgerundet, da für $CW_k \in \mathrm{N}_0$ gilt.

4.2. RTS/CTS und CTS-to-self

Ein weiteres Problem ist das versteckte Knotenproblem (siehe Kapitel 3.1), da die sendenden 802.11-Stationen das CSMA/CA-Protokoll mit binärem Backoff-Algorithmus verwenden (vgl. IEEE Standard 802.11, 2012, Seite 824ff).

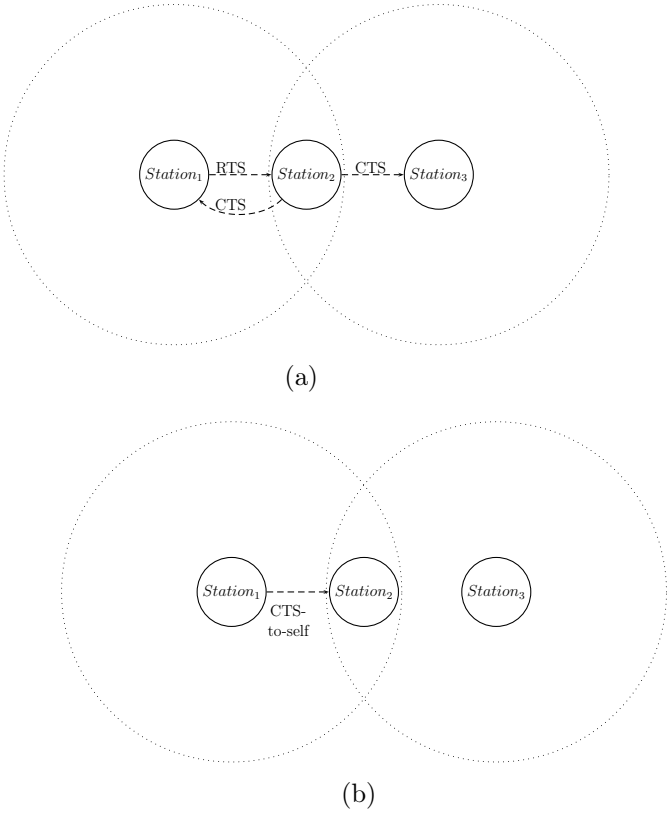


Abbildung 6: *RTS/CTS-Mechanismus (a) und CTS-to-self(b)*

Das versteckte Knotenproblem ereignet sich wegen der begrenzten Reichweite der physikalischen Trägerprüfung (siehe Kapitel 3.1). Um diesen Mangel zu beheben, ist neben der physikalischen Trägerprüfung für die MAC-Schicht die virtuelle Trägerprüfung spezifiziert worden (vgl. IEEE Standard 802.11, 2012, Seiten 825ff). Die virtuelle Trägerprüfung findet mit der Hilfe eines Zeitgebers statt, der als Netzbelegungsvektor (engl. Network Allocation Vector; NAV) bezeichnet wird (vgl. IEEE Standard 802.11, 2012, Seite 825 und Tannenbaum, 2003, Seite 332). Somit gibt der Netzbelegungsvektor an, für welchen Zeitraum eine sendende 802.11-Station

das Medium belegen wird. Daher wird der Netzbelegungsvektor, der von einem Startwert ausgeht, sukzessiv verringert bis dieser abgelaufen ist. Anschließend detektiert die virtuelle Trägerprüfung das Medium wieder als frei. Damit eine sendende und eine empfangende 802.11-Station das Medium für die Rahmenübertragung mittels des Netzbelegungsvektors reserviert, verwendet die sendende und empfangende 802.11-Station den RTS/CTS-Mechanismus (vgl. IEEE Standard 802.11, 2012, Seite 824). Dieser Mechanismus basiert auf einer Modifikation des MACAW-Protokolls (vgl. Bharghavan et al., 1994 und Ray et al.) und wird in Abbildung 6(a) dargestellt.

Beim RTS/CTS-Mechanismus überträgt eine sendende 802.11-Station ($Station_1$) zunächst einen RTS-Rahmen zur empfangenden 802.11-Station ($Station_2$), indem die sendende 802.11-Station den RTS-Rahmen mit der Hilfe des CSMA/CA-Verfahrens und des binären Backoff-Mechanismus an die empfangende 802.11-Station überträgt. Hat die empfangende 802.11-Station diesen Rahmen fehlerhaft oder aufgrund von Kollisionen nicht erhalten, wiederholt die sendende 802.11-Station die Übertragung des RTS-Rahmens (vgl. IEEE Standard 802.11, 2012, Seite 824). Ist jedoch der RTS-Rahmen von der empfangenden 802.11-Station fehlerfrei empfangen worden, bestätigt die empfangende 802.11-Station der sendewilligen 802.11-Station mit der Hilfe eines CTS-Rahmens die Reservierung des Mediums für dessen Rahmenübertragung (vgl. IEEE Standard 802.11, 2012, Seite 824ff). Nach der Reservierung des Mediums durch die sendende und empfangende 802.11-Station findet die Übertragung des Rahmens zur empfangenden 802.11-Station statt.

Durch dieses Konzept verteilt die sendende 802.11-Station ($Station_1$) mit der Übertragung des RTS-Rahmens die benötigte Zeit für seine Rahmenübertragung in seiner Umgebung, da das drahtlose Medium ein Broadcast-Medium ist (siehe Kapitel 2).[5)] Empfängt eine der 802.11-Nachbarstation der sendenden 802.11-Station einen RTS-Rahmen, müssen die 802.11-Nachbarstationen ihren Netzbelegungsvektor entsprechend einstellen (vgl. IEEE Standard 802.11, 2012, Seite 824). Dadurch werden Kollisionen mit der sendenden 802.11-Station vermieden

[5)] Zur Vereinfachung sind jedoch lediglich die wichtigsten Übertragungswege in Abbildung 6 dargestellt

(vgl. IEEE Standard 802.11, 2012, Seite 824). Der selbe Vorgang wird auch bei der empfangenden 802.11-Station ($Station_2$) durchgeführt, indem die empfangende 802.11-Station durch die Übertragung des CTS-Rahmens seinen 802.11-Nachbarstationen ($Station_3$) mitteilt, wie lange die Rahmenübertragung der sendenden 802.11-Station dauern wird. Somit ist das Medium für die Rahmenübertragung zwischen der sendenden und der empfangenden 802.11-Station reserviert worden, indem sowohl die 802.11-Nachbarstationen der sendenden als auch der empfangenden 802.11-Stationen ihren Netzbelegungsvektor eingestellt haben, wobei die Zugehörigkeit der 802.11-Nachbarstationen zu unterschiedlichen BSS (siehe Kapitel 2) bei der Einstellung ihres Netzbelegungsvektors nicht relevant ist (vgl. IEEE Standard 802.11, 2012, Seite 824). Dadurch verzögern die 802.11-Nachbarstationen für die Dauer der Rahmenübertragung zwischen sendender und empfangender 802.11-Station ihre eigene Rahmenübertragung, obwohl die physikalische Trägerprüfung einiger 802.11-Nachbarstationen in der Umgebung der empfangenden 802.11-Stationen das Medium als frei detektieren.

Deshalb wird das versteckte Knotenproblem vermindert, da die virtuelle Trägerprüfung der 802.11-Nachbarstationen in der Umgebung der sendewilligen und der empfangenden 802.11-Station das Medium als belegt detektieren, sofern die jeweiligen 802.11-Nachbarstationen den RTS- oder CTS-Rahmen empfangen haben. Es kann aber sein, dass eine 802.11-Nachbarstation, die sich in Kommunikationsreichweite der empfangenden 802.11-Station befindet, während der RTS/CTS-Übertragung zwischen sendender und empfangender 802.11-Station selbst Rahmen zu einer weiteren empfangenden 802.11-Station übertragen hat (vgl. Bharghavan et al., 1994). Dadurch ist der Netzbelegungsvektor dieser 802.11-Nachbarstation für die bevorstehende Rahmenübertragung zwischen der sendewilligen und der empfangenden 802.11-Station nicht entsprechend angepasst worden. Daher treten trotz RTS/CTS-Rahmenübertragung Kollisionen auf und somit werden Kollisionen beim versteckten Knotenproblem durch den RTS/CTS-Mechanismus lediglich reduziert.

Außerdem kann die virtuelle Trägerprüfung der empfangenden 802.11-Station das Medium als belegt detektieren, obwohl die sendewillige 802.11-Station einen RTS-Rahmen fehlerfrei zur empfangenden 802.11-Station übertragen hat; folglich wird

die empfangende 802.11-Station durch die virtuelle Trägerprüfung blockiert und überträgt somit keinen CTS-Rahmen zur sendewilligen 802.11-Station (vgl. IEEE Standard 802.11, 2012, Seite 831; Bharghavan et al., 1994 und Ray et al.). Somit nimmt die sendewillige 802.11-Station eine Kollision des RTS-Rahmens an und versucht diesen erneut mit vergrößertem Backoff-Fenster zu übertragen (siehe Kapitel 4.1).

Weiterhin kann der RTS/CTS-Mechanismus sowohl gegen das versteckte Knotenproblem als auch gegen *inrange* Kollisionen verwendet werden (vgl. Bruno et al., 2002). Hierbei ist zu beachten, dass der RTS/CTS-Mechanismus durch die Übertragung der RTS- und CTS-Rahmen zwischen sendender und empfangender 802.11-Station einen *Overhead* erzeugt, der lediglich bei einer großen Anzahl von 802.11-Nachbarstationen eine Erhöhung des Durchsatzes gegenüber dem CSMA/CA-Verfahren zur Folge hat (vgl. Bruno et al., 2002 und Chatzimisios et al., 2004).

Ist nämlich der zu sendende Rahmen kleiner als der *Overhead* des RTS/CTS-Mechanismus, vergrößert sich bei einer Kollision der *Overhead* unnötigerweise. Bei großen Rahmen entsteht jedoch im Falle einer Kollision eine höhere Latenz als wenn RTS-Rahmen miteinander kollidieren, da erst am Ende einer Rahmenübertragung die sendende 802.11-Station durch das Ausbleiben der positiven Bestätigung eine Kollision schlussfolgern kann (vgl. Wu et al., 2002). Deshalb sollten große Rahmen vor ihrer Übertragung mit dem RTS/CTS-Mechanismus abgesichert werden, da eine erneute Übertragung im Falle einer Kollision eine geringere Latenz verursacht.

Um den *Overhead* des RTS/CTS-Mechanismus zu reduzieren, ist neben dem RTS/CTS-Mechanismus zur Reservierung des Mediums der CTS-to-self-Mechanismus im IEEE 802.11-Standard spezifiziert worden (vgl. IEEE Standard 802.11, 2012, Seite 405). Beim CTS-to-self-Mechanismus überträgt die sendewillige 802.11-Station einen CTS-Rahmen an seine 802.11-Nachbarstationen. Dies hat eine Reservierung des Mediums zur Folge, wobei der CTS-Rahmen als Empfänger-Adresse die MAC-Adresse der sendewilligen 802.11-Station hat. Deshalb wird dieser CTS-Rahmen auch als CTS-to-self bezeichnet (vgl. IEEE Standard 802.11, 2012, Seite 405). Der Vorteil des CTS-to-self-Mechanismus ist der geringere *Overhead* im Vergleich zum

RTS/CTS-Mechanismus, da der RTS-Rahmen von der sendenden 802.11-Station übertragen werden muss und anschließend diese auf den CTS-Rahmen der empfangenden 802.11-Station warten muss.

Außerdem kann sowohl der RTS/CTS-Mechanismus als auch der CTS-to-self-Mechanismus in Umgebungen eingesetzt werden, in denen 802.11b- und 802.11g-Stationen zur gleichen Zeit vorhanden sind (siehe Kapitel 3.2). Hierbei ist die physikalische Trägerprüfung der 802.11b-Stationen nicht in der Lage sendende 802.11g-Stationen zu detektieren, da sendende 802.11g-Stationen ein für 802.11b-Stationen unbekanntes Modulationsverfahren verwenden. Somit nehmen 802.11b-Stationen das Medium als frei an und versuchen ihren Rahmen zu übertragen. Daher kollidiert die Rahmenübertragung der 802.11b-Station mit der Rahmenübertagung der 802.11g-Station. Um dies zu vermeiden, können 802.11g-Stationen entweder mit dem RTS/CTS- oder CTS-to-self-Mechanismus ihre Rahmenübertragung absichern, indem sie für die benötigte Rahmenübertragungszeit das Medium für sich reservieren (vgl. Wang et al.). Zusätzlich zum RTS/CTS- und zum CTS-to-self-Mechanismus stellt auch der MAC-Rahmen ein Feld für dessen benötigte Übertragungszeit von der sendenden zur empfangenden 802.11-Station zur Verfügung (vgl. IEEE Standard 802.11, 2012, Seite 824). Es wird jedoch im IEEE 802.11-Standard empfohlen lediglich den RTS/CTS- oder den CTS-to-self-Mechanismus zur Reservierung des Mediums zu verwenden (vgl. IEEE Standard 802.11, 2012, Seite 836).

Das Problem des CTS-to-self-Mechanismus ist, dass dieser Mechanismus zum Einen nicht das versteckte Knotenproblem berücksichtigt (vgl. Wang et al.) und zum Anderen nicht gegen *inrange* Kollisionen abgesichert ist, wie dies beim RTS/CTS-Mechanismus der Fall ist (vgl. IEEE Standard 802.11, 2012, Seite 836). Jedoch kann sowohl der RTS/CTS- als auch der CTS-to-self-Mechanismus von 802.11-Stationen manipuliert werden, indem diese sowohl die RTS- als auch die CTS-Rahmen mit maximaler Zeit an nicht existierende 802.11-Stationen übertragen (vgl. Chen et al.). Daraufhin müssen alle 802.11-Nachbarstationen entsprechend ihren Netzbelegungsvektor einstellen und erhalten somit keinen weiteren Zugriff auf das drahtlose Medium, da die virtuelle Trägerprüfung das Medium als belegt detektiert.

4.3. Fragmentierung

Ein weiterer Mechanismus um Paketfehler zu reduzieren ist die Fragmentierung. Beim Fragmentieren wird der zu sendende Rahmen in einzelne Rahmenfragmente mit einheitlicher Größe zerlegt, mit Ausnahme des letzten Rahmens, der auch kleiner sein kann. Anschließend werden alle Rahmenfragmente von der sendenden zur empfangenden 802.11-Station übertragen (vgl. IEEE Standard 802.11, 2012, Seite 822-823). Danach fügt die empfangende 802.11-Station die einzelnen Rahmenfragmente wieder zum Rahmen, wie dieser vor der Fragmentierung gewesen ist, zusammen. Anschließend wird der wieder zusammengesetzte Rahmen an die höhere Schicht weitergegeben, sofern keine Paketfehler aufgetreten sind. Dieser Vorgang wird als Defragmentierung bezeichnet (vgl. IEEE Standard 802.11, 2012, Seite 822-823).

Der Vorteil der Fragmentierung durch die sendewillige 802.11-Station ist die Reduzierung der Paketfehlerwahrscheinlichkeit unter der Annahmen, dass sich die Bitfehlerwahrscheinlichkeit des drahtlosen Mediums nicht verändert. Somit werden durch die Fragmentierung lediglich kleine Rahmen zerstört (vgl. Schiller, 2003, Seite 219) und die Zuverlässigkeit der Paketübertragung erhöht sich (vgl. IEEE Standard 802.11, 2012, Seite 822-823). Aus diesem Grund verringert sich bei einer erneuten Rahmenübertragung durch die Fragmentierung sowohl im Falle eines Paketfehlers als auch bei einer Kollision der *Overhead* (vgl. Perahia und Stacey, 2008, Seite 190).

Wenn die sendende 802.11-Station jedes Rahmenfragment der Rahmenfolge unabhängig voneinander zur empfangenden 802.11-Station überträgt (vgl. IEEE Standard 802.11, 2012, Seite 822-823), entsteht durch das CSMA/CA-Verfahren und dem Backoff-Algorithmus eine hohe Latenz, da nach jeder Rahmenfragment-Übertragung die sendende 802.11-Station einen neuen Backoff bestimmt und erneut um das drahtlose Medium mit seinen sendewilligen 802.11-Nachbarstationen konkurrieren muss. Damit diese Latenz reduziert wird, kann die sendende 802.11-Station die einzelnen Rahmenfragmente als eine Rahmenfolge zur empfangenden 802.11-Station übertragen (vgl. IEEE Standard 802.11, 2012, Seite 840-842). Hierbei muss die sendewillige 802.11-Station lediglich mit seinen sendewilligen 802.11-Nachbarstationen

um die fehlerfreie Übertragung des ersten Rahmenfragmentes der Rahmenfolge konkurrieren.

Hat die sendende 802.11-Station die Konkurrenzphase gegenüber seinen sendewilligen 802.11-Nachbarstationen gewonnen und somit sein erstes Rahmenfragment der Rahmenfolge erfolgreich zur empfangenden 802.11-Station übertragen, kann die sendende 802.11-Station das nächste Rahmenfragment übertragen (vgl. IEEE Standard 802.11, 2012, Seite 840-842). Dies hat den Vorteil, dass die sendende 802.11-Station bei der Übertragung der einzelnen Rahmenfragmente der Rahmenfolge nicht mehr mit seinen sendewilligen 802.11-Nachbarstationen um den Zugriff auf das Medium konkurrieren muss, bis die Rahmenfolge komplett erfolgreich übertragen worden ist (vgl. IEEE Standard 802.11, 2012, Seite 840-842). Dies ist möglich, da die sendende 802.11-Station die einzelnen Rahmenfragmente in einem kürzen Zeitabstand zur empfangenden 802.11-Station überträgt als die physikalische Trägerprüfung der 802.11-Nachbarstationen im BSS-Gebiet der sendenden 802.11-Station das Medium wieder als frei detektiert (vgl. IEEE Standard 802.11, 2012, Seiten 828; 838).

Das Problem beim Austausch von Rahmenfragmenten und positivem Bestätigungsrahmen ist die Rahmenfragment-Übertragung des ersten Rahmenfragmentes in der Rahmenfolge, da es zu *inrange* Kollisionen kommen kann. Dies verursacht wiederum bei der sendenden 802.11-Station eine erneute Übertragung des ersten Rahmenfragments der Rahmenfolge, indem die sendewillige 802.11-Station erneut einen Backoff bestimmen und mit seinen 802.11-Nachbarstationen um das drahtlose Medium konkurrieren muss (vgl. IEEE Standard 802.11, 2012, Seite 840 - 842). Zudem kann es während der Übertragung der Rahmenfragmente zwischen sendender und empfangender 802.11-Station zum versteckten Knotenproblem kommen (siehe Kapitel 4.2). Dies verursacht bei der sendenden 802.11-Station wieder eine erneute Übertragung der Rahmenfragment ab dem fehlgeschlagenen Rahmenfragment bis zum Ende der Rahmenfolge.

Außerdem ist ein drittes Verfahren zur Abschwächung des versteckten Knotenproblems im IEEE 802.11-Standard spezifiziert worden. Bei diesem Verfahren reservieren zuerst die sendende und empfangende 802.11-Station mit dem RTS/CTS-

Mechanismus das drahtlose Medium für die Übertragung des ersten Rahmenfragmentes der Rahmenfolge (vgl. IEEE Standard 802.11, 2012, Seite 829-830). Hierbei kann es bei der Übertragung des RTS-Rahmens zu *inrange* Kollisionen und zum versteckten Knotenproblem kommen. Dadurch wird für die erneute Übertragung des RTS-Rahmens ein neuer Backoff bestimmt und die sendewillige 802.11-Station muss erneut mit seinen sendewilligen 802.11-Nachbarstationen wieder um den Zugriff auf das drahtlose Medium konkurrieren. Hat jedoch die sendewillige und die empfangende 802.11-Station das drahtlose Medium mit dem RTS/CTS-Mechanismus reserviert und ist das erste Rahmenfragment der Rahmenfolge erfolgreich von der sendenden zur empfangende 802.11-Station übertragen worden, ist das Medium für die Dauer des zweiten Rahmenfragments sowohl von der sendenden als auch von der empfangenden 802.11-Station reserviert worden.

Hierbei enthält das erste Rahmenfragment die benötigte Zeit für die Übertragung des eigenen Rahmenfragmentes inklusive des positiven Bestätigungsrahmens als auch die benötigte Zeit für das nächste Rahmenfragment und dessen positiven Bestätigungsrahmen. Somit reserviert die sendende 802.11-Station in seiner Umgebung durch die erfolgreiche Übertragung des ersten Rahmenfragmentes das Medium für seine als auch für die nächste Rahmenfragment-Übertragung, da alle 802.11-Nachbarstationen ihren Netzbelegungsvektor entsprechend einstellen müssen (vgl. IEEE Standard 802.11, 2012, Seite 824).

Durch die erfolgreiche Übertragung des ersten Rahmenfragmentes von der sendenden zur empfangenden 802.11-Station, erhält auch die empfangende 802.11-Station zusätzlich zur Dauer der aktuellen Rahmenfragment-Übertragung die Dauer für das zweite Rahmenfragment inklusive dessen positiven Bestätigungsrahmens (vgl. IEEE Standard 802.11, 2012, Seite 824; 829). Daraufhin überträgt die empfangende 802.11-Station mit der Hilfe seines positiven Bestätigungsrahmens die Dauer für das zweite Rahmenfragment und dessen positiven Bestätigungsrahmen zur sendenden 802.11-Station. Dadurch verteilt die empfangende 802.11-Station die Dauer des zweiten Rahmenfragmentes inklusive dessen positiven Bestätigungsrahmens an ihre 802.11-Nachbarstationen, wobei die 802.11-Nachbarstationen der empfangenden 802.11-Station ebenfalls entsprechend ihren Netzbelegungsvektor einstellen. Somit reserviert der Austausch von Rahmenfragmenten und positivem Bestäti-

gungsrahmen zwischen sendender und empfangender 802.11-Station das Medium für die nächste Rahmenfragment-Übertragung bis zum letzten Rahmenfragment der Rahmenfolge. Nach der erfolgreichen Übertragung des letzten Rahmenfragmentes gibt die sendende 802.11-Station das Medium wieder frei, indem das letzte Rahmenfragment lediglich die Dauer der aktuellen Rahmenfragment-Übertragung enthält. Daraufhin gibt auch die empfangende 802.11-Station in ihrer Umgebung das Medium wieder frei, indem der positive Bestätigungsrahmen keine weiteren Zeitangaben enthält. Aus diesem Grund verhält sich der Austausch von Rahmenfragmenten und positivem Bestätigungsrahmen wie der RTS/CTS-Mechanismus (vgl. IEEE Standard 802.11, 2012, Seite 829). Hierbei ist anzumerken, dass sowohl für die Übertragung der Rahmenfragment-Folge als auch durch die Reservierung des Mediums durch den RTS/CTS-Mechanismus zu Kollisionen kommen kann. Wird ein Rahmenfragment fehlerhaft übertragen oder kommt es zum Rahmenverlust, muss die sendende 802.11-Station dieses Rahmenfragment erneut übertragen, indem diese für dieses Rahmenfragment einen neuen Backoff bestimmt und mit ihren sendewilligen 802.11-Nachbarstationen erneut um das drahtlose Medium konkurriert.

4.4. Ratenanpassung

Ein weiteres Hauptziel des IEEE 802.11-Standards und dessen Erweiterungen IEEE 802.11a/b/g/n ist neben den Mechanismen zur Verringerung von *inrange* Kollisionen und verstecktem Knotenproblem die Erhöhung der Datenrate zwischen sendender und empfangender 802.11-Station. Durch die Erhöhung der Datenrate soll sich der Durchsatz zwischen sendender und empfangender 802.11-Station erhöhen. Aus diesem Grund sind im IEEE 802.11-Standard und dessen Erweiterungen IEEE 802.11a/b/g/n verschiedene Kodierungs- und Modulationsverfahren spezifiziert worden. Hierbei ist das Problem, dass um so höher die Datenrate ist, desto höher sind die Anforderungen an das Signal-Rausch-Verhältnis, damit die empfangende 802.11-Station den Rahmen fehlerfrei dekodieren kann (vgl. Gast, 2005, Seite 7 und Kim et al., 2005). Zudem verringert sich durch die höheren Anforderungen an das Signal-Rausch-Verhältnis zwischen sendender und empfangender 802.11-Station die Reichweite der sendenden 802.11-Station für dessen Rah-

menübertragung (vgl. Gast, 2005, Seite 7). Damit aber die sendewillige 802.11-Station die maximale Datenrate in Abhängigkeit von den Kanalbedingungen des drahtlosen Mediums und des Signal-Rausch-Verhältnisses erzielt, können zwei verschiedene Mechanismen verwendet werden. Zum Einen kann im Fall von mobilen 802.11-Stationen entweder die Entfernung zwischen sendender und empfangender 802.11-Station verringert werden oder zum Anderen kann die Datenrate wie im Fall von statischen 802.11-Stationen entsprechend den Kanalbedingungen angepasst werden (vgl. Gast, 2005, Seite 7). Allerdings ist weder im IEEE 802.11-Standard noch in einen seiner Erweiterungen IEEE 802.11a/b/g/n ein Algorithmus zur Anpassung der Datenrate spezifiziert worden. Deshalb werden in der Literatur einige Verfahren vorgestellt, die sich darin unterscheiden, ob die Entscheidung für die ausgewählte Datenrate durch die sendewillige 802.11-Station oder durch die empfangende 802.11-Station erfolgt und welche Metriken für die Entscheidungsfindung verwendet werden. Dies ist für die Konformität mit dem IEEE 802.11-Standard wichtig, da eine Entscheidungsfindung der Datenrate durch die empfangende 802.11-Station zur Folge hat, dass die empfangende 802.11-Station der sendewilligen 802.11-Station die Datenrate für den nächsten Rahmen mitteilen muss, die dann die sendewillige 802.11.Station für die Rahmenübertragung verwendet. Zudem steht der MAC-Schicht der sendewilligen 802.11-Station für dessen Entscheidungsfindung nicht die Metriken der physikalischen Schicht, wie z. B. die empfangende Signalstärke (engl. Received Signal-Strength Indicator; RSSI), Signal-Rausch-Verhältnis (engl. Signal-To-Noise-Ratio; SNR) oder Rahmenfehlerrate (Frame Error Rate; FER), zur Verfügung. Um diese Metriken zu Verwenden ist eine Modifikation der MAC- und der physikalischen Schicht notwendig. Daher sind diese Verfahren nicht mit dem IEEE 802.11-Standard konform. Außerdem ist es nach Zhang et al. (2010) wichtig, zwischen Verfahren zur Ratenanpassung zu unterscheiden, die lediglich in kollisionsfreien oder in kollisionsbehafteten oder in beiden Umgebungen für die Rahmenübertragung zwischen sendender und empfangender 802.11-Station die maximale Datenrate in Abhängigkeit von den Kanalbedingungen des drahtlosen Mediums erreichen. Somit ist es die Aufgabe des Ratenanpassungs-Mechanismus zum Einen in Abhängigkeit der aktuellen Kanalbedingungen des drahtlosen Mediums die maximale Datenrate für die Rahmenübertragung zwischen sendender und empfangender 802.11-Station zu ermitteln und zu verwenden und zum Anderen konform zum IEEE 802.11-Standard zu

sein.

Kommt es zwischen sendender und empfangender 802.11-Station wegen der Degradierung der Übertragungsbedingungen des drahtlosen Mediums zu Paketfehlern oder Paketverlusten, ist das Signal-Rausch-Verhältnis der aktuellen Datenrate nicht mehr ausreichend. Deshalb ist eine fehlerfrei Dekodierung des übertragenen Rahmens durch die empfangende 802.11-Station nicht mehr möglich. Somit muss der Raten-Anpassungsmechanismus zu einer niedrigeren Datenrate wechseln, um die Anforderungen an das Signal-Rausch-Verhältnis zu verringern. Dies hat zwar durch die Verringerung der Datenrate eine längere Übertragungszeit des Rahmens von der sendenden zur empfangenden 802.11-Station zur Folge, jedoch werden Paketfehler und Paketverluste reduziert. Die Verringerung der Datenrate durch den Raten-Anpassungsmechanismus ist in kollisionsfreien Umgebungen erforderlich, allerdings kann es in kollisionsbehafteten Umgebungen aufgrund von *inrange* Kollisionen oder dem versteckten Knotenproblem ebenfalls zu Paketfehlern oder Paketverlusten kommen. Daher würde sich im Falle von *inrange* Kollisionen der Overhead bei einer erneuten Rahmenübertragung durch die sendende 802.11-Station vergrößern, da eine Verringerung der Datenrate eine Vergrößerung der Rahmenübertragungszeit zwischen sendender und empfangender 802.11-Station zur Folge hat. Zudem kann eine sendende 802.11-Station eine Kollision erst am Ende der Rahmenübertragung durch das Ausbleiben des positiven Bestätigungsrahmens von der empfangenden 802.11-Station detektieren. Im Falle einer Kollision durch versteckte Knoten erhöht sich die Kollisionswahrscheinlichkeit zwischen sendender 802.11-Station und der versteckten 802.11-Station durch die Verringerung der Datenrate durch die sendende 802.11-Station. Dadurch erhöht sich sowohl bei *inrange* Kollisionen als auch beim versteckten Knotenproblem die Wahrscheinlichkeit für Paketfehler und Paketverluste. Dadurch verringert sich der Durchsatz zwischen sendender und empfangender 802.11-Station. Aus diesem Grund muss der Raten-Anpassungsmechanismus zwischen Paketfehlern oder Paketverlusten unterscheiden, die sich aufgrund von Degradierungen der Übertragungsbedingungen des drahtlosen Mediums oder wegen Kollisionen ereignet haben. Natürlich soll auch der Raten-Anpassungsmechanismus die Datenrate wieder erhöhen, wenn sich die Kanalbedingungen des drahtlosen Mediums verbessert haben und somit das Signal-Rausch-Verhältnisses für höhere Datenraten ausreichend ist.

Weiterhin ist anzumerken, dass bei der Verwendung des RTS/CTS-Mechanismus nach dem IEEE 802.11-Standard eine Datenrate verwendet werden soll, die jede 802.11-Station, die sich innerhalb des BSS-Gebietes (siehe Kapitel 2) befindet erreicht. Somit stellt jede 802.11-Station innerhalb des BSS-Gebietes durch den RTS/CTS-Mechanismus ihren Netzbelegungsvektor entsprechend ein (vgl. IEEE Standard 802.11, 2012, Seite 918). Außerdem kann die Kombination von RTS/CTS-Mechanismus (siehe Kapitel 4.2) und Fragmentierung in Abhängigkeit zur Datenrate den möglichen maximalen Durchsatz verringern, da alle Rahmenfragmente nach dem IEEE 802.11-Standard die gleiche Größe haben, die unabhängig von der Datenrate ist. Deshalb kann es sein, dass die sendewillige 802.11-Station das Medium entweder durch den RTS/CTS-Mechanismus oder durch den Austausch von Rahmenfragment und positiver Bestätigung für eine bestimmte Dauer, die abhängig von der Datenrate ist, reserviert hat. Verändern sich jedoch für die nächste Rahmenfragment-Übertragung die Kanalbedingungen des drahtlosen Mediums, indem das Signal-Rausch-Verhältnis eine höhere Datenrate zulässt, verkürzt sich die Zeit für die Rahmenfragment-Übertragung. Daher entsteht eine zeitliche Differenz zwischen der Dauer der Rahmenübertragung und der Reservierungsdauer für das Medium. Deswegen wird in Kim et al. (2005) eine dynamische Anpassung der Rahmenfragment-Größe in Abhängigkeit der Datenrate vorgeschlagen, vorausgesetzt, dass die Datenrate für die Rahmenfragment-Übertragung bekannt ist. Dadurch bleibt trotz höherer Datenrate die Übertragungszeit für das Rahmenfragment zwischen sendender und empfangender 802.11-Station konstant, wobei bei höheren Datenraten mehr Bits übertragen werden, da die Rahmenfragmente größer sind und somit der Durchsatz erhöht wird (vgl. Kim et al., 2005).

4.5. Zusammenfassung

In diesem Kapitel sind die Mechanismen der MAC-Schicht, wie der Backoff-Algorithmus (siehe Kapitel 4.1), RTS/CTS und CTS-to-Self (siehe Kapitel 4.2), Fragmentierung (siehe Kapitel 4.3) und Ratenanpassung (siehe Kapitel 4.4), ausführlich beschrieben worden. Neben diesen genannten Mechanismen der MAC-Schicht, sind noch im IEEE 802.11-Standard die Signalstärkenkontrolle, der Kanalwechsel und die

	Signalschwund	*inrange*	Kollisionen versteckte Knotenproblem	sonstige
Ratenanpassung	verringern	-	erhöhen	erhöhen
Backoff-Algorithmus	-	erhöhen	-	-
Signalstärken-kontrolle	erhöhen	verringern	erhöhen	erhöhen
Fragmentierung	-	verringern	verringern	verringern
Paket-Aggregation	-	verringern	verringern	verringern
RTS/CTS	-	an	an	-
CTS-to-Self	-	an	-	-
Kanalwechsel (Frequenz)	-	Ja	Ja	Ja
Block ACK				
Beacon-Intervall				
Kanal-Aggregation				
Short-Guard				

Tabelle 1: *IEEE 802.11-Mechanismen*

Aggregation[6)] von Paketen in der MAC-Schicht spezifiziert worden. Eine Übersicht über die Verhaltensweisen der einzelnen Mechanismen der MAC-Schicht für bestimmte Szenarien wird in Tabelle 5 dargestellt.

Hierbei sind die einzelnen Mechanismen abhängig von den Bedingungen des Übertragungskanals, die wiederum von dem Signal-Rausch-Verhältnis des Übertragungskanals und der Anzahl an sendewilligen 802.11-Stationen abhängig sind. Bei der Anzahl der sendewilligen 802.11-Stationen wird noch unterschieden, ob sich die sendewillige und die empfangende 802.11-Station sich im selben BSS-Gebiet befinden (*inrange* Kollisionen) oder ob sich die sendewillige 802.11-Station außerhalb des BSS-Gebietes befindet (verstecktes Knotenproblem). Ansonsten werden alle weiteren Kollisionen den „sonstigen“ Kollisionen zugeordnet.

[6)] siehe A-MSDU und A-MPDU des IEEE 802.11n-Standards

5. Implementierung

Die Click-Software wird vom Lehrstuhl für System Architektur[7)] der Humboldt Universität zu Forschungszwecken verwendet. Zum Einen läuft die Click-Software auf den 802.11-Stationen der HWL[8)]-Testumgebung (vgl. HWL Projekt) und zum Anderen wird die Click-Software zusammen mit dem Netzwerksimulator 2 (NS2) für Simulationen verwendet (vgl. Netzwerksimulator 2 Projekt und Issariyakul und Hossain, 2009). Deshalb ist die bestehende Click-Software, um die beiden Elemente „Tos2QueueMapper“ und „SetRTSCTS“ erweitert worden (siehe Kapitel 5.1). Außerdem ist zusätzlich ein Matlab-Simulator für die Standards IEEE 802.11a/b/g/n entwickelt worden, der *inrange* Kollisionen zwischen mehreren sendenden 802.11-Stationen mit der Monte-Carlo-Simulation (siehe Kapitel 5.2) simuliert (vgl. Raychaudhuri, 2008).

5.1. Click-Softwarearchitektur

Ursprünglich ist die Click-Software vom *Massachusetts Institute of Technology* (MIT) entworfen worden, um Netzwerkadministratoren eine Möglichkeit zu bieten, einen Überblick über die vorhandene Software des Routers, dessen Konfiguration und dessen Schnittstellen zu erhalten (vgl. Click Modular Router Projekt; Kohler, 2001 und Morris et al., 1999). Dadurch sollen Netzwerkadministratoren die Funktionalität des Routers nach ihren Bedürfnissen anpassen und erweitern, da dies bei proprietärer Routersoftware lediglich bedingt oder sehr schwer möglich ist, da weder der Quellcode noch Schnittstellen ausreichend bekannt sind (vgl. Click Modular Router Projekt; Kohler, 2001 und Morris et al., 1999).
Ein weiterer Vorteil der Click-Softwarearchitektur ist die flexible Verwendbarkeit des Quellcodes, da die Click-Software ein beliebiges Unix-System erweitert. Somit wird der Click-Quellcode sowohl für 802.11-Stationen in einer Testumgebung als auch für virtuelle 802.11-Stationen in Simulatoren verwendet, denen ein Unix-System zu Grunde liegt. Außerdem gibt es zwei Möglichkeiten, wie die Click-

[7)] siehe http://sar/main/main_page.htm
[8)] Humboldt Wireless Lab

Software in ein bestehendes Unix-System eingebunden wird, nämlich entweder als Kernelmodul oder als Treiber im Benutzermodus. Zudem interagiert die Click-Software beim Empfang und beim Senden von Paketen mit den entsprechenden Treibern des Unix-Systems[9)]. Deshalb verarbeitet nicht das Unix-System die ankommenden und abgehenden Pakete weiter, sondern die Click-Software. Allerdings gibt es zwei wesentliche Unterschiede zwischen der Click-Software-Konfiguration, die auf den 802.11-Stationen der HWL-Testumgebung läuft und der Click-Software-Konfiguration, die in der Doktorarbeit von Eddie Kohler (siehe Kohler, 2001) verwendet worden ist. Hierbei ist in der Doktorarbeit von Eddie Kohler die Ethernet-Schnittstelle des Unix-Systems von der Click-Software gepollt worden (vgl. Kohler, 2001, Seite 91-92), wohingegen die Click-Software-Konfiguration für die 802.11-Stationen der HWL-Testumgebung die WLAN-Schnittstelle verwendet, die einen Interrupt auslöst, wenn ein neues Paket empfangen worden ist oder wenn der WLAN-Treiber bereit ist, ein Paket zu senden. Deshalb wird der WLAN-Treiber des MadWifi-Projektes (siehe MadWifi Projekt) zusammen mit dem Unix-System OpenWrt (siehe OpenWrt Projekt) für die einzelnen 802.11-Stationen in der HWL-Testumgebung verwendet. Außerdem unterstützt die Hardware der einzelnen 802.11-Stationen in der HWL-Testumgebung den IEEE 802.11e-Standard und somit werden für den Backoff-Algorithmus anstatt einer Warteschlange durch die Hardware vier Warteschlangen unterstützt. Damit jedes Paket in eine der vier Warteschlangen eingeordnet werden kann, ist eine Modifizierung des MadWifi-Treibers nötig. Zudem besteht zwischen der aktuellen Implementierung des MadWifi-Treibers und dem IEEE 802.11e-Standard ein Unterschied, da es in der aktuellen Implementierung keine virtuellen Kollisionen gibt. Daher wird erst ein neues Paket vom MadWifi-Treiber angefordert, wenn das aktuelle Paket versendet worden ist. Dieses Verhalten ist auch für die virtuellen 802.11-Stationen des NS2 implementiert worden. Dadurch wird für die Click-Software und dessen Schnittstellen eine Transparenz zwischen den 802.11-Stationen der HWL-Testumgebung und den virtuellen 802.11-Stationen im NS2 erreicht.

Die Click-Softwarearchitektur ist in der Programiersprache C++ implementiert worden und wird als Kernelmodul in das OpenWrt-System eingebunden. Außerdem setzt sich die Click-Softwarearchitektur aus einer Menge von verschiedenen

[9)] siehe http://www.read.cs.ucla.edu/click/docs/linuxmodule

Modulen zusammen, die als Elemente[10)] bezeichnet werden. Diese Elemente werden für eine Click-Software-Konfiguration über ihre Ein- und Ausgänge, die als *Ports* bezeichnet werden, miteinander verbunden. Hierbei gibt es drei verschiedene Typen von *Ports*, nämlich *Push*, *Pull* und *Agnostic* (vgl. Kohler, 2001, Seite 18 – 21). Die beiden Elemente Tos2QueueMapper und SetRTSCTS stellen für

```
1  Funktion Backoff-Strategie(Mac-Paket)
       Ausgabe : Warteschlange für MAC-Paket
2      Zieladresse ← Zieladresse des MAC-Paketes;
3      Falls Zieladresse bekannt dann
4          Paketverlustanteil ← hole(Zieladresse, inrange Kollision;
5          );
6      sonst
7          Paketverlustanteil ← hole(maximalen Paketverlustanteil);
8      Ende
9      Falls ( Kanalstatistik-Element existiert ) dann
10         Anzahl Nachbarstationen ←
           (Kanalstatistik-Element→#Nachbarstationen);
11     sonst
12         Anzahl Nachbarstationen ← hole(maximale Anzahl von
           Nachbarstationen);
13     Ende
14     Backoffwert ← hole(Paketverlustanteil, Anzahl Nachbarstationen);
15     Für ( q ∈ Warteschlangen ) mache
16         Falls ( Backoffwert ≤ maximale Backoff-Fenstergröße ) dann
17             Warteschlange ← q;
18             break;
19         Ende
20     Ende
21     zurück Warteschlange
22 Ende
```

Algorithmus 1 : Backoff-Strategie

ihren Ein- und Ausgang *Agnostic-Ports* zur Verfügung. Hierbei gibt es zwei Varianten, wie *Agnostic-Ports* implementiert werden können. Die erste Variante setzt die Implementierung der beiden Funktionen *push(int port, Packet *p)* und *pull(int*

[10)] siehe http://read.cs.ucla.edu/click/doxygen/classElement.html

```
1  Funktion RTS/CTS-Strategie(Mac-Paket)
       Ausgabe : RTS/CTS {an/aus}
2      RTS/CTS ← aus;
3      Zieladresse ← Zieladresse des MAC-Paketes;
4      Falls Zieladresse bekannt dann
5          Paketverlustanteil ← hole(Zieladresse, verstecktes Knotenproblem);
6          Zufallszahl ← würfle(0,100);
7          Falls (Zufallszahl ≤ Paketverlustanteil) dann
8              RTS/CTS ← an;
9          Ende
10     Ende
11     zurück RTS/CTS
12 Ende
```

Algorithmus 2 : RTS/CTS-Strategie

port) der Elementklasse voraus. In der zweiten Variante wird lediglich die Funktion *simple_ action(Packet *p)* der Elemtklasse[11)] implementiert. Somit ist für eine Vereinfachung des Quellcodes lediglich die Funktion *simple_ action(Packet *p)* implementiert worden. Der Algorithmus, der dem Tos2QueueMapper-Element zu Grunde liegt, wird in Abbildung 1 dargestellt. Hierbei wird für die zur Verfügung stehenden vier Warteschlangen jeweils verschiedene Backoff-Fenstergrößen [CW_{min}, CW_{max}] konfiguriert. Die Backoff-Fenstergrößen werden abhängig von der Anzahl der aktuellen Nachbarstationen und dem prozentualen Anteil für einen Paketverlust durch *inrange* Kollisionen bestimmt. Hierbei liefert das vorhandene Statistik-Element die Anzahl der Nachbarstationen, indem alle Paketübertragungen des aktuellen Kanals abgehört werden. Somit wird die Anzahl der Nachbarstationen über die Anzahl der sendenden Nachbarstationen ermittelt. Der prozentuale Anteil für den Paketverlust bei *inrange* Kollisionen erfolgt durch die Abfrage des Knotens für *inrange* Kollisionen in der Baumstruktur, die in Abbildung 4 des Kapitels 3.3 dargestellt ist. Dieser prozentuale Anteil wird für jede Zieladresse individuell bestimmt, wobei der prozentualen Anteile der einzelnen Knoten in der Baumstruktur (siehe Kapitel 3.3, Abbildung 4) in der Diplomarbeit von Michael Kühn (siehe Kühn, 2013) ermittelt wird. Ist nun der sendenden Station zum Einen die Anzahl seiner Nachbarstationen und zum Anderen der prozentuale An-

[11)] siehe http://read.cs.ucla.edu/click/doxygen/classElement.html

teil für den Paketverlust einer *inrange* Kollision zur Zieladresse bekannt, wird mit der Hilfe einer statischen Tabelle der Backoff für das aktuelle Paket ermittelt. Der ermittelte Backoff soll unter den gegebenen Bedingung den höchsten Durchsatz erreichen, indem unnötige Kollisionen vermieden werden. Anschließend wird die passende Warteschlange für den ermittelten Backoff bestimmt, indem der ermittelte Backoff mit den Backoff-Fenstergrößen der vier Warteschlangen verglichen wird. Fällt der ermittelte Backoff in eine der vier Backoff-Fenstergrößen hinein, wird diese Warteschlange für die aktuelle Paketübertragung bestimmt. Damit nun das Tos2QueueMapper-Element der Click-Software, die entsprechende Warteschlange für das aktuelle Paket dem MadWifi-Treiber bekannt macht, wird für diese Aufgabe das TOS[12)]-Feld verwendet. Hierbei sei auch angemerkt, dass eine erneute Backoff-Fenstergrößen-Konfiguration der vier Warteschlangen aus Gründen der Performanz vermieden werden sollte. Der Algorithmus 2 ist im SetRTSCTS-Element implementiert worden. Hierbei wird, wie schon für die Backoff-Strategie des Tos2QueueMapper-Elementes die Baumstruktur verwendet, die in der Abbildung 1 im Kapitel 3.3 dargestellt wird. Für den Algorithmus 2 wird nun der prozentuale Anteil für das versteckte Knotenproblem von der Baumstruktur abgefragt, da dieser als Schwellwert für die Aktivierung des RTS/CTS-Mechanismus dient. Deshalb wird eine Zufallszahl aus dem Intervall [0,100] ermittelt und mit dem Schwellwert verglichen. Ist die Zufallszal kleiner gleich dem Schwellwert, wird der RTS/CTS-Mechanismus für die aktuelle Paketübertragung aktiviert. Ansonsten bleibt der RTS/CTS-Mechanismus deaktiviert.

5.2. Matlab-Monte-Carlo-Simulator

Der Matlab-Simulator verwendet die Monte-Carlo-Simulation[13)] zur Berechnung von Kollisionen in Abhängigkeit des aktuellen Backoffs CW_k und der aktuellen Anzahl von Nachbarstationen n (siehe Kapitel 4.1). Dies wird in Abbildung 7 dargestellt.

Zudem wird für die Generierung von Pseudozufallszahlen der Mersenne-Twister-

[12)] Type of Service
[13)] siehe Raychaudhuri, 2008

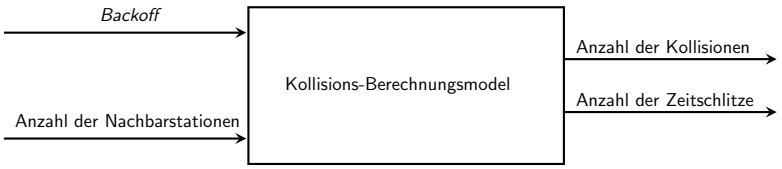


Abbildung 7: *Monte-Carlo-Simulation für die Berechnung von Kollisionen und benötigten Zeitschlitzen für die Paketübertragungen*

Algorithmus verwendet (vgl. Matsumoto und Nishimura, 1998). Hierbei wird für die Reproduzierbarkeit der Zufallszahlen ein Startwert, der auch als Saat (engl. seed) bezeichnet wird, einmalig vor dem Beginn der Simulation festgelegt.
Für das Kollisions-Berechnungs-Model wird der Backoff-Algorithmus des IEEE 802.11-Standards verwendet, indem ein Vektor mit verschiedenden Backoff-Fenstergrößen an den Algorithmus übergeben wird, um anschließend für eine feste Anzahl von 802.11-Nachbarstationen n die Anzahl der ereigneten Kollisionen k zu ermitteln.
Außerdem wird über verschiedene Backoff-Fenstergrößen und unterschiedliche Anzahlen von 802.11-Nachbarstationen iteriert, um in jedem Simulationsdurchgang für eine bestimmte Backoff-Fenstergröße und eine bestimmte Anzahl von 802.11-Nachbarstationen die Anzahl der aufgetretenen Kollisionen zu bestimmen.
Anschließend wird die Kollisionswahrscheinlichkeit p_c aus den aufgetretenen Kollisionen, wie folgt berechnet:

$$p_c(k, pakete_{\text{ausgeliefert}}) = \frac{k}{k + pakete_{\text{ausgeliefert}}} \cdot 100 \tag{5.1}$$

Betrachtet man einen Simulationsdurchlauf, muss zur Berechnung der aufgetretenen Kollisionen k zwischen den 802.11-Stationen für eine bestimmte Backoff--Fenstergröße CW_k und einer bestimmten Anzahl von 802.11-Nachbarstationen das folgende Ausführungskriterium(n, CW_k) gelten:

$$\text{Ausführungskriterium}(n, CW_k) = \frac{n}{CW_k} \tag{5.2}$$

Hierbei ist der Bereich des Ausführungskriteriums$(n\,, CW_k) \in [0, 1]$, wobei n wie

folgt berechnet wird:

$$n_{\text{total}} = n\ + 1 \tag{5.3}$$

Aus Gleichung (5.3) ist ersichtlich, dass n_{total} sich aus der betrachteten, sendewilligen 802.11-Station und dessen sendewilligen 802.11-Nachbarstationen berechnet wird. Ist das Ausführungskriterium erfüllt, werden die Schritte des Algorithmus 3 für die Simulation ausgeführt.

```
1  Funktion Simulation(n, Paketobergrenze, Vektor-Backoff-Fenstergröße;                    )
       Eingabe : n:= maximale Anzahl der sendenden 802.11-Stationen Paketobergrenze:= zusendende Pakete pro
                 802.11-Station Vektor-Backoff-Fenstergröße;
       := Backoff-Fenstergrößen;
       Ausgabe : Anzahl der globalen Kollisionen
2      Kollisionen_global ← 0;
3      Pakete_ausgeliefert[1...n] ← 0;
4      pos_VBF ← 1;
5      Backoff[1...n] ← würfel ∈ [0, Vektor-Backoff-Fenstergröße;[pos_VBF]];
6      Solange ( ∑_{i=1}^{n} Pakete_ausgeliefert[i] < ( n · Paketobergrenze)) mache
7          Backoff_min ← min(Backoff[1...n]);
8          Backoff[1...n] ← Backoff[1...n] - Backoff_min;
9          Stationen_sendend ← summiere( Backoff[1...n] == 0 );
10         Falls (Stationen_sendend ≥ 2) dann                                  /* Kollisionsfall */
11             Kollisionen_global ← Kollisionen_global + 1;
12             pos_VBF ← pos_VBF + 1;
13             Falls (pos_VBF ≥ n) dann
14                 pos_VBF ← n;
15         sonst                                  /* erfolgreiche Paketübertragung von einer Station */
16             Station_index ← suche_index(Backoff[1...n] == 0);
17             Pakete_ausgeliefert[Station_index] ← Pakete_ausgeliefert[Station_index] + 1;
18         Ende
19         bestimme(Backoff[1...n],Vektor-Backoff-Fenstergröße;
20         );
21     Ende
22     zurück Kollisionen_global
23 Ende
```

Algorithmus 3 : Kollisionsbestimmung ohne warten

6. Auswertung

Im Unterkapitel 6.1 werden das „klassische“ Geburtstagsparadoxon mit dessen Approximationsgleichung für die Backoff-Fenstergröße (siehe Gleichungen (4.2) und (4.5)), das „intuitive“ Geburtstagsparadoxon (siehe Gleichung (4.7)) und die Kollisionswahrscheinlichkeiten der Monte-Carlo-Simulation (siehe Kapitel 5.2) miteinander verglichen. Zudem werden noch der Durchsatz und die Effizienz für die optimalen Backoff-Fenstergrößen und deren Kollisionswahrscheinlichkeit untersucht.

6.1. Monte-Carlo-Simulation und Geburtstagsparadoxon

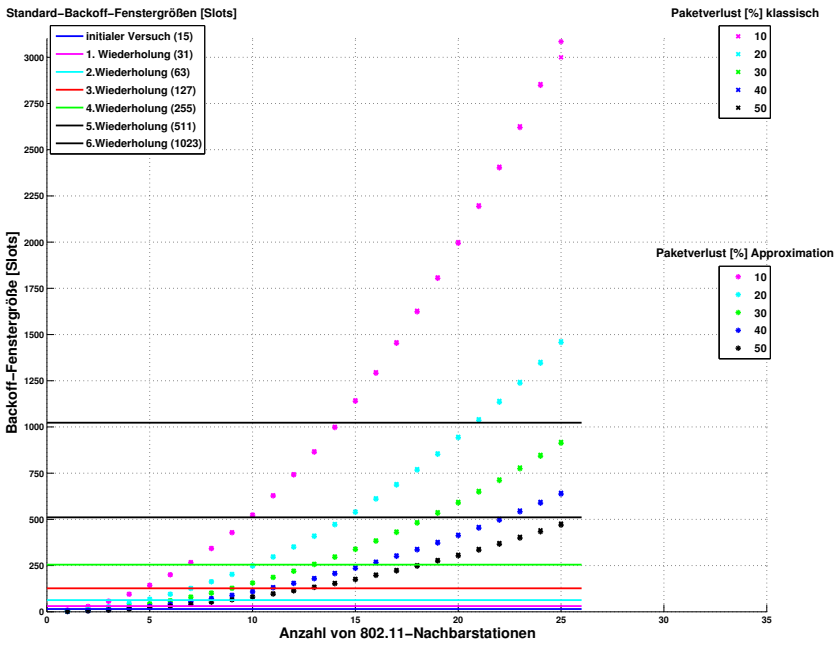


Abbildung 8: *Vergleich „klassisches“ Geburtstagsparadoxon mit dessen Approximation für verschiedene Paketverluste*

In Abbildung 8 werden für die Gleichung (4.2) des „klassischem“ Geburtstagsparadoxons und dessen Approximationsgleichung (4.5) für die Backoff-Fenstergrößen im Bereich [1,3000] und für bestimmte Anzahlen von 802.11-Nachbarstatio-

nen im Bereich [1,25] dargestellt. Hierbei werden ideale Bedingungen für das drahtlose Medium angenommen und somit entsprechen die Kollisionswahrscheinlichkeiten den Paketverlusten für jede sendewillige 802.11-Station im selben BSS-Gebiet. Außerdem wird in Abbildung 8 zusätzlich zum „klassischem“ Geburtstagsparadoxon und dessen Approximation die Backoff-Fenstergrößen[14)] dargestellt, die in den Standards IEEE 802.11a/b/g/n spezifiziert worden sind (siehe durchgezogene Linien).
Weiterhin lässt sich mit der Hilfe von Abbildung 8 erkennen, dass mit steigender Anzahl von sendewilligen 802.11-Nachbarstationen die Backoff-Fenstergröße der sendewilligen 802.11-Station vergrößert werden muss, damit die Paketverluste (Kollisionswahrscheinlichkeiten) für 10, 20, 30, 40 oder 50 Prozent auf einer konstanten Prozentzahl bleiben. Sonst erhöht sich bei konstanter Backoff-Fenstergrößen die Kollisionswahrscheinlichkeit und somit die Paketverluste für jede sendewillige 802.11-Station. Daher muss stets ein Kompromiss zwischen der Backoff-Fenstergröße und der damit verbundenen Wartezeit und der Anzahl der aufgetretenen *inrange* Kollisionen getroffen werden, die abhängig von der Anzahl der sendewilligen 802.11-Nachbarstationen sind. Deshalb wird nach dem „klassischem“ Geburtstagsparadoxon eine Kollisionswahrscheinlichkeit von z. B. maximal 10 Prozent erreicht, wenn für eine bestimmte Anzahl von sendewilligen 802.11-Nachbarstationen eine entsprechende Backoff-Fenstergröße gewählt wird. Diese Backoff-Fenstergröße ist nach Abbildung 8 bei einer sendewilligen 802.11-Nachbarstation 9 Zeitschlitze (Slots) und bei vierzehen sendewilligen 802.11-Stationen 1001 Zeitschlitze groß. Zudem differenzieren die statisch festgelegeten Backoff-Fenstergrößen[15)], die in den Standards IEEE 802.11a/b/g/n spezifiziert worden sind, lediglich indirekt zwischen der Anzahl der sendewilligen 802.11-Nachbarstationen n und der Kollisionswahrscheinlichkeit p_{c} . Somit entstehen unnötige Kollisionen, die den Durchsatz jeder sendewilligen 802.11-Station im BSS-Gebiet und daher auch den Durchsatz des gesamten BSS-Gebietes verringern.

Zudem kann man anhand von Tabelle 2 den minimalen und maximalen euklidischen Abstand zwischen den Backoff-Fenstergrößen des „klassischem“ Geburtstagsparadoxon und dessen Approximationsgleichung (4.5) für bestimmte Anzahlen von sendewilligen 802.11-Nachbarstationen und verschiedenen Paketverlusten

[14)] siehe im Kapitel 4 Gleichung (4.1)
[15)] siehe durchgezogene Linien Abbildung 8

802.11-Nachbarstationen	euklidischer Abstand [Slots]	
	minimal	maximal
5	0	1
15	4	5
20	5	6
25	7	85

Tabelle 2: *Euklidischer Abstand zwischen den Backoff-Fenstergrößen des „klassischem“ Geburtstagsparadoxon und dessen Approximationsgleichung* (4.5) *für verschiedene Paketverluste von Abbildung 8*

sehen. Außerdem wird durch Tabelle 2 ersichtlich, dass mit steigender Anzahl von 802.11-Stationen, sich der euklidische Abstand zwischen den Backoff-Fenstergrößen des „klassischem“ Geburtstagsparadoxon und dessen Approximationsgleichung (4.5) vergrößert.

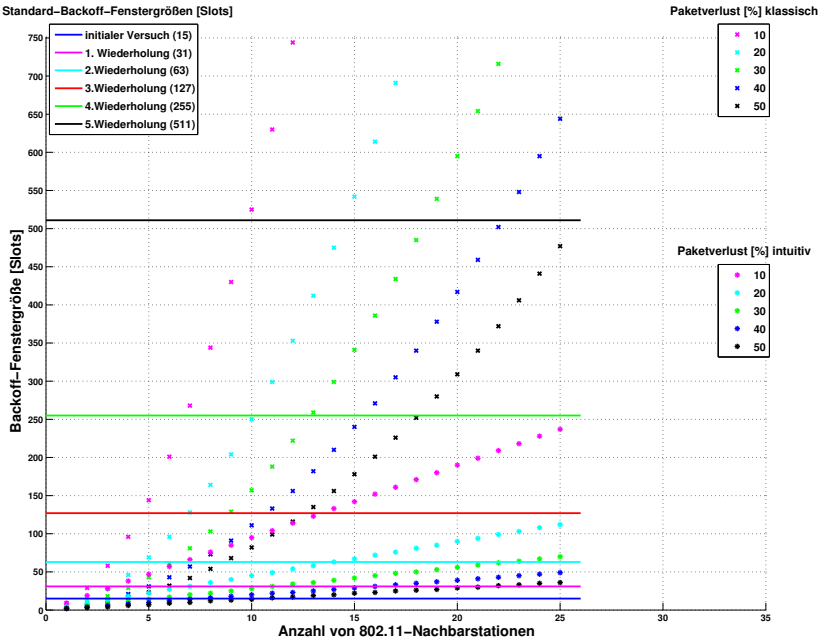


Abbildung 9: *„Klassisches“ Geburtstagsparadoxon und „intuitives“ Geburtstagsparadoxon für verschiedene Paketverluste*

Neben dem „klassischem“ Geburtstagsparadoxon existiert noch das „intuitive“ Ge-

burtstagsparadoxon (siehe Gleichungen (4.6) und (4.7)). Das „intuitive“ Geburtstagsparadoxon wird in Abbildung 9 dargestellt und mit dem „klassischem“ Geburtstagsparadoxon verglichen. Somit soll der Unterschied zwischen dem „klassischem“ und dem „intuitiven“ Geburtstagsparadoxon verdeutlicht werden, da bei einer gegebenen Anzahl von 802.11-Nachbarstationen das „intuitive“ Geburtstagsparadoxon eine geringere Backoff-Fenstergröße als das „klassische“ Geburtstagsparadoxon hat.

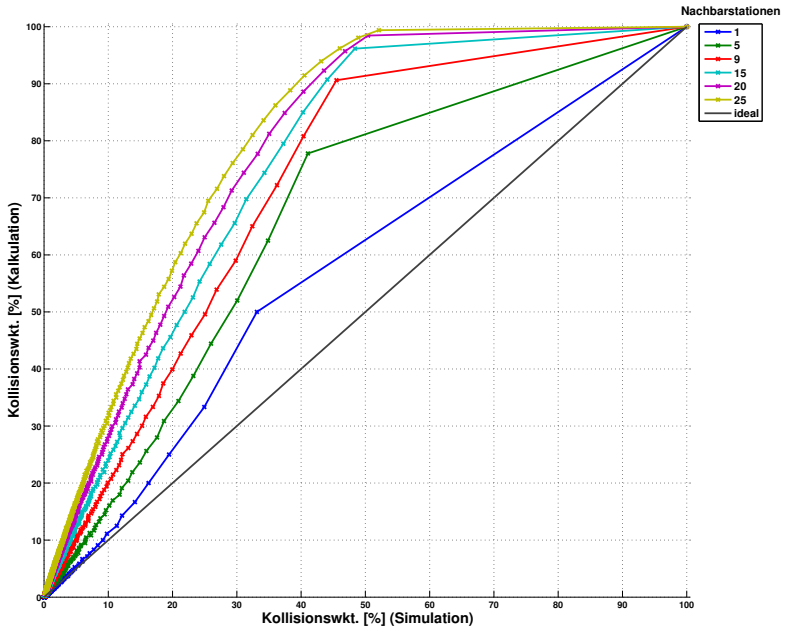


Abbildung 10: *Vergleich Kollisions-Berechnungs-Model* **??** *mit dem „klassischem“ Geburtstagsparadoxon für verschiedene Nachbarstationen*

In Abbildung 10 wird nun das „klassische“ Geburtstagsparadoxon mit den Kollisionswahrscheinlichkeiten der Monte-Carlo-Simulation (siehe Algorithmus 3 in Kapitel 5.2) für die verschiedenen 802.11-Nachbarstationen und entsprechenden Backoff-Fenstergrößen dargestellt. Anhand von Abbildung 10 ist ersichtlich, dass die Kollisionswahrscheinlichkeiten der Monte-Carlo-Simulation und des „klassischem“ Geburtstagsparadoxon sich nicht der „ideal“ Linie (durchgezogene, schwarze Diagonallinie) nähern, sondern sich sogar mit steigender Anzahl von 802.11-Nachbarstationen weiter von der „ideal“ Linie entfernen. Dieses Verhalten wird auch durch Tabelle 3 ersichtlich, da in Tabelle 3 der euklidische Abstand zwischen bestimmten

Paketverluste [%]	802.11-Nachbarstationen					
	1	5	9	15	20	25
5	0.1691	9.5935	17.9369	28.6465	37.2755	43.4560
10	1.4959	17.9170	32.4152	47.7926	58.0496	65.2830
20	5.8561	32.1498	49.9234	64.9560	71.5198	75.2814
30	17.6693	43.0775	57.3706	65.8262	68.4205	69.3845

Tabelle 3: *Euklidischer Abstand zwischen „idealer Linie“ und bestimmten Kollisionswahrscheinlichkeiten für verschiedene Paketverluste in Abbildung 10*

Kollisionswahrscheinlichkeiten (Paketverlusten) und der „idealen“ Linie für berechnet worden sind. Hierbei ist zu beachten, dass der euklidische Abstand in Tabelle 3 und Tabelle 4 linear interpoliert worden ist, falls die Kollisionswahrscheinlichkeiten der Monte-Carlo-Simulation und die des „klassischem“ Geburtstagsparadoxon von den gesuchten Kollisionswahrscheinlichkeiten in Tabellen 3 voneinander abweichen (vgl. Lohninger). Außerdem ist die Berechnung für bestimt Kollisionswahrscheinlichkeiten abhängig von der Anzahl der 802.11-Nachbarstationen (siehe Abbildung 10).

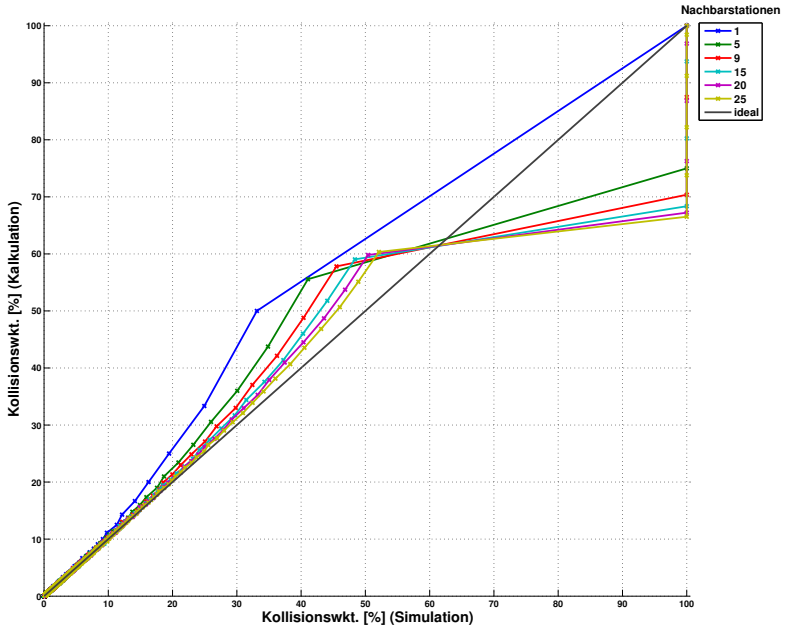


Abbildung 11: *Vergleich Kollisions-Berechnungs-Model* **??** *mit dem „intuitiven“ Geburtstagsparadoxon für verschiedene Nachbarstationen*

Paketverluste [%]	802.11-Nachbarstationen					
	1	5	9	15	20	25
5	0.1691	0.0525	0.0014	0.0794	0.0169	0.1083
10	1.4959	0.0530	0.1296	0.0997	0.0343	0.1343
20	5.8561	0.5237	0.0319	0.2664	0.4095	0.4286
30	17.6693	2.0618	0.5769	0.4545	0.5994	0.8152

Tabelle 4: *Euklidischer Abstand zwischen „idealer Linie“ und bestimmten Kollisionswahrscheinlichkeiten für verschiedene Paketverluste in Abbildung 11*

Im Gegensatz zum „klassischem“ Geburtstagsparadoxon wird durch Abbildung 11 verdeutlicht, dass sich die Kollisionswahrscheinlichkeiten der Monte-Carlo-Simulation und des „intutitiven“ Geburtstagsparadoxons sich der „ideal“ Linie (durchgezogene, schwarze Diagonallinie) bis zu einer Kollisionswahrscheinlichkeit von 50 bis 60 Prozent, je nach Anzahl der 802.11-Nachbarstationen , annähern. Dies wird auch durch Tabelle 4 verdeutlicht, wobei auch für die Berechnung des euklidischen Abstandes von Tabelle 4, wie in Tabelle 3, die lineare Interpolation verwendet worden ist.

Daher kann nun mit der Hilfe des „intuitiven“ Geburtstagsparadoxons die Backoff-Fenstergröße für den IEEE 802.11-Standard (siehe durchgezogene Linien in Abbildung 9) abhängig von der Kollisionswahrscheinlichkeit und der Anzahl der 802.11-Nachbarstationen bestimmt werden. Hierzu wird zunächst der Schnittpunkt zwischen der Gleichung (4.1) für $CW_{\min}$ und der Gleichung (4.7) ermittelt. Ersetzt man nun k in Gleichung (4.1) durch $k = \frac{p_c(k,1)}{1-p_c(k,1)}$, wobei $p_c(k,1)$ die Kollisionswahrscheinlichkeit für einen auszuliefernden Rahmen ist, erhält man die folgende Gleichung:

$$\frac{2^{\frac{p_c(k,1)}{(1-p_c(k,1))}}}{1-\sqrt[n]{1-p_c(n,CW_k)}} \cdot CW_{\min} = 0 \tag{6.1}$$

Approximiert man noch $2^{\frac{p_c(k,1)}{(1-p_c(k,1))}} \approx \frac{1}{(1-p_c(k,1))}$ für $p_c(k,1) \in [0;0,5]$ und sei Gleichung (6.1) die Backoff-Verzögerung $\mathrm{D}_{\mathrm{Backoff}}$, erhält man die folgende Gleichung (vgl. Cesana et al., 2010):

$$\mathrm{D}_{\mathrm{Backoff}} = \frac{1}{(1-p_c(k,1)) \cdot 1-\sqrt[n]{1-p_c(n,CW_k)}} \cdot CW_{\min} \tag{6.2}$$

Außerdem sind für die verschiedenen Kollisionswahrscheinlichkeiten, die durch die Monte-Carlo-Simulation simuliert worden sind und natürlich auch durch das „intuitve“ Geburtstagsparadoxon approximiert werden können, der Durchsatz ([Mbps]) und die Effizienz ϵ ([%]) nach den Gleichungen (6.3) und (6.4), wie folgt berechnet worden (vgl. Jun et al.):

$$Durchsatz = \frac{\text{Pakete}_{\text{ausgliefert}} \cdot (\text{MSDU} \cdot byte)}{(D_{\text{Backoff}} + D_{\text{k}} + D_{\text{Pakete}_{\text{ausgliefert}}})} \cdot \frac{1}{MB} \tag{6.3}$$

Hierbei ist $\text{Pakete}_{\text{ausgliefert}}$ die Anzahl der ausgelieferten Pakete der sendewilligen 802.11-Stationen (siehe Kapitel 5.2), MSDU die Größe der Nutzdaten des Rahmens, *MB* steht für Megabyte und dementsprechend steht *byte* für ein Byte. Die Dauer D_{Backoff} wird durch

$$D_{\text{Backoff}} = \text{Zeitschlitze}_{\text{gesamt}} \cdot D_{\text{Zeitschlitz}} \,,$$

wobei $\text{Zeitschlitze}_{\text{gesamt}} \in \text{N}_0$ und $D_{\text{Zeitschlitz}}$ die Dauer für einen Zeitschlitz ist, die wiederum abhängig von den Standards IEEE 802.11a/b/g/n sind. Die Dauer der fehlgeschlagenen Paketübertragungsversuche (U_{f}^{P}) wird durch

$$D_{\text{k}} = k \cdot U_{\text{f}}^{\text{P}} \,,$$

berechnet, wobei $k \in \text{N}_0$ ist. Die Dauer $D_{\text{Pakete}_{\text{ausgliefert}}}$ aller erfolgreichen Paketübertragungsversuche (U_{e}^{P}) werden durch

$$D_{\text{Pakete}_{\text{ausgliefert}}} = U_{\text{e}}^{\text{P}} \cdot \text{Pakete}_{\text{ausgliefert}}$$

ermittelt. Hierbei ist zu beachten, dass U_{f}^{P} und U_{e}^{P} abhängig von der MSDU-Größe und der verwendeten Datenrate ist und nach den folgenden Gleichungen berechnet wird:

$$U_{\text{f}}^{\text{P}} = \frac{\text{MSDU} + \text{Overhead}_{\text{MAC}}}{r} + \frac{Overhead_{\text{Phy}}}{r_{\text{Phy}}}$$

$$U_{\text{e}}^{\text{P}} = U_{\text{f}}^{\text{P}} + \frac{\text{ACK} + \text{Overhead}_{\text{MAC}}}{r} + \frac{Overhead_{\text{Phy}}}{r_{\text{Phy}}}$$

Ist der Durchsatz ermittelt worden, wird die Effizienz nach Gleichung 6.4 durch die Basisrate r dividiert.

$$\epsilon = \frac{Durchsatz}{r} \tag{6.4}$$

Aus der Berechnung des Durchsatzes für die Kollisionswahrscheinlichkeiten der Monte-Carlo-Simulation sind für bestimmte Datenraten des IEEE 802.11g-Standards (1, 6, 24, 54 Mbps) und für bestimmte Rahmengrößen (500, 1500, 3000, 8000 Bytes) für den Wertebereich der 802.11-Nachbarstationen der optimale Durchsatz berechnet worden. Bei der Berechnung des optimalen Durchsatzes werden *Greenfield*-Bedingungen und 1 Mbps für die Datenrate des Bestätigungsrahmens (ACK-Rahmen) angenommen. Zudem wird das vierte Adressfeld des MAC-Rahmens und die Einschränkungen der Rahmengrößen, die durch den jeweiligen Standard IEEE 802.11a/b/g/n für die physikalische Schicht spezifiziert worden ist, nicht berücksichtigt. Somit findet keine Fragmentierung statt.
Ist der optimale Durchsatz für den Wertebereich der 802.11-Nachbarstationen ermittelt worden, wird in Abhängigkeit des optimalen Durchsatzes die Effizienz, die Backoff-Fenstergröße und die Kollisionswahrscheinlichkeit ermittelt.

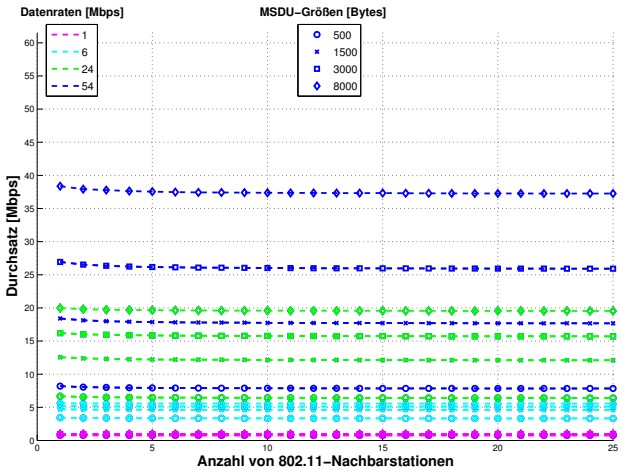


Abbildung 12: *Durchsatz für verschiedene Nachbarstationen , Datenraten und MSDU-Größen*

Aus diesem Grund wird in Abbildung 12 der optimale Durchsatz unter den oben beschriebenen Bedingungen für die verschiedenen Anzahlen von 802.11-Nachbar-

stationen ([1,25]) dargestellt. Hierbei müssen die beiden Legenden „Datenrate“ und „MSDU-Größen“ miteinander kombiniert werden, um die einzelnen Graphen interpretieren zu können. Außerdem kann man anhand von Abbildung 12 sehen, dass der optimale Durchsatz bei den Datenraten 1 und 6 Mbps sich in einem schmaleren Bereich befindet als dies bei den Datenraten 24 und 54 Mbps der Fall ist. Deshalb ist der optimale Durchsatz für die Datenraten 24 und 54 Mbps stark von der Rahmengröße (MSDU-Größe) abhängig. Somit hängt bei den Datenraten 24 und 54 Mbps der optimale Durchsatz von der Relation *Overhead* zu Rahmengröße und der Relation Kollisionswahrscheinlichkeit zur Anzahl der 802.11-Nachbarstationen ab.

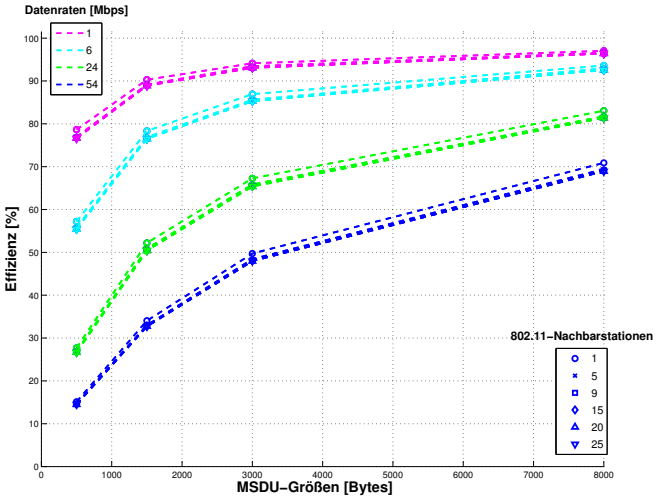


Abbildung 13: *Effizienz für verschiedene Nachbarstationen , Datenraten und MSDU-Größen*

Betrachtet man nun Abbildung 13, dann wird für die Effizienz der einzelnen Datenraten und der einzelnen Rahmengrößen (MSDU-Größen) deutlich, dass die Effizienz der Datenraten 24 und 54 Mbps im Gegensatz zu den Datenraten 1 und 6 Mbps mit zunehmender Rahmengröße zunimmt. Außerdem wird durch Abbildung 14 ersichtlich, dass die Kollisionswahrscheinlichkeit nicht auf Null reduziert werden muss, um den optimalen Durchsatz zu erhalten. Zudem verdeutlicht Abbildung 14, dass mit wachsender Rahmengröße die Kollisionswahrscheinlichkeit verringert wird. Aber die Kollisonswahrscheinlichkeit mit steigender Datenrate deutlich zunimmt.

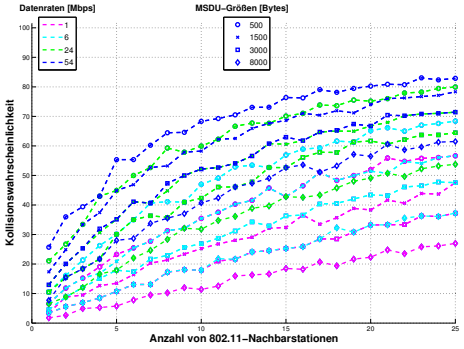


Abbildung 14: *Kollisionswahrscheinlichkeit für verschiedene Nachbarstationen , Datenraten und MSDU-Größen*

Wie sich die Kollisionswahrscheinlichkeit auf die Backoff-Fenstergröße auswirkt, wird in Abbildung 15 dargestellt. Hieran kann man sehen, dass die Backoff-Fenstergröße bei den Datenraten 1 und 6 Mbps mit steigender Rahmengröße einen wesentlichen Einfluss auf die Berechnung des optimalen Durchsatzes hat, wohingegen die Backoff-Fenstergrößen mit steigender Datenrate sich in einem schmaleren Bereich befinden als bei den Datenraten 1 und 6 Mbps.

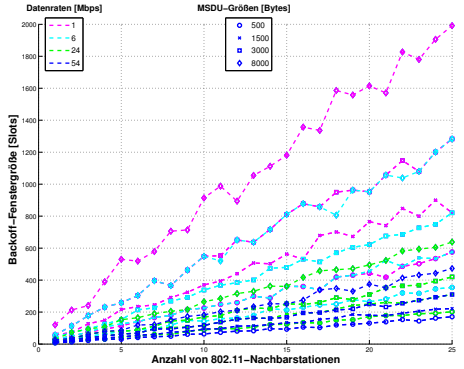


Abbildung 15: *Backoff-Fenstergrößen für verschiedene Nachbarstationen , Datenraten und MSDU-Größen*

6.2. Hot-Spot-Szenario mit Click

6.2.1. Simulation mit NS2

In diesem Kapitel wird die Click-Software zusammen mit dem NS2 verwendet, um *inrange* Kollisionen zu simulieren. Der Unterschied zwischen dem NS2 und dem Matlab-Simulator, der im Kapitel 6.1 ausführlich beschrieben worden ist, besteht darin, dass beim Matlab-Simulator lediglich Paketfehler oder Paketverluste durch Kollisionen entstehen, da ein „idealer“ Übertragungskanal vorausgesetzt wird. Wohingegen der NS2 standardmäßig drei Funkausbreitungsmodelle[16)] zur Verfügung stellt, nämlich das Freiraummodel[17)], das Zwei-Strahlen-Boden-Reflektionsmodel[18)] und das Abschattungsmodel[19)] (vgl. Netzwerksimulator 2 Projekt und Walke et al., 2006, Seite 10ff).

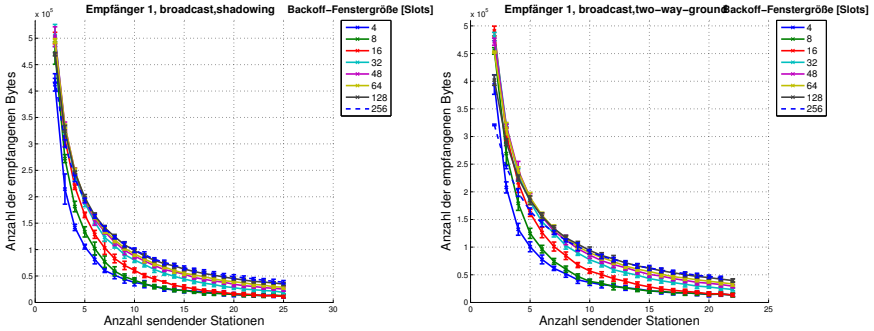
Abbildung 16: *Simulationsszenario für den NS2*

Im Folgenden wird der saturierte Fall für das in Abbildung 16 dargestellte Szenario mit dem Zwei-Strahlen-Boden-Reflektionsmodel und dem Abschattungsmodel für Broadcast und Unicast untersucht. Somit haben alle sendenden 802.11-Stationen

[16)] engl. radio probagation models (siehe http://www.isi.edu/nsnam/ns/doc/node216.html und http://kom.aau.dk/group/05gr1120/ref/Channel.pdf)
[17)] engl. Free space model
[18)] Two-ray ground reflection model
[19)] shadowing model

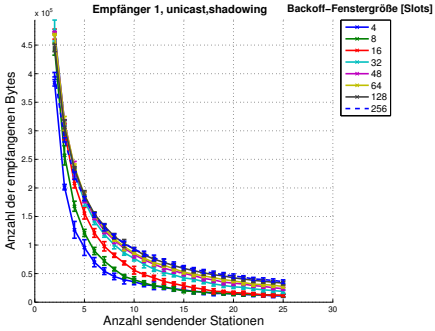
volle Warteschlangen. Deshalb versuchen die einzelnen sendenden 802.11-Stationen (S_1 bis S_{22}) permanent Pakete mit einer Datenrate von 1 Mbps für eine Dauer von 70 Sekunden zu übertragen. Zudem übertragt die empfangende 802.11-Station E_1 im Unicast-Szenario ihren Bestätigungsrahmen ebenfalls mit einer Datenrate von 1 Mbps.
Für das in Abbildung 16 dargestellte Szenario wird die Anzahl der sendenden 802.11-Stationen [1,22] variiert. Daher hat jede sendende 802.11-Station bis zu maximal 21 sendewillige 802.11-Nachbarstationen. Außerdem werden für jede Anzahl von sendenden 802.11-Stationen verschiedene Backoff-Fenstergrößen [4, 256] untersucht. Hierbei ist zu beachten, dass $\mathrm{CW}_{\mathrm{min}}$ und $\mathrm{CW}_{\mathrm{max}}$ gleich sind. Daher bestimmt jede sendende 802.11-Station ihren Backoff für eine bestimmte Anzahl von 802.11-Stationen immer aus dem selben Backoff-Fenster. Mit diesen Ausgangsbedingungen werden für die verschiedenen Anzahlen von sendenden 802.11-Stationen und die verschiedenen Backoff-Fenstergrößen die Anzahl der empfangenden Bytes und der RSSI-Wert[20)] durch die empfangende 802.11-Station E_1 ermittelt. Anschließend wird die Anzahl der empfangenden Bytes und der RSSI-Wert den jeweiligen Anzahlen von sendenden 802.11-Stationen und deren Backoff-Fenstergrößen zugeordnet.

In Abbildung 17(a), (b) und (c) wird die maximale Anzahl an empfangenden Bytes durch E_1 für verschiedene Anzahlen von sendenden 802.11-Stationen für das Abschattungsmodel und das Zwei-Strahlen-Boden-Reflektionsmodel für Broadcast und Unicast dargestellt. Außerdem wird der Größenunterschied zwischen der Broadcast und der Unicast-Verbindung ersichtlich, da mehr Bytes als bei Unicast-Verbindungen von den sendenden 802.11-Stationen an die empfangende 802.11-Station E_1 übertragen, da bei Unicast-Verbindungen ein *Overhead* durch den von E_1 versendeten Bestätigungsrahmen entsteht.



(a) Broadcast, Abschattungsmodel

(b) Broadcast, Zwei-Strahlen-Boden-Reflektionsmodel



(c) Unicast, Abschattungsmodel

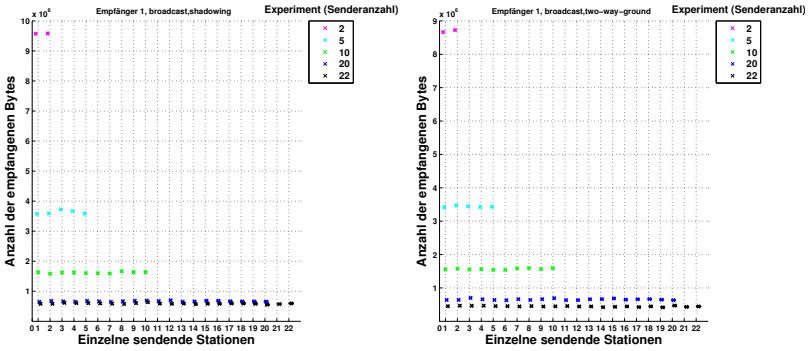
Abbildung 17: *Maximamle Anzahl von empfangenden Bytes an der empfangenden Station*

6.2.2. Testbed

7. Zusammenfassung und Ausblick

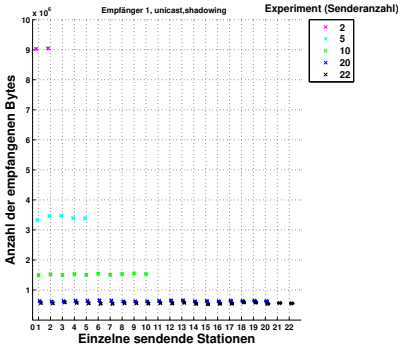
Zuerst sind die Ursachen für Paketverluste und Paketfehler klassifiziert worden, um dann passende Mechanismen des IEEE 802.11-Standards abhängig von den aufgetretenen Ursachen für Paketverluste und Paketfehler zu ermitteln. Dies ist notwendig, um um den Durchsatz jeder einzelnen 802.11-Station zu steigern und somit den Durchsatz des gesamten 802.11-Netzes zu erhöhen. Aus diesem Grund sind Kollisionen als Hauptursache für Paketverluste und Paketfehler identifiziert

[20] Mittelwert aus allen empfangenden RSSI-Werten



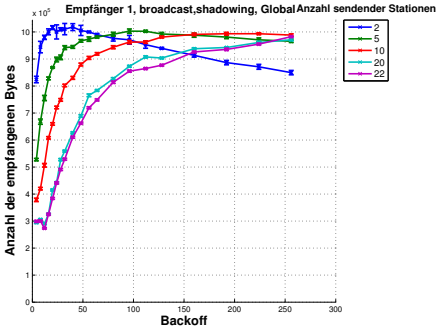
(a)

(b)

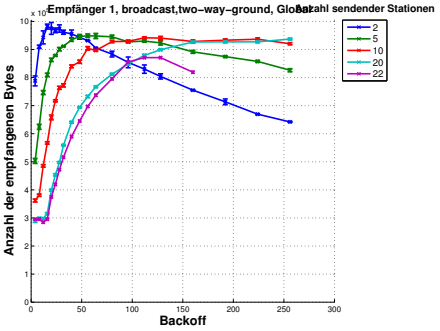


(c)

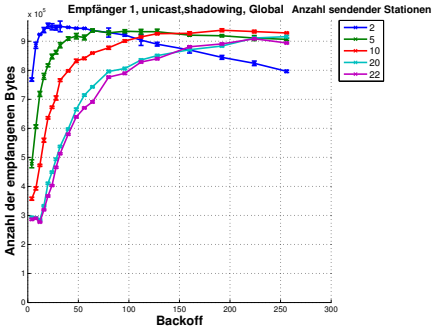
worden, da der IEEE 802.11-Standard sich für die drahtlose Kommunikation etabliert hat. Somit erhöht sich die Auslastung der einzelnen Übertragungskanäle des ISM-Bandes, die im IEEE 802.11-Standard spezifiziert worden sind. Deshalb sind *inrange* Kollisionen für verschiedene Szenarien sowohl in der Simulation als auch in einer realen Testumgebung untersucht worden. Daher sind mit der Monte-Carlo-Simulation die aufgetretenen Kollisionen in Abhängigkeit von verschiedenen Backoff-Fenstergrößen und verschiedenen Anzahlen von sendenden 802.11-Stationen in einem BSS-Gebiet im saturierten Fall ermittelt worden. Hieraus hat sich ergeben, dass das „intuitive“ Geburtstagsparadoxon eine Approximation für den Backoff-Algorithmus liefert. Daher wird mit dem „intuitiven“ Geburtstagsparadoxon für eine bestimmte Anzahl die Verzögerungsdauer des Backoff-Algorithmus berechnet.



(d)



(e)



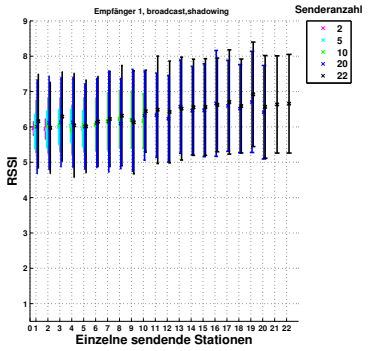
(f)

A. Anhang

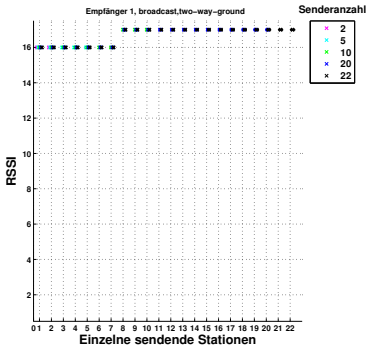
B. Herleitung

A. Backoff-Verzögerung und „intuitives“ Geburtstagsparadoxon

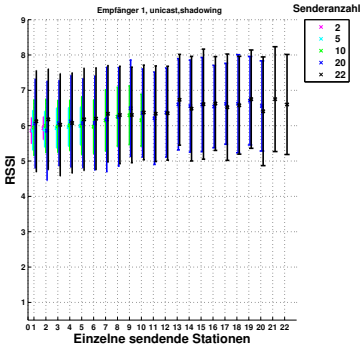
Sei k die aufgetretenen Kollisionen für eine Anzahl von ausgelieferten Paketen $\text{pakete}_{\text{ausgeliefert}}$, dann ergibt sich folgende bedingte Kollisionswahrscheinlichkeit



(g)



(h)



(i)

(vgl. Basler, 1994, Seite 70 ff):

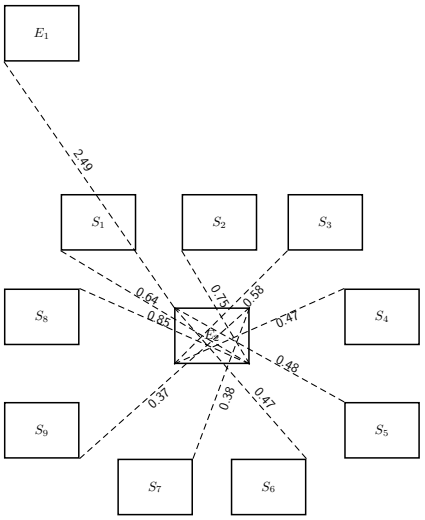
$$p_c(k, \text{paket}_{\text{ausgeliefert}}) = \frac{k}{k + \text{pakete}_{\text{ausgeliefert}}} \tag{B.1}$$

Daraus folgt für ein auszulieferndes Paket ($\text{paket}_{\text{ausgeliefert}} = 1$) und durch Auflösen von Gleichung (B.1) nach k:

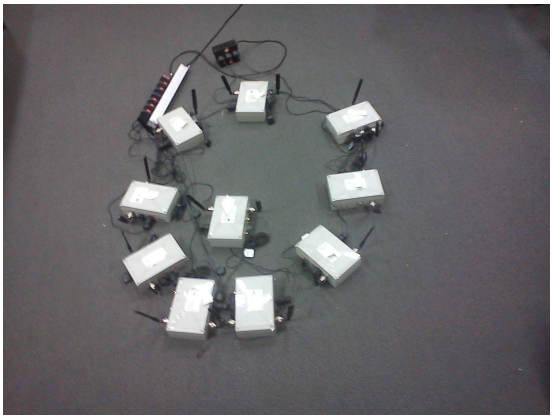
$$k = \frac{p_c(k,1)}{(1 - p_c(k,1))} \tag{B.2}$$

Damit man nun den Schnittpunkt zwischen den beiden Gleichungen (4.7) und (B.2) erhält, werden diese gleich gesetzt und für k die Gleichung (B.2) eingesetzt:

$$(2^{\frac{p_c(k,1)}{(1-p_c(k,1))}} \cdot (CW_{\min})) - 1 = 1 - \sqrt[n]{1 - p_c(n, CW_{\text{aktuell}})}$$



(j)



(k)

Abbildung 18: *Skizze (j) und Bidlausschnitt (k) des Testbed-Szenarios*

$$\Rightarrow \frac{2^{\frac{p_c(k,1)}{(1-p_c(k,1))}}}{1-\sqrt[n]{1-p_c(n,CW_{\text{aktuell}})}} \cdot CW_{\min} = 0 \tag{B.3}$$

B. RTS/CTS-*Overhead* und Rahmengröße

Sei die Dauer für eine Paketübertragung D_{Paket}, dann gilt für einen erfolgreichen Paket-Übertragungsversuch U_{e}^{P} des CSMA/CA-Protokolls (ohne RTS/CTS-Mechanismus):

$$U_{\text{e}}^{\text{P}} = D_{\text{Backoff}} + D_{\text{DIFS}} + D_{\text{MSDU}} + D_{\text{SIFS}} + D_{\text{ACK}} \tag{B.4}$$

Außerdem gilt für einen fehlgeschlagenen Paket-Übertragungsversuch U_{f}^{P}:

$$U_{\text{f}}^{\text{P}} = D_{\text{Backoff}} + D_{\text{DIFS}} + D_{\text{MSDU}} + D_{\text{SIFS}} \tag{B.5}$$

Analog zu den Gleichungen (B.4) und (B.5) gilt für einen erfolgreichen Paket-Übertragungsversuch $U_{\text{e}}^{\text{RTS/CTS}}$ mit RTS/CTS und einen fehlgeschlagenen Paket-

Übertragungsversuch $U_{\mathrm{f}}^{\mathrm{RTS/CTS}}$ mit RTS/CTS die folgenden Gleichungen:

$$U_{\mathrm{e}}^{\mathrm{RTS/CTS}} = U_{\mathrm{e}}^{\mathrm{P}} + D_{\mathrm{RTS}} + D_{\mathrm{SIFS}} + D_{\mathrm{CTS}} + D_{\mathrm{SIFS}} \tag{B.6}$$

$$U_{\mathrm{f}}^{\mathrm{RTS/CTS}} = D_{\mathrm{Backoff}} + D_{\mathrm{DIFS}} + D_{\mathrm{RTS}} + D_{\mathrm{SIFS}} \tag{B.7}$$

Damit der *Overhead* des RTS/CTS-Mechanismus zum Basis-Mechanismus des CSMA/CA-Protokols gleich ist oder diesen übertrifft, muss die folgende Ungleichung gelten:

$$\mathrm{D}_{U_{\mathrm{e}}^{\mathrm{P}}} + \mathrm{D}_{U_{\mathrm{f}}^{\mathrm{P}}} \geq \mathrm{D}_{U_{\mathrm{e}}^{\mathrm{RTS/CTS}}} + \mathrm{D}_{U_{\mathrm{f}}^{\mathrm{RTS/CTS}}} \tag{B.8}$$

Sei nun die Kollisionswahrscheinlichkeit p_c, dann ergibt sich für die Gleichung (B.8):

$$\begin{aligned}
&(1-p_c)\cdot U_{\mathrm{e}}^{\mathrm{P}} + p_c \cdot U_{\mathrm{f}}^{\mathrm{P}} \geq (1-p_c)\cdot U_{\mathrm{e}}^{\mathrm{RTS/CTS}} + p_c \cdot U_{\mathrm{f}}^{\mathrm{RTS/CTS}} \\
\Rightarrow\ &(1-p_c)\cdot U_{\mathrm{e}}^{\mathrm{P}} + p_c \cdot (U_{\mathrm{e}}^{\mathrm{P}} - D_{\mathrm{ACK}}) \geq (1-p_c)\cdot U_{\mathrm{e}}^{\mathrm{RTS/CTS}} + p_c \cdot U_{\mathrm{f}}^{\mathrm{RTS/CTS}} \\
\Rightarrow\ &U_{\mathrm{e}}^{\mathrm{P}} - \cancel{p_c \cdot U_{\mathrm{e}}^{\mathrm{P}}} + \cancel{p_c \cdot U_{\mathrm{e}}^{\mathrm{P}}} - p_c \cdot D_{\mathrm{ACK}} \geq U_{\mathrm{e}}^{\mathrm{RTS/CTS}} - p_c \cdot U_{\mathrm{e}}^{\mathrm{RTS/CTS}} + p_c \cdot U_{\mathrm{f}}^{\mathrm{RTS/CTS}} \\
\Rightarrow\ &\cancel{D_{\mathrm{Backoff}}} + \cancel{D_{\mathrm{DIFS}}} + \cancel{D_{\mathrm{MSDU}}} + \cancel{D_{\mathrm{SIFS}}} + \cancel{D_{\mathrm{ACK}}} - \cancel{p_c \cdot D_{\mathrm{ACK}}} \\
&\geq \cancel{D_{\mathrm{Backoff}}} + \cancel{D_{\mathrm{DIFS}}} + D_{\mathrm{RTS}} + D_{\mathrm{SIFS}} + D_{\mathrm{CTS}} + D_{\mathrm{SIFS}} + \cancel{D_{\mathrm{MSDU}}} + \cancel{D_{\mathrm{SIFS}}} + \cancel{D_{\mathrm{ACK}}} \\
&- p_c \cdot (\cancel{D_{\mathrm{Backoff}}} + \cancel{D_{\mathrm{DIFS}}} + \cancel{D_{\mathrm{RTS}}} + \cancel{D_{\mathrm{SIFS}}} + D_{\mathrm{CTS}} + D_{\mathrm{SIFS}} + D_{\mathrm{MSDU}} + D_{\mathrm{SIFS}} + \cancel{D_{\mathrm{ACK}}}) \\
&+ \cancel{p_c} \cdot (\cancel{D_{\mathrm{Backoff}}} + \cancel{D_{\mathrm{DIFS}}} + \cancel{D_{\mathrm{RTS}}} + \cancel{D_{\mathrm{SIFS}}}) \\
\Rightarrow\ &0 \geq D_{\mathrm{RTS}} + D_{\mathrm{SIFS}} + D_{\mathrm{CTS}} + D_{\mathrm{SIFS}} - p_c \cdot D_{\mathrm{CTS}} - p_c \cdot D_{\mathrm{SIFS}} - p_c \cdot D_{\mathrm{MSDU}} - p_c \cdot D_{\mathrm{SIFS}} \\
\Rightarrow\ &p_c \cdot D_{\mathrm{MSDU}} \geq D_{\mathrm{RTS}} + 2 \cdot D_{\mathrm{SIFS}} + D_{\mathrm{CTS}} - p_c \cdot D_{\mathrm{CTS}} - 2 \cdot p_c \cdot D_{\mathrm{SIFS}} \\
\Rightarrow\ &D_{\mathrm{MSDU}} \geq \frac{D_{\mathrm{RTS}} + 2 \cdot D_{\mathrm{SIFS}} \cdot (1-p_c) + D_{\mathrm{CTS}} \cdot (1-p_c)}{p_c}
\end{aligned}$$

Stationen	x	y	z
E_1	0	15	0
S_1	50	8	0
S_2	50	9	0
S_3	50	10	0
S_4	50	11	0
S_5	50	12	0
S_6	50	13	0
S_7	49	8	0
S_8	49	9	0
S_9	49	10	0
S_{10}	49	11	0
S_{11}	49	12	0
S_{12}	49	13	0
S_{13}	48	8	0
S_{14}	48	9	0
S_{15}	48	10	0
S_{16}	48	11	0
S_{17}	48	12	0
S_{18}	48	13	0
S_{19}	47	8	0
S_{20}	48	9	0
S_{21}	48	10	0
S_{22}	48	11	0
S_{23}	48	12	0
S_{24}	48	13	0
S_{25}	48	14	0

Tabelle 5: *Szenario Hot-Spot*

C. Tabelle für das NS2-Szenario

D. Auslastung des Mediums

Um die Auslastung des drahtlosen Mediums zu zeigen, sollen 802.11-Stationen[21)] den Datenverkehr in den Frequenzbereichen des 2,4 GHz als auch des 5 GHz ISM-Bandes in einer realen Testumgebung (siehe HWL Projekt) passiv mithören. Das passive Mithören der einzelnen 802.11-Stationen erfolgt systematisch, indem die einzelnen 802.11-Stationen zuerst die Kanäle 1 bis 11 des 2,4 GHz ISM-Bandes und anschließend die Kanäle 36 bis 64 des 5 GHz ISM-Bandes passiv abhören. Außerdem verweilen die einzelnen 802.11-Stationen in jedem Kanal für eine Dauer von 5 Minuten und sammeln innerhalb dieser Dauer sekündlich Informationen über den Datenverkehr im jeweiligem Kanal.
Zudem wird der beschriebene Messvorgang fünfmal wiederholt. Somit wird über eine Gesamtdauer von 25 Minuten der Datenverkehr der einzelnen Kanäle von den 802.11-Stationen in ihrer jeweiligen Umgebung passiv mitgeschnitten.
Damit die Auswertung der Informationen der einzelnen 802.11-Stationen, die passiv mitgehört haben, nicht den Rahmen dieser Arbeit sprengt, wird exemplarisch für alle 802.11-Stationen eine 802.11-Stationen ausgewählt, die eine entsprechende Anzahl von sendenden 802.11-Nachbarstationen in ihrer Empfangsreichweite hat. Außerdem soll exemplarisch für alle Kanäle ein Kanal mit einer entsprechenden Anzahl von sendenden 802.11-Stationen ausgewählt werden.

Deshalb werden in Abbildung 21 und in Abbildung 22 mit der Hilfe des Box-Whisker-Plots die jeweiligen 802.11-Stationen, die passiv mitgehört haben, in Abhängigkeit zu den sendenden 802.11-Nachbarstationen für das 2,4 GHz und das 5 GHz ISM-Band der gesamten Messreihe (über alle Kanäle und Wiederholungen der Messung) dargestellt.

Hierbei hat jede 802.11-Nachbarstation innerhalb der Zeitspanne, in der der Datenverkehr des jeweiligen Kanals mitgeschnitten worden ist, mindestens einen Rahmen übertragen. Außerdem kann man einen deutlichen Unterschied hinsichtlich

[21)] insgesamt 37

der Auslastung des Mediums zwischen den Frequenzbereichen des 2,4 GHz (siehe Abbildung 21) und des 5 GHz ISM-Bandes (siehe Abbildung 22) erkennen, da im 2,4 GHz ISM-Band mehr sendende 802.11-Nachbarstationen als im 5 GHz ISM-Band vorhanden sind. Daher wird das 2,4 GHz ISM-Band zurzeit häufiger von sendenden 802.11-Stationen als das 5 GHz ISM-Band verwendet. Aus diesem Grund wird im Folgenden lediglich das 2,4 GHZ ISM-Band betrachtet.
Um dies nochmals zu verdeutlichen und um einen Kanal mit einer entsprechenden Anzahl von sendenden 802.11-Nachbarstationen zu bestimmen, wird in Abbildung 23 und in Abbildung 24 mithilfe des Box-Whisker-Plots zu jedem Kanal im 2,4 GHz und im 5 GHz ISM-Band die sendenden 802.11-Nachbarstationen über die gesamte Messreihe (über alle Knoten und Wiederholungen der Messung) dargestellt.

Anhand von Abbildung 21 wird ersichtlich, dass die mithörende 802.11-Station (Knoten 35) eine wesentliche Anzahl von sendenden 802.11-Nachbarstationen in seiner Empfangsreichweite hat. Daher wird in Abbildung 25 für die mithörende Station 35 zu jedem Kanal die Anzahl der sendenden 802.11-Station in einem Box-Whisker-Plot, über jeweils eine Minute gemittelt, dargestellt. Außerdem wird in Abbildung 26 zu jeder Messung (5 Minuten) die sich verändernde Anzahl von sendenden 802.11-Nachbarstationen deutlich.
Dieses Verhalten wird ebenfalls beobachtet, wenn lediglich ein Kanal betrachtet wird.
Aus Abbildung 23 wird daher ersichtlich, dass Kanal 1 eine wesentliche Anzahl von sendenden 802.11-Nachbarstationen hat. Daher wird Kanal 1 in den Abbildungen 27 und 28, wie bei der mithörenden 802.11-Station 35, näher betrachtet.
Schließlich kann man beobachten, dass die Anzahl der sendenden 802.11-Nachbarstationen abhängig vom Ort (siehe Abbildung 25), vom jeweiligen Frequenzbereich (siehe Abbildung 23 und 24) und innerhalb eines bestimmten Frequenzbereiches von der Frequenz (siehe Abbildung 27) und dem Zeitpunkt (siehe Abbildung 26 und 28) abhängig ist.

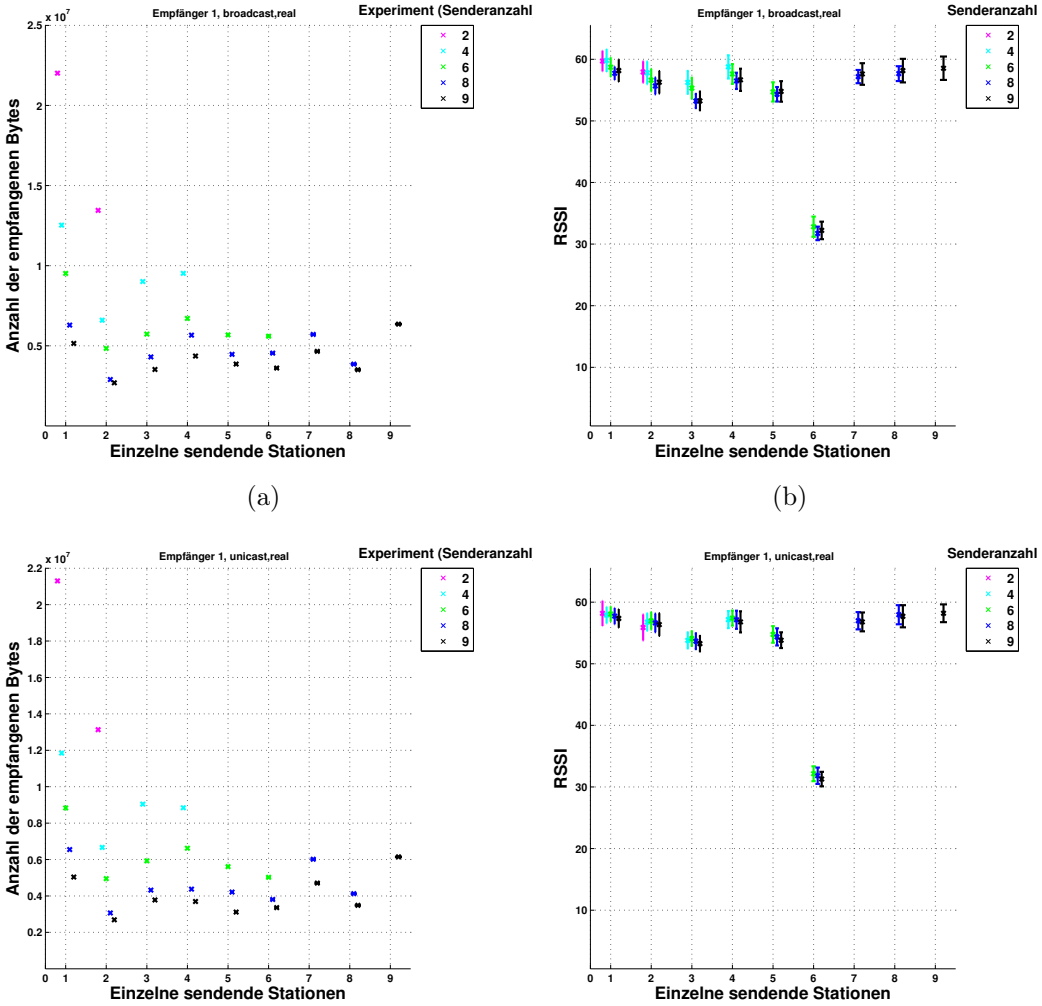
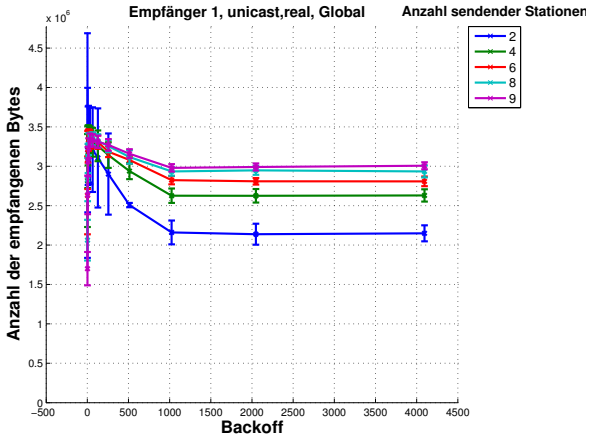
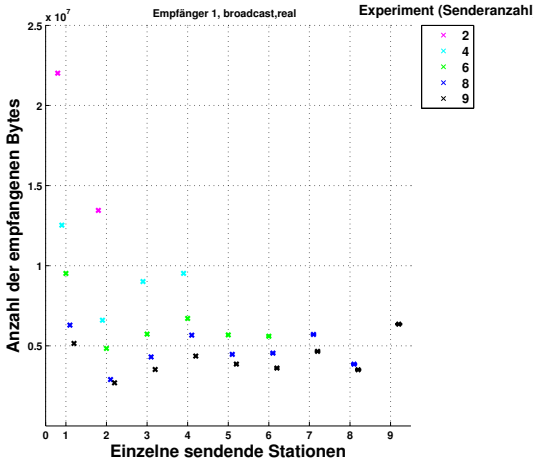


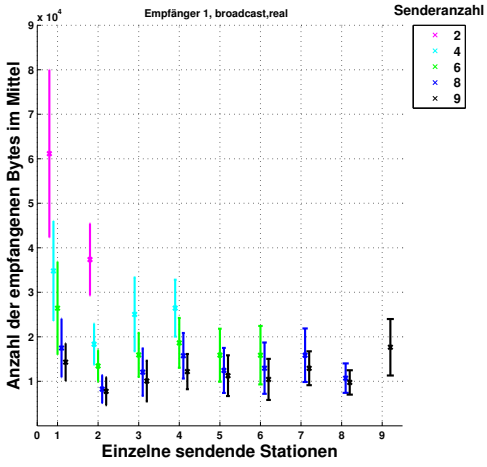
Abbildung 19: *TESTBED*



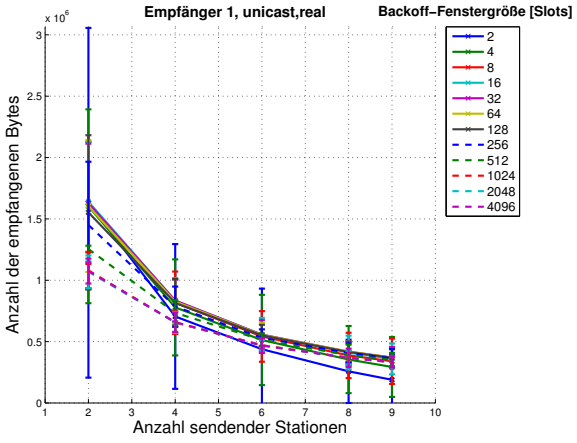
(a)



(b)



(c)



(d)

Abbildung 20: *TESTBED*

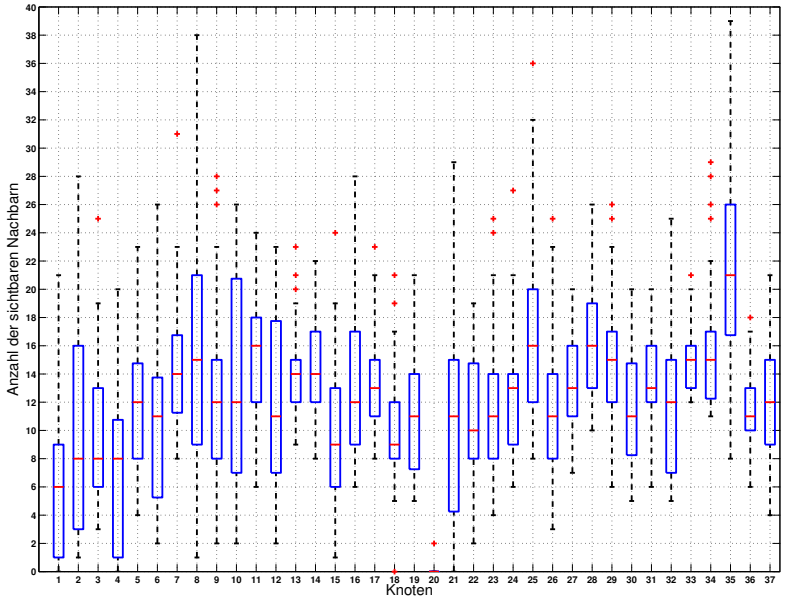


Abbildung 21: *Box-Whisker-Plot für jede 802.11-Station und ihre jeweiligen 802.11-Nachbarstationen im 2,4 GHz ISM-Band*

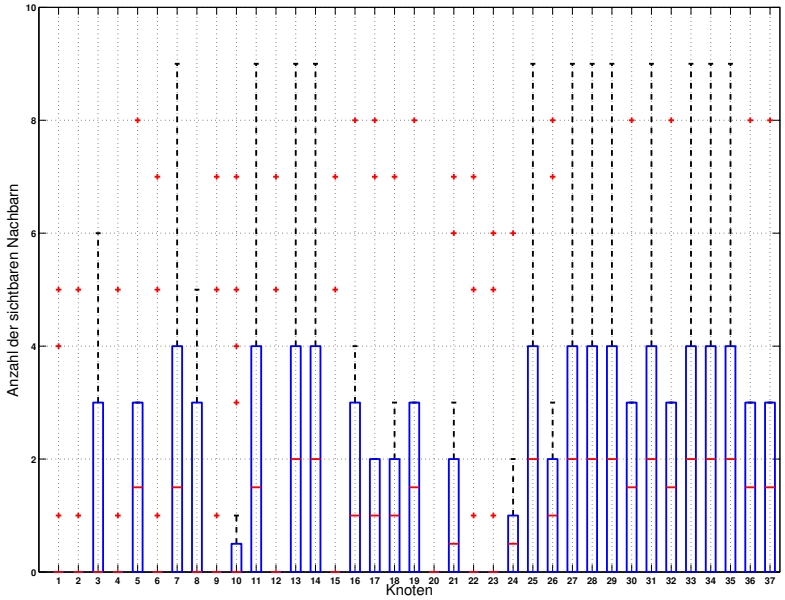


Abbildung 22: *Box-Whisker-Plot für jede 802.11-Station und ihre jeweiligen 802.11-Nachbarstationen im 5 GHz ISM-Band*

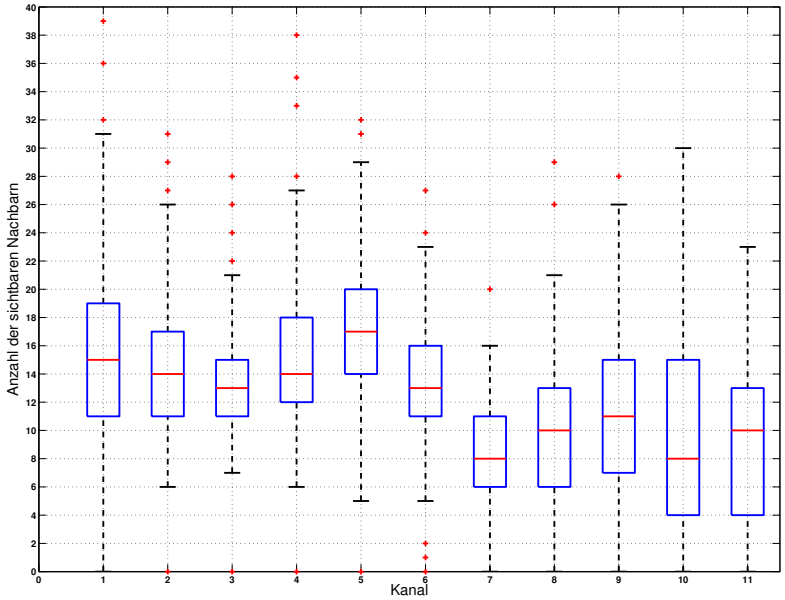


Abbildung 23: *Box-Whisker-Plot für jeden Kanal im 2,4 GHz ISM-Band und den jeweiligen 802.11-Nachbarstationen*

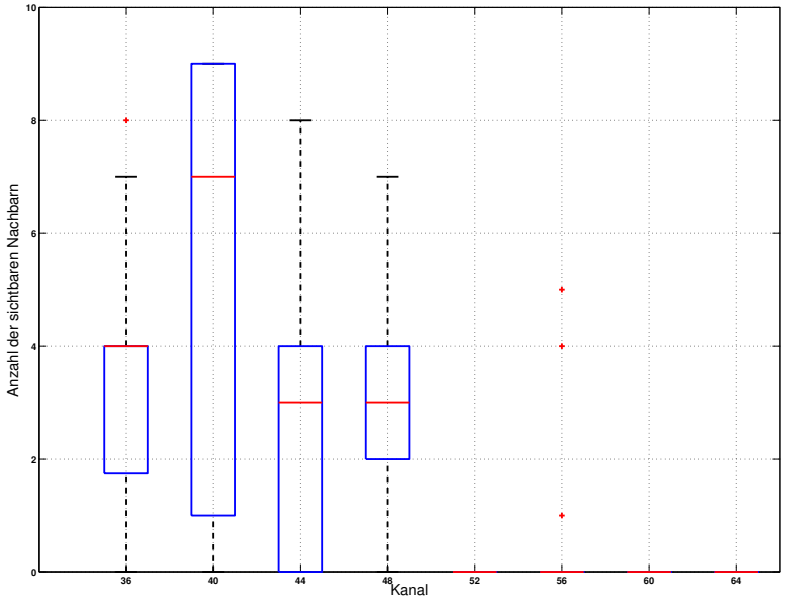


Abbildung 24: *Box-Whisker-Plot für jeden Kanal im 5 GHz ISM-Band und den jeweiligen 802.11-Nachbarstationen*

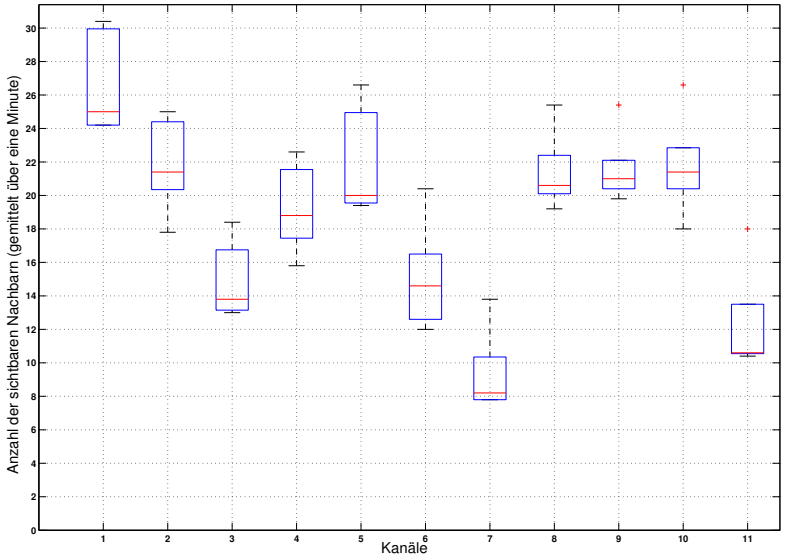


Abbildung 25: *Box-Whisker-Plot für Knoten 35*

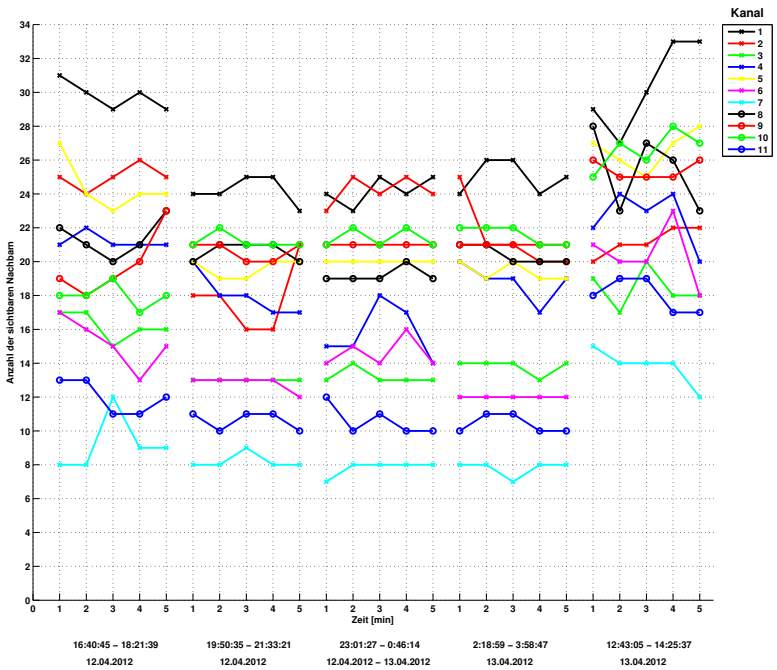


Abbildung 26: *Knoten 35, Messungen von je 5 Minuten*

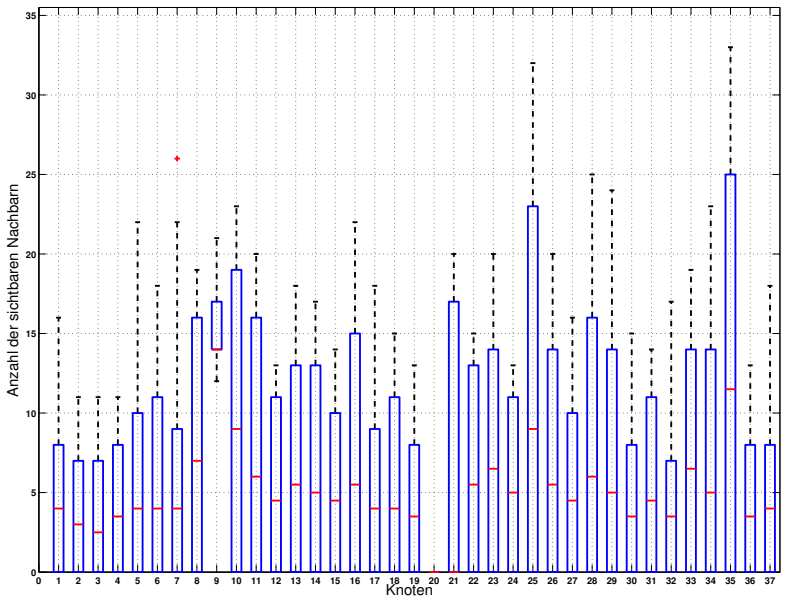


Abbildung 27: *Box-Whisker-Plot von Kanal 1*

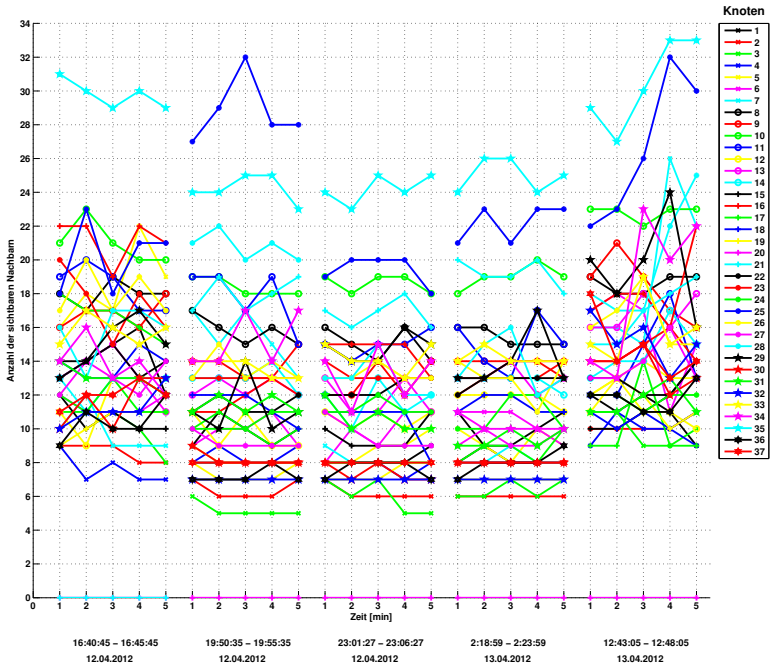


Abbildung 28: *Kanal 1, Messungen von je 5 Minuten*

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

Basler, Herbert (1994): *Grundbegriffe der Wahrscheinlichkeitsrechnung und Statistischen Methodenlehre.* Physica-Verlag

Bharghavan, Vaduvur und Demers, Alan und Shenker, Scott und Zhang, Lixia (1994): *MACAW: A Media Access Protocol for Wireless LAN's.* , *SIGCOM*

Bianchi, Giuseppe (2000): *Performance Analysis of the IEEE 802.11 Distributed Cordination Function.* , *IEEE Journal on selected areas in communications* 18, No.3

Bicket, John C. (2005): *Bit-rate Selection in Wireless Networks.* Diplomarbeit, Massachusetts Institute of Technology

Bruno, Raffaele und Conti, Marco und Gregori, Enrico (2002): *IEEE 802.11 OPTIMAL PERFORMANCES: RTS/CTS MECHANISM VS. BASIC ACCESS.* , *IEEE*

Cesana, Matteo und Cuomo, Francesca und Ekici, Eylem (2010): *Routing in cognitive radio networks: Challenges and solutions.* , *Ad Hoc Netw.*

Chatzimisios, P. und Boucouvalas, A. C. und Vitsas, V. (2004): *Optimisation of RTS/CTS handshake in IEEE 802.11 Wireless LANs for maximum performance.* , *IEEE Communications Society - Globecom Workshops*

Chen, Dazhi und Deng, Jing und Varshney, Pramod K.: *Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming.* , *EECS Dept., Syracuse University, Syracuse, NY 13244*

Click Modular Router Projekt: *The Click Modular Router Project.* http://www.read.cs.ucla.edu/click/click – besucht am 25.02.2013

Frankfurt, Flughafen (2012): *Flughafen Frankfurt erster deutscher Airport mit*

gratis WLAN. http://www.frankfurt-airport.de/content/frankfurt_airport/de/news0/flughafen-frankfurt-erster-deutscher-airport-mit-gratis-w-lan.html – besucht am 25.02.2013

Freifunk Deutschland: http://start.freifunk.net/ – besucht am 3.01.2013

Freifunk Schweiz: http://www.openwireless.ch/ – besucht am 25.02.2013

Freifunk Östereich: http://www.funkfeuer.at/ – besucht am 25.02.1013

Garcia Villegas, Eduard und López-Aguilera, Elena und Vidal, Rafael und Paradells, Josep (2007): *Effect of adjacent-channel interference in IEEE 802.11 WLANs*. In *Cognitive Radio Oriented Wireless Networks and Communications*.

Gast, Matthew (2005): *802.11Wireless Networks The Definitive Guide*. O'Reilly

Hashemi, Homayoun (1993): *The Indoor Radio Propagation Channel*. , *Proceedings of the IEEE* Vol. 81, No. 7

HWL Projekt: http://hwl.informatik.hu-berlin.de/ – besucht am 25.02.2013

IEEE Standard 802.11 (1997): *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*.

IEEE Standard 802.11 (2012): *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*.

IEEE Standard 802.11a (1999): *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band*.

IEEE Standard 802.11b (1999): *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*.

IEEE Standard 802.11e (2005): *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment: Medium Access Method (MAC) Quality of Service Enhancements.*

IEEE Standard 802.11g (2003): *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.*

IEEE Standard 802.11n (2009): *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 5: Enhancements for Higher Throughput.*

IEEE Standard 802.2 (1998): *Part 2: Logical Link Control.* http://standards.ieee.org/about/get/802/802.2.html

Issariyakul, Teerawat und Hossain, Ekram (2009): *Introduction to Network Simulator NS2.* Springer Science+Business Media, LLC

Jun, Jangeun und Peddabachagari, Pushkin und Sichitiu, Mihail: *Theoretical Maximum Throughput of IEEE 802.11 and its Applications.*

Kim, Byung-Seo und Fang, Yuguang und Wong, Tan F. (2005): *Throughput Enhancement Through Dynamic Fragmentation in Wireless LANs.* , *IEEE Transactions on Vehicular Technology* 54, Nr. 4

Kim, Seong-Cheol und Bertoni, Henry L. und Stern, Miklos (1996): *Pulse Propagation Characteristics at 2.4 GHz Inside Buildings.* , *IEEE Transactions on Vehicular Technology* 45

Kohler, Eddie (2001): *The Click Modular Router.* Dissertation, Massachusetts Institute of Technology,

Kovar, Petr und Vít, Novontý (2008): *New Analytical Model of Distributed Coordination Function.* , *New Analytical Model of Distributed Coordination Function* 8 No.12,

Kühn, Michael (2013): *In Search of a Packet Loss Discriminator*. Diplomarbeit, Humboldt Universität Berlin

Labiod, H. und AfifiI, H. und Santis, C. de (2007): *WI-FI, Bluetooth, ZIG BEE and WIMAX*. Springer

Lohninger, Hans: *Grundlagen der Statistik*. http://www.statistics4u.info/fundstat_germ/wrapnt536532_statistische_tests.html – besucht am 21.03.2013

MadWifi Projekt: *The MadWifi project*. http://madwifi-project.org/ – besucht am 25.02.2013

Matsumoto, M. und Nishimura, T. (1998): *"Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator"*. , *ACM Trans. on Modeling and Computer Simulation*, 8, Nr. 1, 3–30

Metrik: *Modellbasierte Entwicklung von Technologien für selbstorganisierende dezentrale Informationssysteme im Katastrophenmanagement*. http://metrik.informatik.hu-berlin.de/grk-wiki/index.php/Hauptseite – besucht am 25.02.2013

MIT Roofnet Projekt: http://pdos.csail.mit.edu/roofnet/doku.php – besucht am 25.02.2013

Morris, Robert und Kohler, Eddie und Jannotti, John und Kaashoek, M. Frans (1999): *The Click Modular Router*. , *ACM SIGOPS Operating Systems Review*, 33, Nr. 5, 217– 231 http://www.sigops.org/sosp99/program.html

Netzwerksimulator 2 Projekt: *The Network Simulator - ns-2*. http://isi.edu/nsnam/ns/ – besucht am 25.02.2013

OpenWrt Projekt: *OpenWrt - Wireless Freedom*. https://openwrt.org/ – besucht am 26.02.2013

Perahia, Eldad und Stacey, Robert (2008): *Next Generation Wireless LANs Throughput, Robustness, and Reliability in 802.11n*. Cambridge University Press

Ray, Saikat und Carruthers, Jeffrey B. und Starobinski, David: *RTS/CTS-Induced Congestion in Ad Hoc Wireless LANs.* , *National Science Foundation under NSF CAREER grant ANI-0132802 and by a SPRInG award from Boston University*

Rayanchu, Shravan und Patro, Ashish und Banerjee, Suman (2011): *Airshark: Detecting Non-WiFi RF Devices using Commodity WiFi Hardware*. In *IMC'11, Berlin, Germany.*

Raychaudhuri, Samik (2008): *INTRODUCTION TO MONTE CARLO SIMULATION*. In *Proceedings of the 2008 Winter Simulation Conference*. Hrsg. v. **Mason,** S. J. und **Hill,** R. R. und **Mönch,** L. und **Rose,** O. und **Jefferson,** T. und **Fowler,** J. W..

Rohm, Wilfried: *Das Geburtstagsparadoxon.* www.math-tech.at/Beispiele/upload/ro_geburtstagsparadox.PDF – besucht am 14.03.2013

Schiller, Jochen H. (2003): *Mobile Communications, Second Edition.* Addison-Wesley

Seemann, Jochen und von Gudenberg, Jürgen Wolff (2006): *Software-Entwurf mit UML 2 Objektorientierte Modellierung mit Beispielen in Java 2. Auflage*. Springer-Verlag Berlin Heidelberg

Tannenbaum, Andrew S. (2003): *Computernetzwerke, 4., überarbeitete Auflage.* Pearson Studium

Treiber, Martin: *Trainingsaufgaben zur Klausurvorbereitung in Statistik I und II.* http://vwitme011.vkw.tu-dresden.de/~treiber/statistikTrainingsaufg/geburtstagsparadoxon.pdf – besucht am 25.02.2013

Unterrainer, Andreas und Rohm, Wilfried: *Statistik der Geburten.* http://www.ammu.at/archiv/11/11_6.htm – besucht am 14.03.2013

Valadas, Rui T. und Tavaras, Antonio R. und Oliveira Duarte, A. M. de und Moreira, Adriano C. und Lomba, Cipriano T. (1998): *The Infrared Physical Layer of the IEEE 802.11 Standard for Wireless Local Area Networks.* , *IEEE Communications Magazine*

Walke, Bernhard H. und Mangold, Stefan und Berlemann, Lars (2006): *IEEE 802 Wireless Systems.* John Wiley & Sons, Ltd http://books.google.de/books?hl=de&lr=&id=sX1w2xpi0mkC&oi=fnd&pg=PR5&dq=IE-+EE+802+Wireless+Systems&ots=7hRtBCBkFZ&sig=1g5KGYSKsow2YDF7rOJLxKu_xPQ#v=onepage&q=IE-%20EE%20802%20Wireless%20Systems&f=true

Wang, Shao-Cheng und Chen, Yi-Ming und Lee, Tsern-Huei und Helmy, Ahmed: *Performance Evaluations for Hybrid IEEE 802.11b and 802.11g Wireless Networks.*

Wu, Haitao und Peng, Yong und Long, Keping und Cheng, Shiduan und Ma, Jian (2002): *Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancements.* , *IEEE*

Wysocki, Tadeusz A. und Zepernick, Hans-Jürgen (2000): *Characterization of the indoor radio propagation channel at 2.4 GHz.* , *Journal of Telecommunications and Information Technology*

Zhang, K. und Lim, A. und Wu, S. und Q.Yang (2010): *A High TCP Performance Rate Adaptation Algorithm for IEEE 802.11 Networks.* , *International Journal of Computer Networks & Communications (IJCNC)*, vol. 2, no. 6, 31–44

Selbständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig verfasst und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Weiterhin erkläre ich, eine Diplomarbeit in diesem Studiengebiet erstmalig einzureichen.

Berlin, den 18. April 2013 .....