Klassifizierung von Paketverlusten in 802.11-Netzwerken

Diplomarbeit

zur Erlangung des akademischen Grades
Diplominformatiker

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

eingereicht von:	Michael Kühn
geboren am:	26.02.1980
in:	Frankfurt/Oder
Gutachter:	Prof. Dr. Jens-Peter Redlich
	Prof. Dr. Joachim Fischer
Betreuer:	Robert Sombrutzki
eingereicht am:	.....

Zusammenfassung

Drahtlose Kommunikation ist eine weit verbreitete und fast allgegenwärtige Methode Daten auszutauschen. Viele Geräte unterstützen die drahtlose Datenübertragung über 802.11-Netzwerke.

In dieser Diplomarbeit werden die Ursachen von Paketverlusten bzw. ineffizienter Ausnutzung der Mediumszeit in IEEE-802.11-Netzwerken betrachtet. Ziel ist mit Hilfe von zu entwickelnden Elementen die Klassifizierung von Paketverlusten vorzunehmen und Ursachen von Paketverlusten abzuschätzen.

Paketverluste in 802.11-Netzwerken wirken sich negativ auf den Datendurchsatz aus. Diese Paketverluste können unterschiedliche Ursachen wie zum Beispiel zu schwache oder gestörte Signale, Kollisionen durch gleichzeitiges Senden mehrerer Stationen oder Interferenzen durch Störquellen in der Umgebung haben.

Es gibt verschiedene Mechanismen, um Paketverluste zu reduzieren. Da beim Einsatz dieser Mechanismen die genauen Ursachen der Paketverluste aber nicht berücksichtigt werden, kann deren Einsatz ineffizient und in wenigen Fällen auch kontraproduktiv sein. So reduziert die Vergrößerung des Backoff die Wahrscheinlichkeit von Kollisionen durch gleichzeitiges Senden mehrerer Stationen, ermöglicht aber keine Verringerung der Paketverluste durch zu schwache Signale.

Durch Kenntnis der genauen Ursachen für auftretende Paketverluste können die Mechanismen zur Reduzierung von Paketverlusten gezielt genutzt werden, um Übertragungsparameter effektiver anzupassen und so Paketverluste zu reduzieren.

Diese Arbeit geht speziell auf Paketverluste verursacht durch „Hidden-Nodes“, „In-Range-Kollisionen“, „Weak-Signal“ und „Non-Wifi-Störungen“ genauer ein. Außerdem wird versucht, eine Abschätzung der Wahrscheinlichkeit eines Paketverlustes auf Grund einer der genannten vier Ursachen zu geben. Es bietet so die Grundlage, die Übertragungsparameter wie den Backoff besser entsprechend der Ursache für Paketverluste anzupassen.

Weiterhin werden Komponenten für Simulationen und Testbed-Evaluierungen entwickelt und dafür Elemente in C++ für das Click-Framework erstellt.

Für die darauf folgenden Simulationen und Testbed-Evaluierungen werden Szenarien entwickelt, die bestimmte Ursachen für Paketverluste provozieren. Dadurch kann überprüft werden, ob und wie genau eine bestimmte Paketverlustursache durch die erstellten Elemente erkannt wird.

Die Simulationen und Testbed-Evaluierungen haben dabei ergeben, dass sich beispielsweise die Paketverlustursache „Weak-Signal“ recht gut erkennen lässt. Die Ursache „Hidden-Nodes“ ist dagegen nicht immer gut zu erkennen, da „In-Range-Kollisionen“ und „Non-Wifi-Störungen“ die Erkennung dieser Ursache beeinflussen.

Abstract

Wireless communication is a widely-used and almost ubiquitous method for transmitting data and many devices support the wireless communication over 802.11 networks.

This diploma thesis examines the causes of packet losses and inefficient usage of medium time in IEEE 802.11 networks. The goal is the classification of packet losses and the estimation of the causes of packet losses with the help of software elements that will be developed.

Packet losses in IEEE 802.11 networks have negative effects on the network performance. These packet losses can have different causes like too weak signals or too strong electromagnetic noise, collisions caused by stations sending data simultaneously or sources of interference nearby.

There are various mechanisms to reduce packet loss. But these mechanisms ignore the exact causes, so their usage could be inefficient and in some cases even counterproductive. For example increasing the backoff reduces the probability of collisions caused by several senders transmitting data simultaneous. But the increased backoff does not prevent packet losses caused by weak signals.

By understanding what the exact causes of the occurrent packet losses are the mechanisms for reducing packet loss can be applied more accurately. The transmission parameter can be adjusted precisely, thus reducing packet loss.

This thesis focuses on packet losses caused by "hidden nodes", "inrange collisions", "weak signal" and "non wifi signals". In addition, the probability of packet losses caused by one of the four mentioned causes above will be estimated. This can be the basis for better adaption of the transmission parameters like the backoff according to the cause of packet losses.

Furthermore, the necessary components will be developed and elements implemented in C++ for the click frame work.

For the following simulations and test bed evaluations scenarios will be developed to provoke certain reasons of packet loss. With the help of those scenarios it can be tested if and how exact a certain source of packet loss is detected by the developed elements.

The simulations and test bed evaluations have shown that for instance the packet loss reason "weak signal" can be detected quite well. In contrast it is not always easy to detect the packet loss reason "hidden nodes" because of occurring "inrange collisions" and "non wifi disturbances" that influenced the recognition.

Inhaltsverzeichnis

1 Einleitung **1**
1.1 Motivation . . . 1
1.2 Ziel der Arbeit . . . 2
1.3 Aufbau der Arbeit . . . 3

2 Grundlagen **5**
2.1 Einführung IEEE-802.11 . . . 5
2.1.1 Zugriff auf das Übertragungsmedium . . . 5
2.1.2 802.11-Frames . . . 9
2.2 Ursachen für Paketverluste . . . 12
2.2.1 schwaches Signal . . . 12
2.2.2 In-Range-Kollision . . . 13
2.2.3 Hidden-Node . . . 15
2.2.4 Exposed-Node . . . 16
2.2.5 Nachbarkanalstörung (Adjacent-Channel-Interference, ACI) 17
2.2.6 Interferenzen durch Non-Wifi-Geräte . . . 18

3 Erkennung von Ursachen von Paketverlusten **21**
3.1 Weak-Signal . . . 21
3.2 In-Range-Kollisionen . . . 22
3.3 Hidden-Node . . . 23
3.4 Non-Wifi . . . 25
3.5 Datenspeicherung . . . 26

4 Evaluierung **29**
4.1 Paketverluste durch schwache Signale (Weak-Signal) . . . 29
4.1.1 Stationäre Szenarien . . . 30
4.1.2 Szenario mit Mobilität, Verkleinerung der Distanz . . . 38
4.1.3 Szenario mit Mobilität, Vergrößerung der Distanz . . . 43
4.2 Paketverluste durch In-Range-Kollisionen . . . 48
4.2.1 Zwei Nachbarn . . . 48
4.2.2 Fünf Nachbarn . . . 50
4.2.3 Zehn Nachbarn . . . 51
4.2.4 Zwanzig Nachbarn . . . 52
4.2.5 Auswertung . . . 54
4.3 Paketverluste durch Hidden-Nodes . . . 56
4.3.1 Ein Hidden-Node . . . 56
4.3.2 Zwei Hidden-Nodes . . . 61
4.3.3 Vier Hidden-Nodes . . . 63

4.3.4 Auswertung 66
4.4 Paketverluste durch Non-Wifi-Störungen 68
4.4.1 Two-Ray-Ground-Reflection-Model 68
4.4.2 Shadowing-Model 69
4.4.3 Auswertung 70
4.5 Szenarien mit Mobilität 71
4.5.1 Hidden-Node zu In-Range 71
4.5.2 In-Range zu Hidden-Node 75
4.5.3 Hidden-Node zu In-Range zu Hidden-Node 79
4.5.4 Auswertung 83
4.6 Testbed 85
4.6.1 Weak-Signal-Messung 85
4.6.2 In-Range-Messung 86
4.6.3 Hidden-Node-Messungen 87
4.6.4 Auswertung 88

5 Zusammenfassung **91**
5.1 Ergebnisse 91
5.2 Ausblick 92

Abkürzungsverzeichnis **95**

Literaturverzeichnis **97**

Abbildungsverzeichnis **103**

1 Einleitung

1.1 Motivation

WLAN, auch Wi-Fi oder Wifi in einigen Ländern genannt, ist eine Technik, um Computer per Funk zu vernetzen. Als Standard für diese Technik wird die 802.11-Normenfamilie des **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers (IEEE)-802.11 verwendet.

Für die Übertragung von Daten zwischen den Teilnehmern eines **W**ireless **L**ocal **A**rea **N**etwork (WLAN) (hier als WLAN-Stationen bezeichnet) werden die zu übertragenden Daten in kleine Einheiten aufgeteilt und in Datenpakete verpackt. Diese Datenpakete werden dann über das von allen Stationen gemeinsam genutzte Funkmedium zum jeweiligen Empfänger gesendet und dort wieder zusammengesetzt.

Die Entwicklung dieser Technik schreitet schnell voran und erreicht inzwischen Datenraten, die kabelgebundenen Netzwerken nicht nachstehen. Wird heute ein neuer Internetanschluss bereitgestellt, findet sich in den Modems der Internetprovider häufig zusätzlich ein WLAN-Router, mit dem Computer kabelunabhängig auf das Internet zugreifen können. Dadurch haben sich privat betriebene WLAN-Netze stark verbreitet. Zusätzlich bieten immer mehr Internetprovider WLAN-Hotspots für ihre Kunden an und selbst kostenloser Internetzugang per WLAN wird in einigen Städten eingeführt [ONL12], [Bor12]. In Unternehmen werden WLAN-Netzwerke aufgebaut, um beispielsweise Konferenz- und Besprechungsräume mit drahtlosen Internet zu versorgen und so allen Teilnehmern den Zugriff auf wichtige Informationen zu ermöglichen, und in vielen Universitäten und Hochschulen existieren ebenfalls WLAN-Netzwerke, um Mitarbeitern und Studierenden den Zugriff auf das Internet unabhängig von ihren jeweiligen Standorten zu ermöglichen.

So hat sich WLAN zu einer weit verbreiteten und fast allgegenwärtigen Technik entwickelt, die Menschen ortsunabhängig den Zugriff auf das Internet ermöglicht.

Durch die weite Verbreitung von WLAN kommt der Nachteil von Funknetzwerken zum Tragen, dass die Übertragung der Daten nicht auf einen eng begrenzten Raum wie bei Netzwerkkabeln beschränkt ist und das Übertragungsmedium zwischen allen Teilnehmern aufgeteilt werden muss. WLAN-Signale breiten sich frei im Raum aus, wodurch sich die Reichweite und Ausbreitung des Funknetzes kaum kontrollieren lassen. Dadurch kann es bei vielen WLAN-Netzwerken mit vielen konkurrierenden WLAN-Stationen zu gegenseitiger Beeinflussung und gegenseitigen Störungen kommen. Gerade innerhalb eines einzigen WLAN-Netzwerkes, welches nur einen einzigen Funkkanal nutzt, kann es durch mehrere sendende WLAN-Stationen zu gegenseitigen Störungen kommen, wenn mehrere Stationen versuchen, gleichzeitig Datenpakete zu senden. Das eingesetzte **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance (CSMA/CA)-Protokoll, welches den Zugriff auf das Medium regelt, kann

diese Störungen nicht vermeiden sondern nur mindern. Auch können Störungen durch andere Geräte wie zum Beispiel Mikrowellenherde verursacht werden, was ebenfalls durch das CSMA/CA-Protokoll nicht vermieden werden kann.

Treten die eben genannten Störungen auf, kann es passieren, dass Datenpakete nicht korrekt übertragen werden und es zu sogenannten Paketverlusten kommt. Werden diese erkannt, weil der Sender keine Empfangsbestätigung für die gesendeten Daten erhält, werden die fehlerhaft übertragenen Pakete so lange erneut gesendet bis diese Datenpakete den Empfänger unbeschadet erreicht haben oder die maximale Anzahl der Wiederholungen erreicht wird.

Wollen viele Stationen, die sich alle in Empfangsreichweite befinden Daten per WLAN senden, kann es zu Engpässen kommen, da auf einer Frequenz immer nur eine Station gleichzeitig senden kann. Wenn durch viele Paketverluste viele Datenpakete mehrmals gesendet werden müssen, wird das Medium durch die wiederholten Übertragungen mehr und mehr ausgelastet, und der effektive Durchsatz sinkt. Das Netzwerk ist überlastet.

Um Paketverluste zu reduzieren, gibt es verschiedene Methoden: beispielsweise kann durch die Wahl der Modulation und Kodierung der Signale die Datenübertragung robuster gemacht werden, was allerdings durch eine niedrigere Datenrate erkauft wird.

Um viele verschiedene Stationen in einem WLAN-Netzwerk den Zugriff zu ermöglichen, kann vor dem Senden eine zufällige Zeitspanne gewartet werden. Dieses Backoff-Verfahren verringert die Wahrscheinlichkeit, dass zwei Stationen gleichzeitig senden und es so zu Paketkollisionen kommt.

All die verschiedenen Methoden zur Paketverlustreduzierung haben den Nachteil, dass sie nur an einem Punkt ansetzen und es vorkommen kann, dass nicht vorhandene Ursachen für Paketverluste bekämpft werden. Zum Beispiel kann die Reduzierung der Datenrate Paketverluste durch Signale, welche durch Dämpfung zu schwach empfangen werden, verringern. Kollisionen durch gleichzeitig sendende Stationen lassen sich mit der Reduzierung der Datenrate nicht verringern.

Wäre dagegen bekannt, welche Ursachen Paketverluste in einer bestimmten Umgebung haben, ließen sich die Methoden der Paketverlustreduzierung gezielt einsetzen und so die Paketverluste verringern. Dadurch ließen sich erneute Übertragungen von Datenpaketen vermeiden und der Datendurchsatz für alle Stationen erhöhen.

1.2 Ziel der Arbeit

Diese Arbeit beschäftigt sich mit der Klassifizierung von Paketverlusten in 802.11-Netzwerken.

Es soll untersucht werden, ob und in wie weit es möglich ist, Ursachen von Paketverlusten zu ermitteln.

Ein weiterer Punkt ist die Untersuchung, in wie weit lokal gesammelte Statistiken für die Klassifizierung der Ursachen ausreichen und ob zusätzliche kooperative Statistiken einen weiteren Nutzen für die Erkennung haben und diese genauer machen.

Dazu werden im Click-Framework (siehe Seite 21) Elemente in C++ implementiert, mit deren Hilfe die Klassifizierung erfolgen wird. Mit Hilfe eines Netzwerksi-

mulators werden dann verschiedene Netzwerkumgebungen simuliert. Des weiteren werden Messungen im Testbed durchgeführt. In den Messungen und Simulationen werden bestimmte Ursachen für Paketverluste (Kollisionen, schwache Signale) provoziert. So kann gezielt geprüft werden, ob und wie genau eine bestimmte Fehlerklasse von den erstellten Elementen erkannt wird. Die in den Simulationen und durch die Messungen gewonnenen Daten werden dann ausgewertet und analysiert.

1.3 Aufbau der Arbeit

Das zweite Kapitel beginnt mit einer kurzer Einführung in die Grundlagen der IEEE-802.11-Normenfamilie und gibt dann eine Übersicht über die möglichen Ursachen für Paketverluste. Im dritten Kapitel werden dann die Methoden zur Erkennung und Klassifizierung der Ursachen der Paketverluste beschrieben, sowie auf die Möglichkeiten der Hardware eingegangen. Das vierte Kapitel zeigt die Evaluierung der Methoden. Dabei werden die Szenarien im Simulator und im Testbed beschrieben und die Ergebnisse dargelegt und diskutiert. Im fünften Kapitel wird die Arbeit zusammengefasst und ein Ausblick gegeben.

2 Grundlagen

2.1 Einführung IEEE-802.11

Im Juni 1997 wurde von der IEEE im Rahmen des 802-Standards ein Standard für drahtlose Funknetzwerke mit der Bezeichnung 802.11 veröffentlicht und zu einer ganzen Familie von Standards für WLAN weiterentwickelt. In den 802.11-Standards wird der Zugriff auf das Übertragungsmedium definiert, was im OSI-Modell den Schichten eins (Physical Layer bzw. Bitübertragungsschicht) und zwei (Data Link Layer bzw. Sicherungsschicht) entspricht. Die Schicht zwei wird in den 802-Standards nochmals in zwei Unterschichten unterteilt, die als **L**ogical **L**ink **C**ontrol (LLC)-Schicht und **M**edium **A**ccess **C**ontrol (MAC)-Schicht bezeichnet werden.

Der Ursprungsstandard 802.11 wurde im Juni 1997 verabschiedet und definiert Übertragungsraten von 1 und 2 MBit/s. Als Übertragungsmedium ist sowohl eine Funkübertragung im 2,4-GHz-Mikrowellenbereich als auch eine optische Übertragung im **I**nfra**r**otbereich (IR) ($\lambda = 850 - 950\,\text{nm}$) spezifiziert. Das 2,4 GHz-Band ist das so genannte **I**ndustrial, **S**cientific and **M**edical (ISM)-Band, welches weltweit genehmigungs- und lizenzfrei für industrielle, wissenschaftliche und medizinische Zwecke genutzt werden darf. Die optische Übertragung wird nur der Vollständigkeit halber genannt, da im Moment keine Geräte bekannt sind, welche die Infrarotübertragung implementieren.

Für die Bitübertragung werden im 802.11-Standard zwei Frequenzspreizverfahren spezifiziert: zum einen **F**requency **H**opping **S**pread **S**pectrum (FHSS) und zum anderen **D**irect **S**equence **S**pread **S**pectrum (DSSS). In späteren Erweiterungen wurde zusätzlich **O**rthogonal **F**requency **D**ivision **M**ultiplexing (OFDM) eingeführt. Auf Grund der mehrfachen Erweiterungen der Ursprungsform wird der ursprüngliche 802.11-Standard so gut wie nicht mehr in aktuellen Produkten genutzt. Da aber alle erweiterten Standards der 802.11-Familie auf der Ursprungsform aufbauen und grundsätzliche Eigenschaften, wie zum Beispiel der Zugriff auf das Übertragungsmedium, in der Ursprungsform definiert wurden, findet der Ursprungsstandard hier Erwähnung.

2.1.1 Zugriff auf das Übertragungsmedium

Stationen die gemeinsam ein Netzwerk nutzen wollen, benötigen einen Mechanismus, der den Zugriff auf das Übertragungsmedium, sei es drahtgebunden (elektrische Kabel oder Lichtwellenleiter) oder drahtlos (vorwiegend elektromagnetische Wellen), reguliert, um ohne Störungen Informationen übertragen zu können. In den

802-Standards werden Informationen vor dem Senden geteilt und in einzelne Datenpakete verpackt, welche dann über das Übertragungsmedium gesendet und vom Empfänger wieder zusammengesetzt werden.

Um den Zugriff auf das Medium zu regulieren haben sich das Token-Verfahren, wahlfreier Zugriff und verschiedene Multiplex-Verfahren etabliert. Die Token-Verfahren IEEE-Standards Token-Bus (IEEE 802.4) und Token-Ring (IEEE 802.5) wurden inzwischen von der IEEE zurückgezogen [D'A12]. Dabei handelt es sich um eine im Netzwerk zirkulierende Sendemarke, welche der Station, die diese besitzt, das Recht Datenpakete zu senden einräumt (Abbildung 2.1).

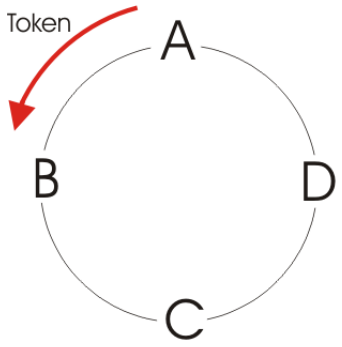

Abbildung 2.1: Token Ring

Das ALOHA-System der University of Hawai'i nutzte einen wahlfreien Zugriff auf das Medium, indem jede Station sendete sobald Datenpakete vorlagen. Sendeten mehrere Stationen gleichzeitig, kam es zur Kollision und die Empfangsbestätigung für die gesendeten Pakete blieb aus. Daraufhin sendeten beide Stationen nach einer zufälligen Zeit erneut ihre Pakete. [Abr70] (Abbildung 2.2).

Die Multiplexverfahren teilen die Zugriffe auf das Medium auf. Dies geschieht durch Einteilung der Zugriffszeiten, auch als Zeitmultiplex oder **T**ime **D**ivision **M**ultiple **A**ccess (TDMA) bezeichnet, durch Teilung des Mediums in verschiedene Frequenzen, Frequenzmultiplex oder **F**requency **D**ivision **M**ultiple **A**ccess (FDMA) oder durch unterschiedliche Spreizungen und Kodierungen der Signale, welches als **C**ode **D**ivision **M**ultiple **A**ccess (CDMA) bekannt ist [AMM+99].

In 802.11-Netzwerken wird das verfügbare Frequenzspektrum in 20 bis 160 MHz breite Kanäle, je nach Funkstandard und Konfiguration, aufgeteilt. Ein Kanal teilen sich verschiedene Stationen, um darüber Datenpakete auszutauschen. Für den Zugriff auf das Medium, also in diesem Fall, den 20 bis 160 MHz breiten Kanal, kann entweder **P**oint **C**oordination **F**unction (PCF) oder **D**istributed **C**oordination **F**unction (DCF) genutzt werden.

Bei der Verwendung von PCF übernimmt im Gegensatz zu DCF eine zentrale Station die Kontrolle über den Zugriff auf das Medium und koordiniert durch Polling der einzelnen Stationen den Zugriff, schaltet aber immer wieder zwischendurch auf DCF um [G+07]. PCF wird recht selten implementiert, so dass meist DCF für den Zugriff auf das Medium genutzt wird.

Da DCF keine koordinierende Stelle für den Zugriff auf das Medium hat, ist es notwendig Paketkollisionen mit Hilfe von **C**arrier **S**ense **M**ultiple **A**ccess (CSMA)

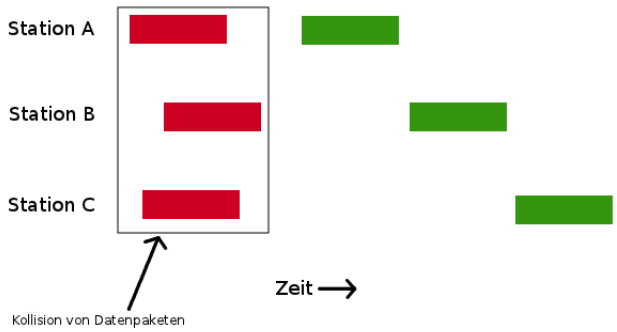

Abbildung 2.2:

wahlfreier Zugriff im ALOHA-System
rot: Pakete mit Kollisionen, grün: Pakete ohne Kollisionen

zu vermeiden. Dafür wird das aus drahtgebundenen Netzen bekannte Verfahren in angepasster Form eingesetzt.

In drahtgebundenen Netzwerken werden für den gemeinsamen Zugriff auf das Übertragungsmedium unter anderem das CSMA-Verfahren eingesetzt. CSMA fordert von einer Station, die Informationen senden möchte, vor der Übertragung zu prüfen, ob das Übertragungsmedium belegt ist, die sogenannte Trägerprüfung oder auch Carrier-Sensing genannt. Solange das Übertragungsmedium nicht frei ist, darf nicht gesendet werden. Dadurch wird verhindert, dass laufende Übertragungen von anderen Stationen im Netzwerk gestört werden. Trotz der Überprüfung des Übertragungsmediums kann es zu gleichzeitigen Aussendungen zweier oder mehrere Stationen kommen. Denn wenn zwei (oder mehr) Stationen das Übertragungsmedium prüfen und feststellen, dass es nicht belegt ist und beide Stationen kurz darauf zum gleichen Zeitpunkt ihre Übertragung starten, kommt es zu einer sogenannten Kollision.

Um solchen Kollisionen zu verhindern, kann **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **R**esolution (CSMA/CR) eingesetzt werden, indem unter Anwendung von Bitarbitrierung die Station mit der höchsten Priorität ihre Informationsübertragung beenden darf. Dieses Verfahren wird beispielsweise bei Feldbussen, wie dem CAN-Bus, eingesetzt. Allerdings ist das Protokoll recht aufwändig zu implementieren, da jede Station eine bestimmte Priorität zugewiesen bekommen muss und diese möglichst nicht doppelt vergeben werden darf.

Eine andere Möglichkeit mit Kollisionen umzugehen ist **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection (CSMA/CD). Durch Messung des Spannungspegels am Übertragungsmedium kann erkannt werden, ob gleichzeitig mehr als eine Über-

tragung stattfindet. Ist der Spannungspegel höher als die Ausgangsspannung des gesendeten Signals, wird die Aussendung sofort gestoppt. Danach wird eine zufällig ausgewählte Zeitspanne lang gewartet und das Übertragungsmedium geprüft, ob es frei ist, bevor ein erneuter Übertragungsversuch gestartet wird. Dadurch wird mit großer Wahrscheinlichkeit verhindert, dass es erneut zu einer Kollision kommt, da beide Stationen unterschiedlich lange vor ihrem nächsten Übertragungsversuch warten.

Diese Verfahren haben sich bei drahtgebundenen Übertragungsmedien bewährt. Da sich aber der Zugriff auf ein drahtloses Übertragungsmedium in einigen Punkten fundamental von dem eines drahtgebundenen unterscheidet, lassen sich die oben genannten Verfahren nicht einfach auf den 802.11-Standard übertragen.

Wie in [G+09] beschrieben, hat ein drahtloses Übertragungsmedium keine festen Grenzen, die Stationen vom Datenempfang ausschließen könnten. Der Zugriff auf das Übertragungsmedium ist nicht vor anderen Signalen, mit denen sich das Übertragungsmedium geteilt wird, geschützt. Die Datenübertragung ist wesentlich unzuverlässiger als über ein drahtgebundenes Übertragungsmedium und die Netzwerktopologie kann dynamisch sein. Zwei Sender können sich in Empfangsreichweite eines Empfängers befinden, nehmen sich gegenseitig jedoch nicht wahr. Dadurch kann es trotz CSMA zu Kollisionen kommen. Nicht auszuschließen sind außerdem Interferenzen durch andere 802.11-Netzwerke, die in der selben Umgebung funken, wobei es keinen Unterschied macht, ob die anderen 802.11-Netzwerke auf dem gleichen oder anderen Kanälen funken. Auch können Störungen durch andere Geräte wie Mikrowellenherde oder Bluetoothgeräte auftreten. Außer in kontrollierten Umgebungen ist es oft nicht möglich, den störungsfreien Betrieb eines Funknetzwerkes zu garantieren. Daher muss ein 802.11-Netzwerk mit den auftretenden Problemen umgehen können.

Der 802.11-Standard nutzt für den gemeinsamen Zugriff auf das Übertragungsmedium, ähnlich wie in drahtgebundenen Netzwerken, ein CSMA-Verfahren. Das heißt vor dem Senden wird ebenfalls erst geprüft, ob das Funkmedium belegt ist und erst wenn es frei ist, werden Datenpakete gesendet. Da die Radios nicht duplexfähig sind (gleichzeitiges Senden und Empfangen), können Kollisionen während des Sendens nicht erkannt werden. Das Collision-Detection-Verfahren kann daher nicht angewendet werden. Die Datenpakete zweier gleichzeitig sendender Stationen überlagern sich, so dass der Empfänger die Information nicht dekodieren kann. Das ausgesendete Datenpaket wird auf Grund der fehlenden Kollisionserkennung komplett gesendet, wird aber bei Empfänger von dem Datenpaket des anderen Senders überlagert. Durch Interference-Cancellation, wie in beispielsweise in [HAAW07] und [GPK09] beschrieben, lassen sich mit einigem Aufwand Kollisionen erkennen.

Da die Erkennung von Kollisionen aufwändig ist, wird versucht, die Wahrscheinlichkeit von Kollisionen mit Hilfe von CSMA/CA zu minimieren. Dazu wird, nach dem das Übertragungsmedium als frei erkannt wird, eine zufällige Zeitspanne aus dem Backoff-Intervall gewartet und danach die Informationsübertragung gestartet. Sollte es zu einer Kollision kommen, wird das Backoff-Intervall vergrößert, so dass die Wahrscheinlichkeit für Kollisionen sinkt. Eine erfolgreiche Übertragung wird im Anschluss von der Empfangsstation quittiert, wodurch die vollständige Übertragung der Daten sichergestellt werden kann [G+07].

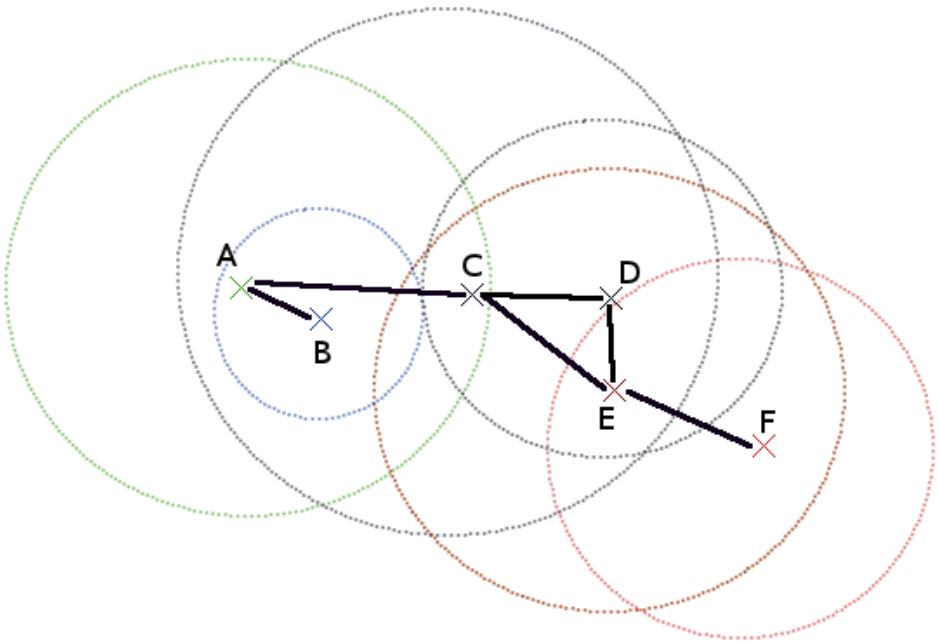

Abbildung 2.3: Funknetzwerk

Trotz CSMA/CA ist die Wahrscheinlichkeit von Kollisionen nicht null. Je mehr Stationen gleichzeitig in einem Funknetzwerk aktiv sind, desto wahrscheinlicher findet eine Kollision statt und ein Datenpaket muss erneut übertragen werden, was immer dann geschieht, wenn nach Ablauf einer bestimmten Zeit die Empfangsbestätigung des Empfängers nicht beim Sender eingetroffen ist. Wobei es dabei unwichtig ist, ob das gesendete Datenpaket oder die Empfangsbestätigung nicht korrekt übertragen wurde.

Empfangsbestätigungen werden laut dem 802.11-Standard nur bei Unicast-Übertragungen, also bei Punkt-zu-Punkt-Übertragungen, gesendet. Bei Broadcast-Übertragungen, die an alle Stationen gesendet werden, sind Empfangsbestätigungen nicht vorgesehen [G+07]. Kommt es während der Übertragung eines Broadcast-Paketes zu einer Kollision, kann diese Kollision nicht entdeckt werden.

2.1.2 802.11-Frames

Wie bereits auf Seite 5 erwähnt wurde, spezifiziert der 802.11-Standard den Zugriff auf die **phy**sische Schicht (PHY)-Schicht, sowie die zwei Unterschichten MAC-Layer und LLC-Layer. Frames auf PHY-Ebene sind je nach verwendetem Mediumszugriff (FHSS, IR, OFDM, DSSS) unterschiedlich.

Das Frame-Format bei FHSS besteht aus einer Präambel mit einem 80 Bit langen Sync-Feld und dem 16 Bit langen **S**tart **F**rame **D**elimiter (SFD). Danach folgt der **P**hysical **L**ayer **C**onvergence **P**rocedure (PLCP)-Header mit drei Feldern. Die Länge des **P**LCP **S**ervice **D**ata **U**nit (PSDU) wird im 12 Bit langen

PSDU-Length-Word-Field gespeichert. Im vier Bit langen PLCP-Signaling-Field wird die Datenrate bestimmt und zuletzt kommt noch das 16 Bit lange Header-Error-Correction-Field, welches für die Fehlerkorrektur zuständig ist. Hinter dem Header folgt dann der PSDU. Weitere Details sind in [G+07, S. 487] zu finden.

Der Zugriff auf das Medium im Bereich des infraroten Spektrums sei hier nur kurz der Vollständigkeit halber erwähnt. Die Frames bestehen ebenfalls aus Präambel, Header und PSDU. Weitere Details sind in [G+07, S. 575] zu finden.

Im DSSS besteht ein Frame aus der PLCP-Preamble, dem PLCP-Header und der **M**AC **P**rotocol **D**ata **U**nit (MPDU) (Siehe Abbildung 2.4).

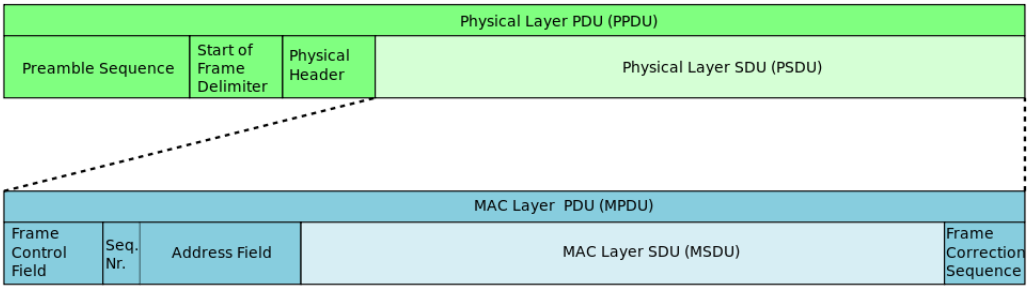

Abbildung 2.4: PPDU und MPDU für DSSS

Die Preamble besteht aus einem Sync-Field, welches vom Empfänger für die Synchronisierung genutzt werden kann [G+07, S. 538] und SFD-Field, welches den Start des Headers anzeigen soll [G+07, S. 538].

Der Header besteht aus vier Feldern, welche unter anderem die Datenrate, die Länge des Paketes und eine Checksumme enthalten [G+07, S. 539].

Das Format für OFDM-Frames beginnt ebenfalls mit einer Präambel, die zwei Trainingssequenzen enthält, von denen zuerst die kürzere zehn Mal wiederholt wird und dann die längere zwei Mal wiederholt wird. Die kurze Sequenz wird zur Signalerkennung, zeitlichen Synchronisierung und groben Frequenzanpassung bei Empfänger eingesetzt. Die lange Sequenz wird dann zur Frequenzfeinabstimmung genutzt. Bei einem 20 MHz breiten Kanal dauert die Übertragung 16 μs. Für jede Halbierung der Kanalbreite verdoppelt sich die Übertragungszeit. Danach folgt das SIGNAL-Field, in welchem der Modulationstyp und die Kodierungsrate und die Länge des restlichen Frames festgelegt wird. Das SIGNAL-Field wird mit der robustesten Kodierung übertragen, die alle OFDM-Stationen verstehen, sodass jede OFDM-Station Länge und Datenrate des restlichen Frames erfährt, auch wenn es die folgende Kodierung nicht kennt. Als letztes kommt das DATA-Field, welches das Service-Field, die PSDU und Tail- und PAD-Bits beinhaltet. Weitere Details sind in [G+07, S. 591] zu finden. Das MPDU-Field beinhaltet den MAC-Layer, der wiederum aus einem Header-Teil und dem Frame-Body besteht.

Der MAC-Header setzt sich aus acht Feldern zusammen, wobei die ersten drei Felder (Frame Control, Duration/ID und Address 1) in jedem 802.11-Frame vor-

kommen, die restlichen fünf Felder werden nur für spezielle Frame-Typen bzw. Frame-Subtypen gebraucht. Im Frame-Control-Field wird neben der Protokollversion, für die 2 Bit zur Verfügung stehen, auch der jeweilige Frame-Typ und Frame-Subtyp angegeben. Für die drei verschiedenen Frame-Typen stehen 2 Bit zu Verfügung und für die Frame-Subtypen 4 Bit (pro Frame-Typ). Weitere Details sind in [G+07, S. 60ff] zu finden.

Die drei definierten Frame-Typen sind: Management-Frame, Control-Frame und Data-Frame. Management-Frames sind für Verwaltungsaufgaben im Netz zuständig, Control-Frames regeln den Zugriff auf das Übertragungsmedium und Data-Frames werden für die Übertragung von Daten eingesetzt. Interessant für die Fehleranalyse sind die Control-Frames und die Data-Frames. In den Control-Frames speziell die Subtypen RTS, CTS und ACK.

Die Länge eines Frames errechnet sich also aus der Länge der PLCP-Präambel (144 Bits), des PLCP-Headers (48 Bits) und der maximalen MPDU-Länge. Die Länge des MPDU errechnet sich aus der Länge des MAC-Headers (256 Bits) und der Länge des Frame-Bodies, die variabel ist, aber maximal 18432 Bits beträgt. Hinzu kommen noch Bits für Sicherheitsfunktionen und FCS mit 32 Bits. Damit wird eine maximale Länge von 18912 Bits (ohne Sicherheitsfunktionen) erreicht. In Anbetracht der Tatsache, dass meist 802.3-Ethernet-Frames transportiert werden, die eine **M**aximum **T**ransfer **U**nit (MTU) von 1500 Byte haben, ist es sinnvoll anzunehmen, dass der größte Frame-Body 12000 Bits nicht übersteigen wird. Das heißt, es kann davon ausgegangen werden, dass 802.11-Frames maximal 12800 Bit lang sind.

Unter dieser Voraussetzung lässt sich bei einer Bandbreite von 1 MBit/s direkt errechnen, wie lange das Funkmedium bei Übertragung eines solchen Frames blockiert ist:

$$\begin{aligned} 1\,MBit/s &= 1048576\,Bit/s \\ \frac{12800\,Bits}{1048576\,Bit/s} &= 12,2\,ms \end{aligned} \tag{2.1.1}$$

Während dieser maximal 12,2 ms kann es zu Störungen des Signals kommen und damit zu Übertragungsfehlern.

Für einen tieferen Einstieg in das Thema Wireless-LAN empfehlen sich [Gas05] und [Rec06], da beide Bücher detailliert die Grundlagen von 802.11-Netzwerken behandeln. Eine gute Übersicht über Grundlagen der drahtlosen Kommunikation bietet auch [TV05].

2.2 Ursachen für Paketverluste

2.2.1 schwaches Signal

Eine allgegenwärtige Störquelle bei Übertragungen von Signalen stellt das Rauschen dar. Dabei handelt es sich um Störungen in einem breiten Frequenzspektrum, die unter anderem durch die Hintergrundstrahlung, Wärmestrahlung oder auch durch die brownsche Molekularbewegung verursacht werden [Hor07] [Wol12b].

Dieses Rauschsignal hat meist eine relativ geringe Leistung. Wenn nun die Leistung eines Nutzsignals beim Empfänger ähnlich groß wie die Rauschleistung ist, also das Verhältnis zwischen Signal und Rauschen sehr gering ausfällt, ist es für den Empfänger schwer, das Nutzsignal aus dem allgemeinen Rauschen herauszufiltern. Das Verhältnis zwischen der mittleren Nutzsignalleistung und der mittleren Rauschleistung wird auch als **S**ignal to **N**oise **R**atio (SNR) bezeichnet. Jeder Empfänger hat eine bestimmte Empfindlichkeit mit der er ein Nutzsignal erkennen kann, welche sich durch den SNR ausdrücken lässt.

Signal to **N**oise plus **I**nterference **R**atio (SNIR) ist das Verhältnis der mittleren Leistung des Nutzsignals und der Summe von Rauschen und Interferenzen. Weak-Signal tritt genau dann auf, wenn der SNIR nicht ausreicht, um das Signal zu dekodieren. Dies ist abhängig von der Modulation.

Durch mehrere Faktoren kann Weak-Signal begünstigt werden. Zu nennen sind eine zu schwache Sendeleistung des Senders und zu großer Abstand zum Empfänger, da die Strahlungsintensität des ausgesandten Signals mit der Entfernung vom Sender quadratisch abnimmt, wie aus den Formeln (2.2.1) hervorgeht.

$$\begin{aligned} \text{Kugelfläche: } A &= \pi * d^2 \\ \text{Strahlungsintensität: } I &= \frac{P}{A} \\ \text{d: Durchmesser, P: Sendeleistung} & \end{aligned} \tag{2.2.1}$$

Da Antennen meist keine idealen isotropen Strahler sind, die eine gleichmäßige Sendeleistung in alle Raumrichtungen haben, können durch die Ausrichtung der Antennen Winkel mit geringerer Strahlungsintensität entstehen.

Eine weitere Ursache für Weak-Signal ist das Fading, womit Schwankungen der Signalstärke auf Grund von Interferenzen mit dem selben Signal oder Abschattungen bezeichnet werden. Interferenzen können durch Brechungen, Reflexionen, Mehrwegeausbreitung oder Dopplereffekte auftreten, wodurch sich die Phasen der elektromagnetischen Wellen, die beim Empfänger eintreffen verschieben können und dadurch sich teilweise auslöschend oder verstärkend beim Empfänger eintreffen.

Mit Paketverlusten in einem 802.11b-Mesh-Netzwerk beschäftigt sich [ABB+04]. Es wird festgestellt, dass in dem untersuchten Netzwerk die bedeutendste Ursache für Paketverluste Multi-Path-Fading darstellt.

Die Empfangsfeldstärke eines Signals kann durch den **R**eceived **S**ignal **S**trength **I**ndication (RSSI)-Wert, der aus den WLAN-Chips ausgelesen werden kann, ermittelt werden. Der RSSI-Wert gibt die Größe der empfangenen Energie an der Antenne an. Der RSSI-Wert ist dabei nur ein relativer Wert, dessen Genauigkeit nicht spezifiziert ist. [G+07, S. 489] Der Wertebereich umfasst bis zu 8 Bit, was

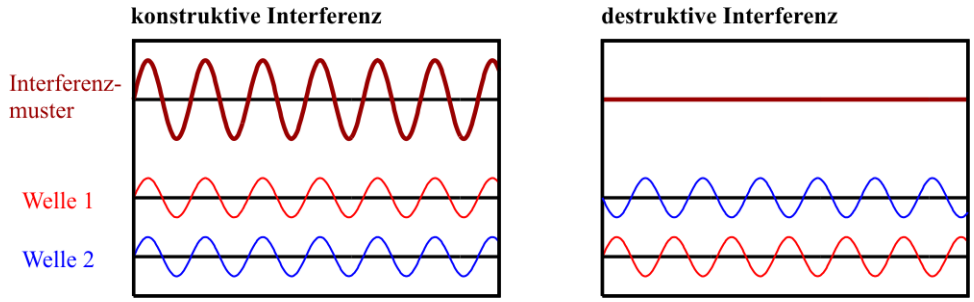

Abbildung 2.5: Interferenz zweier Sinuswellen

256 Stufen entspricht [G+07, S. 635], der aber je nach Hersteller nicht komplett ausgeschöpft wird und unterschiedlich implementiert wird [Bar02].

Die Wahrscheinlichkeit des Auftretens von Weak-Signal ist bei WLAN außerdem von der gewählten Datenrate abhängig, da bei geringeren Datenraten robustere Kodierungen der Informationen genutzt werden als bei höheren Datenraten und somit bei höheren Datenraten schwache Signalstärken eher zu Weak-Signal führen als bei geringeren Datenraten. Zusätzlich kann die Redundanz der Informationen für die jeweiligen Kodierungen erhöht werden und so die Wahrscheinlichkeit für Weak-Signal ebenfalls verringert werden.

Die Nutzdaten werden nach der 802.11-Standard durch eine Phasenmodulation (**B**inary **P**hase **S**hift **K**eying (BPSK)), bzw. einer Kombination aus Phasen- und Amplitudenmodulation (**Q**uadrature **A**mplitude **M**odulation (QAM)) auf das Trägersignal aufmoduliert. Je mehr Informationen pro Zeiteinheit aufmoduliert werden, desto höher ist die Wahrscheinlichkeit, dass bei schlechten Übertragungsbedingungen diese Informationen verloren gehen. Weniger robuste Modulationen benötigen einen höheren SNIR. Bei geringerer Informationsdichte lässt sich die Robustheit gegenüber Störungen erhöhen [Rö04, S. 49], [TV05, S. 72ff], [G+07, S. 615, 617].

Die Anpassung der Datenrate (Rate-Selection) kann empfängerbasiert (Receiver-Based-Rate-Selection) oder ohne Kenntnis der Empfängerfeldstärke nach Paketverlusten geschehen. Idealerweise sollte die Datenrate an die beim Empfänger gemessene Signalstärke angepasst werden. Wie in [LMT04] beschrieben, müsste für diese Receiver-Based-Rate-Selection allerdings der MAC-Layer angepasst werden, was recht aufwändig ist. So wird dem Standard entsprechend die Datenrate ohne Signalstärkeninformationen vom Empfänger ausgewählt.

Die Wahrscheinlichkeit für Weak-Signal lässt sich durch Beobachtungen des RSSI-Wertes und der Schwankungen des RSSI-Wertes prognostizieren, wenn man davon ausgeht, dass die Ausbreitungsbedingungen der Signale in beide Richtungen (Sender–Empfänger und umgedreht) annähernd symmetrisch sind. Selbst bei nicht ganz symmetrischen Bedingungen lassen sich die Tendenzen schwächer werdender Signale nutzen, um die Datenrate anzupassen.

2.2.2 In-Range-Kollision

In-Range-Kollisionen treten auf, wenn zwei (oder auch mehr) Stationen in Empfangsreichweite zum gleichen Zeitpunkt mit dem Senden beginnen. Wie in Kapitel

2.1.1 beschrieben, überlagern sich die Nutzsignale bei den Empfängern, sodass deren Informationen nicht mehr dekodiert werden können. Eine Erkennung von In-Range-Kollisionen ist ohne Fullduplexradio nicht direkt möglich und dritte Stationen können die auftretende Störung nicht eindeutig identifizieren.

Deshalb wird mit Hilfe des Collision-Avoidance-Verfahrens (siehe S. 8) die Wahrscheinlichkeit von In-Range-Kollisionen verringert, indem, nachdem das Medium frei ist, eine zufällige Zeitspanne vor dem Senden gewartet wird. Diese Zeitspanne wird Backoff-Zeit (Backoff Time) genannt. Wird das Medium während dieser Zeitspanne wieder als belegt erkannt, wird der Backoff-Zähler gestoppt und der aktuelle Wert des Zählers beibehalten. Sobald das Medium wieder als frei erkannt wird, wird nur die noch vom letzten Warten verbliebene Zeit gewartet und dann, vorausgesetzt das Medium ist noch frei, mit dem Senden begonnen.

Die Backoff-Zeit berechnet sich aus der SlotTime und einer Zufallszahl aus dem geschlossenem Intervall von 0 bis zur aktuellen Contention-Window-Größe. Die SlotTime hängt vom jeweiligen Physical-Layer (siehe S. 9) abhängt und beträgt zwischen $8\,\mu s$ (IR) und $50\mu s$ (FHSS) [G+07].

Die Contention-Window-Größe wiederum ist ein Wert aus dem geschlossenem Intervall von CW_{min} bis CW_{max}. CW_{min} und CW_{max} hängen ebenfalls vom verwendeten Physical-Layer ab. Wobei CW_{min} zwischen 15 (OFDM, FHSS) und 63 (IR) und CW_{max} bei 1023 liegen. [G+07]

Wird **E**nhanced **D**istributed **C**hannel **A**ccess (EDCA) eingesetzt, ist der CW_{min} je nach Verkehrsklasse $\frac{CW_{min}+1}{2} - 1$ für Video und $\frac{CW_{min}+1}{4} - 1$ für Sprache. CW_{max} liegt in der Verkehrsklasse Sprache bei $\frac{aCW_{min}+1}{2} - 1$ [G+07].

Die Contention-Window-Größe wird bei jedem fehlgeschlagenen Übertragungsversuch um die zweite Potenz minus eins erhöht, beginnend mit dem jeweiligen CW_{min}-Wert, bis der CW_{max}-Wert erreicht wird [G+07].

Die daraus resultierenden möglichen Contention-Window-Größen sind 3, 7, 15, 31, 63, 127, 255, 511 und 1023. Das heisst, mit jeder fehlgeschlagenen Übertragung wartet die Station im Mittel länger.

Dieses Verfahren senkt zwar die Wahrscheinlichkeit von In-Range-Kollisionen, kann sie aber nicht verhindern, da immer noch die Möglichkeit besteht, dass zwei Stationen aus dem Intervall der verschiedenen Backoff-Zeiten dieselbe Zeit auswählen.

Tritt eine Kollision auf, ist das Medium bis zu Ende der längsten Sendung der Stationen belegt. Alle an der Kollision beteiligten sendenden Stationen bemerken die fehlgeschlagene Übertragung nur dadurch, dass die Empfangsbestätigungen der Empfänger nicht eintreffen, was allerdings kein hinreichendes Kriterium für In-Range-Kollisionen ist.

Treten Kollisionen sehr häufig auf, verringert sich durch die notwendigen Neuübertragungen die effektiv genutzte Zeit auf dem Medium und damit auch die Datenrate.

Die Wahrscheinlichkeit für Paketverluste auf Grund von In-Range-Kollisionen lässt sich über die Backoff-Zeit und die Anzahl der Nachbarknoten abschätzen und die Parameter wie CW_{min} und CW_{max} können so entsprechend angepasst werden [KV08].

2.2.3 Hidden-Node

Hidden-Nodes, auch Hidden-Station oder Hidden-Terminals genannt, sind Stationen, die nicht von jeder anderen Station gehört werden können. Das Hidden-Node-Problem tritt auf, wenn eine Station A in der Empfangsreichweite einer zweiten Station B liegt. Station B liegt außerdem in der Sendereichweite einer dritten Station C, wobei sich die erste Station A und die dritte Station C gegenseitig nicht wahrnehmen können (Siehe Abbildung 2.6).

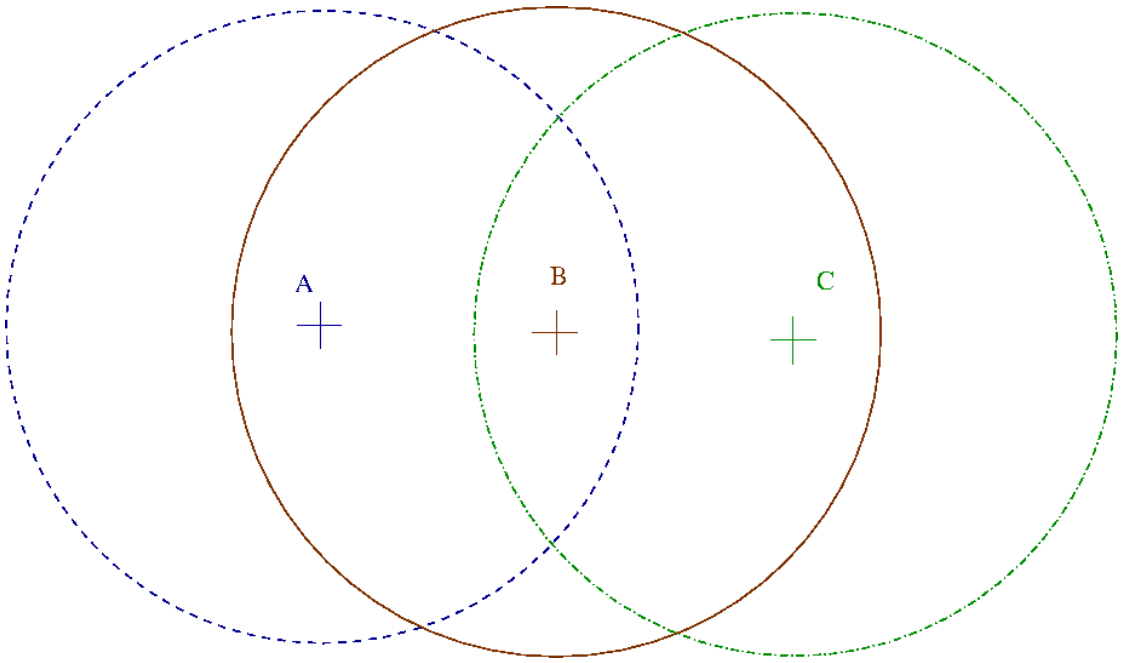

Abbildung 2.6: Hidden Node, A kann C nicht wahrnehmen

Senden jetzt die zwei Stationen A und C Frames (siehe Seite 9) an Station B, kann es zu Kollisionen kommen, da der Carrier-Sense-Mechanismus von CSMA/CA nicht funktioniert: Station A prüft, ob das Funkmedium belegt ist und beginnt, nachdem die Backoff-Zeit abgelaufen ist, mit dem Senden der Frames an Station B. Während Station A sendet, prüft Station C, ob das Übertragungsmedium belegt ist. Da Station A und Station C sich nicht hören können, wird von Station C das Übertragungsmedium als frei erkannt. Nach dem Ablauf der Backoff-Zeit fängt Station C ebenfalls an, Frames an Station B zu senden, wodurch es zu Überlagerungen der Signale bei Station B kommt und die Informationen der Nutzsignale der Stationen A und C von Station B aus den überlagerten Signalen nicht mehr dekodiert werden können.

Das Hidden-Node-Problem wird in [KKJ98] sehr übersichtlich behandelt. In [WZZN06] werden Hidden-Nodes speziell in 802.11-Netzwerken im Access-Point-Modus analysiert und mit Hilfe von Markov-Ketten ein analytisches Modell entwickelt und in [JKLS10] wird das Hidden-Node-Problem in 802.11-Netzwerken untersucht und dabei zwischen Situationen mit und ohne Carrier-Sensing unterschieden.

Eine abgeschwächte Form des Hidden-Node-Problems tritt auf, wenn das Signal des Hidden-Node zu schwach für eine Dekodierung des Signals ist (siehe Weak-Signal), aber der Carrier-Sense-Mechanismus noch Energie auf dem Übertragungsmedium detektieren kann. Dann lässt sich zwar nicht feststellen, für welche Stationen die Hidden-Node-Situation gilt, aber die Wahrscheinlichkeit von Kollisionen auf Grund von Hidden-Nodes sinkt. In diesem Falle kann dann das nachfolgend beschriebene Exposed-Node-Szenario auftreten, wie in [RCS03] dargestellt wird. Dort wird auch eine Lösung dieses Problems vorgeschlagen.

Wird eine Hidden-Node-Situation festgestellt, lässt sich die Kollisionswahrscheinlichkeit herabsetzen, indem die Kommunikation mit RTS/CTS abgesichert wird. Bevor die eigentlichen Daten-Frames ausgesendet werden, wird ein **R**eady **t**o **S**end (RTS)-Paket mit einer Länge von 352 Bit gesendet, worauf die Empfangsstation mit einem **C**lear **t**o **S**end (CTS)-Paket, welches 304 Bit lang ist, antwortet. Dabei wird die benötigte Übertragungszeit angegeben. Durch das CTS-Paket werden alle Stationen in Sendereichweite der Empfangsstation darauf hingewiesen, dass für eine bestimmte Zeit eine Datenübertragung stattfindet und der Kanal exklusiv für diese Übertragung reserviert wird [G+07].

Die Kollisionswahrscheinlichkeit auf Grund von Hidden-Nodes wird dabei allerdings nicht auf null reduziert, da das sehr kurze RTS-Paket immer noch durch die Aussendung eines Hidden-Node gestört werden kann. Die Wahrscheinlichkeit, dass das kurze RTS-Paket ohne Störungen übertragen wird, ist dabei wesentlich größer, als die Wahrscheinlichkeit ein langes Datenpaket ohne Störungen zu übertragen. Außerdem wird weniger Übertragungszeit durch die eventuelle Wiederholung des kurzen RTS-Paket benötigt, als durch die eines langen Datenpaketes.

Das zusätzliche Datenaufkommen für das RTS-CTS-Verfahren ist allerdings nicht zu unterschätzen, da jede Übertragung durch zwei weitere Pakete abgesichert wird und damit die Menge an übertragenen Nutzdaten sinkt. Wie aus Formel 2.2.2 hervorgeht, verlängert sich die Zeit in der das Medium belegt ist pro Datenpaket um 0,656 ms bei 1 MBit/s.

$$\begin{aligned} \text{RTS-CTS-Datenaufkommen: } & 352\,Bit + 304\,Bit = 656\,Bit \\ \text{Mediumszeit bei 1 MBit/s: } & 656 * 10^{-6}\,s = 0,656\,ms \end{aligned} \tag{2.2.2}$$

Sind keine Hidden-Nodes vorhanden, kann durch das Ausschalten des RTS-CTS Verfahren zusätzliche Übertragungszeit für Nutzdaten gewonnen werden.

2.2.4 Exposed-Node

Exposed-Nodes, auch Exposed-Stations oder Exposed-Terminals genannt, sind Stationen, welche Datenpakete an eine Station senden möchten, aber auf Grund von Kommunikation anderer Stationen unnötigerweise mit der Datenübertragung warten (siehe Abbildung 2.7), obwohl die Übertragung der wartenden Station andere Datenübertragungen nicht stören oder nur sehr gering stören würden, da die jeweiligen anderen Empfänger gar nicht innerhalb der Sendereichweite liegen. Station A könnte Daten an Station D senden, tut dies aber nicht, da Station B an Station C Daten sendet, wobei Station D Station B gar nicht wahrnehmen kann.

Dadurch kommt es zu einer ineffizienten Nutzung des Mediums und unnötiger Weise zu geringerem Durchsatz. Allerdings treten durch dieses Situation keine Paketverluste durch Kollisionen auf.

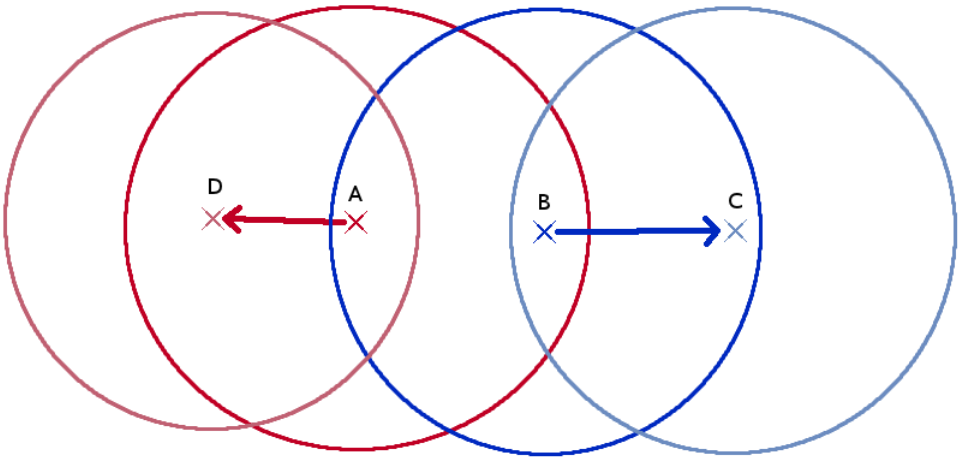

Abbildung 2.7: Exposed Node

Erkennen lässt sich ein Exposed-Node nur durch Kooperation. Wenn Stationen ihren Nachbarstationen mitteilen, welche Stationen sie hören können, lassen sich Exposed-Nodes erkennen.

Eine Möglichkeit das Exposed-Node-Problem zu umgehen, ist der Einsatz von RTS-CTS. Sendet eine Station ein RTS-Paket, antwortet der Empfänger mit einem CTS-Paket. Hört eine dritte Station nur das RTS- und das entsprechende Datenpaket, sofern die Datenrate den korrekten Empfang nicht verhindert (siehe S. 13), und kein dazugehöriges CTS-Paket, wäre es möglich, dass die dritte Station in Bezug auf die zwei anderen Station ein Exposed-Node ist. Diese dritte Station kann dann ihrerseits Datenpakete an eine vierte Station senden, ohne dass es zu Kollisionen kommt. Allerdings lässt sich nicht ausschließen, dass das CTS-Paket durch Kollisionen oder Interferenzen verloren gegangen ist, wodurch ein nicht vorhandenes Exposed-Node-Szenario angenommen würde und es so zu Kollisionen kommen könnte [RCS03] [RCS05].

2.2.5 Nachbarkanalstörung (Adjacent-Channel-Interference, ACI)

Nachbarkanalstörungen, auch Adjacent-Channel-Interference (ACI) genannt, beschreibt eine Art von Störungen, welche zu Problemen durch Aussendungen von 802.11-Stationen auf Nachbarkanälen führen kann, da sich die Kanäle im 802.11-Standard überlappen. Außerdem können durch Nahfeldeffekte bei zu dicht stehenden Antennen, oder durch elektrische Kopplungen Sendeenergien in die jeweiligen anderen Sender induziert werden. Da eine Antenne, wie in [Wol12a] ausführlich beschrieben, in der Rayleigh-Zone in einer Entfernung bis $\frac{(\text{Antennenausdehnung in m})^2}{(\text{Wellenlänge in m})_{*2}}$

nicht nur Energie abstrahlt, sondern auch wieder aufnimmt, hat das Auswirkungen auf zu nah stehende Sender.

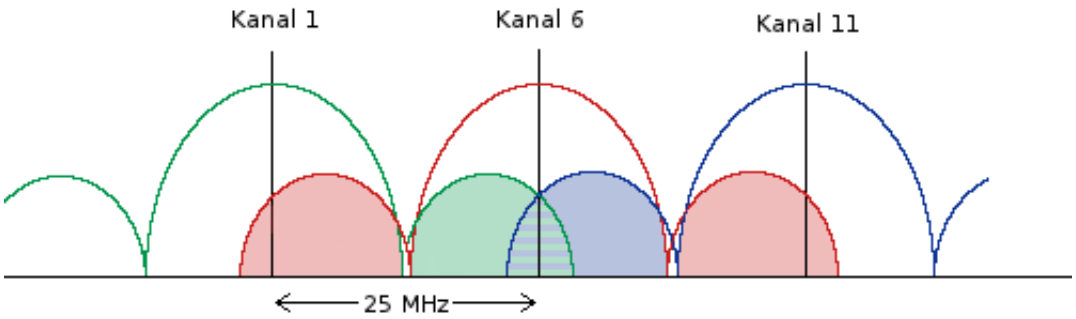

Abbildung 2.8: Nachbarkanalstörungen

Ein weiteres Problem besteht darin, dass selbst nicht-überlappende Kanäle, die dicht nebeneinander liegen, Energie in die jeweiligen Nachbarkanäle abgeben, wie in Abbildung 2.8 schematisch dargestellt. Dadurch können nahe Stationen, die auf Nachbarkanälen senden und empfangen, gestört werden [Gas05].

Sobald die empfangene oder induzierte Energie den Schwellwert der Carrier-Sense-Erkennung überschreitet, wird das Übertragungsmedium als belegt erkannt, obwohl auf dem eigentlichen Kanal keine Datenübertragung stattfindet und der Kanal eigentlich frei ist. Weiterhin kann es auch zu Störungen beim Empfang von Datenpaketen und dadurch zu Paketverlusten durch Kollisionen kommen [NZR08], [ZS11].

Um Nachbarkanalstörungen zu erkennen, könnte man die Belegung der benachbarten Kanäle prüfen und mit einer Statistik über empfangene Datenpakete auf dem eigenen Arbeitskanal und über die Häufigkeit der Empfangsenergieerkennung abgleichen. So ließen sich eventuell Nachbarkanalstörungen erkennen. Wobei es schwierig sein könnte die Nachbarkanalstörung von Störungen durch Non-Wifi-Geräte abzugrenzen, da auch Non-Wifi-Signale einen Anstieg der Empfangsenergieerkennung auslösen.

2.2.6 Interferenzen durch Non-Wifi-Geräte

Non-Wifi-Geräte funken nicht nach dem 802.11-Standard. Entweder nutzen sie eigene Übertragungsstandards, wie zum Beispiel Bluetooth, oder Hiperlan-Geräte, oder aber sie geben in den im 802.11-Standard definierten Frequenzen Störstrahlungen ab.

Dabei lassen sich die störenden Signale in schmal- und breitbandige Signale unterteilen. Der Übergang zwischen schmal- und breitbandige Signalen ist dabei nicht scharf abgegrenzt. In dieser Arbeit wird von breitbandigen Signalen ausgegangen, wenn die Bandbreite des Signals mehr als einen 802.11-Kanal belegt. Die

verschiedenen Bandbreiten der Kanäle sind in [G+07] und [G+09] zu finden. Hier wird von einem 20 MHz breiten Kanal ausgegangen.

Ein Beispiel für schmalbandige Signale sind Bluetoothgeräte, die eine relativ geringe Bandbreite für ihre Signale verwenden und ein Frequenzsprungverfahren nutzen. Dadurch werden abwechselnd nur kleine Frequenzbereiche gestört [G+05].

Andere störende Signalquellen können eine Bandbreite, die mehreren 802.11-Kanälen entspricht, haben und können so mehrere Kanäle gleichzeitig stören.

Weiter lassen sich die Non-Wifi-Signale kooperativen und nicht-kooperativen Geräten zuordnen. Kooperative Geräte nutzen einen Carrier-Sense-Mechanismus, der verhindert, dass laufende Übertragungen gestört bzw. unterbrochen werden. Nicht-kooperative Geräte besitzen keinen Carrier-Sense-Mechanismus und können dadurch laufende Übertragungen stören. Beispiele für nicht-kooperative Geräte sind Bluetoothgeräte [MCA03], Mikrowellen und Babyphones.

Den Einfluss von oft vorkommenden Störquellen in CSMA-Funknetzwerken untersucht [Tou01] genauer und beschreibt auch Möglichkeiten, die Auswirkungen zu reduzieren. Unter anderem wird vorgeschlagen, die Störeinflüsse von Mikrowellenherden durch Reduktion der Fragmentierung der Pakete zu verringern.

Allgemeiner wird in [GWGS07] der Einfluss von Geräten, die im 2,4 GHz-Band nicht nach dem IEEE-802.11-Standard arbeiten, untersucht, ebenso wie Geräte, die gezielt 802.11-Übertragungen stören.

Um generell Interferenzen durch Non-Wifi-Geräte zu entdecken, kann man zum Beispiel die Häufigkeit der Energieerkennung mit der Menge der empfangenen Pakete vergleichen und so die Größe der Interferenzen abschätzen, wie in [HMS10] beschrieben.

Würde man die Nachbarfrequenzen mit überwachen, ließen sich auch schmal- und breitbandige Störungen erkennen. Die genaue Art der Interferenz ließe sich eventuell an der Dauer und der Form des Signals festmachen, sofern die zeitliche und spektrale Auflösung der Hardware das hergeben. So weisen Bluetooth-Signale ein spezielle Sprungsequenz auf [G+05], die man erkennen könnte. Die Leckströme eines Mikrowellenherdes würden eine pulsartige Störung von 10 ms Dauer bei 2,45 Ghz verursachen, die eventuell auch entdeckt werden könnte [KE97].

3 Erkennung von Ursachen von Paketverlusten

Im vorherigen Kapitel wurde auf die Ursachen von Paketverlusten eingegangen. In diesem Kapitel soll für die vier Fehlerursachen Weak-Signal, In-Range-Kollisionen, das Hidden-Node-Problem und Non-Wifi-Signale Elemente entworfen werden, die für jede Station eine Statistik erstellen. Mit Hilfe dieser Statistiken soll dann die Wahrscheinlichkeit für eine bestimmte Ursache eines Paketverlustes, welcher bei der Übertragung von Datenpaketen zu einer anderen Station auftritt, abgeschätzt werden. Mit Hilfe dieser Daten könnten die Übertragungsparameter gezielt so eingestellt werden, dass nur die vorliegende Ursache für Paketverluste eingedämmt wird.

Für die Implementierung wird das Click-Framework verwendet. „Click ist ein modularer open-source Software-Router[...]“ [Sch06], welcher den Netzwerksimulator NS-2 [Ins12] nutzen kann, um mit dessen Hilfe Szenarien drahtloser Netzwerke zu simulieren. So lassen sich die erstellten Elemente evaluieren, ob und wie gut sich die Paketverlustursachen abschätzen lassen. Elemente für Click werden in C++ implementiert und lassen sich über eine Konfigurationsdatei sogenannte Click-Skripte miteinander verbinden [Koh00], [KMC+00].

Click lässt sich nicht nur mit NS-2 sondern ebenfalls als User-Space-Programm auf Rechnern verwenden. So kann Click im HWL-Testbed auf WLAN-Routern laufen [ZS12]. Dadurch können die Ergebnisse, die in Simulationen mit Hilfe von NS-2 gesammelt werden, mit Ergebnissen realer WLAN-Stationen verglichen werden.

3.1 Weak-Signal

Für die Berechnung der Wahrscheinlichkeit von Paketverlusten auf Grund von zu schwachen Signalen bzw. gestörten Signalen wird die Verteilung der RSSI-Werte der letzten empfangenen Pakete der jeweiligen Station benötigt. Dabei wird von der minimalen Datenrate von 1 MBit/s bzw. 6 MBit/s ausgegangen, sodass die robusteste Kodierung genutzt wird. Die Liste der RSSI-Werte stellt das Click-Element ChannelStats zur Verfügung. Aus der Liste der RSSI-Werte wird dann ein Histogramm erstellt, aus welchem sich dann die Verteilung der Werte ermitteln lässt. Die Tatsache, dass die RSSI-Werte nur relative Werte sind und die Implementierung herstellerabhängig macht, ist für den Vergleich der Werte innerhalb eines Chipsatzes unerheblich. Der Vergleich der Werte zwischen verschiedenen Chipsätzen ist ohne das Wissen der tatsächlichen Implementierung der Berechnung der RSSI-Werte nicht möglich.

Liegt das Histogramm mit den absoluten Häufigkeiten vor, werden daraus mit der Formel 3.1.1 die relativen Häufigkeiten berechnet.

$$\text{relative Häufigkeit: } h_i = \frac{H_i(x)}{n} \tag{3.1.1}$$

Aus der relativen Häufigkeiten können dann mit Hilfe der Formeln 3.1.2 der Erwartungswert, Varianz und die Standardabweichung berechnet werden.

$$\begin{aligned} \text{Erwartungswert: } \mu &= \sum_{i=0}^{n} x_i * h_i \\ \text{Varianz: } V(X) &= \sum_{i=0}^{n} (x_i - \mu)^2 * h_i \\ \text{Standardabweichung: } \sigma &= \sqrt{V(X)} \end{aligned} \tag{3.1.2}$$

Ist die Differenz von Erwartungswert und dreifacher Standardabweichung kleiner oder gleich null, wird von 25 Prozent Wahrscheinlichkeit für Paketverluste auf Grund von Weak-Signal ausgegangen.

Von 50 Prozent Wahrscheinlichkeit für Paketverluste wird ausgegangen, sobald die Differenz von Erwartungswert und doppelter Standardabweichung kleiner oder gleich null ist.

Wenn die Differenz von Erwartungswert und einfacher Standardabweichung kleiner gleich null sein sollte, wird von 100 Prozent für Paketverluste ausgegangen.

Liegt die Differenz von Erwartungswert und dreifacher Standardabweichung über null, wird die Wahrscheinlichkeit eines Paketverlustes auf Grund von Weak-Signal auf null Prozent geschätzt.

Die oben genannten Abstufungen der Wahrscheinlichkeitswerte von 0, 25, 50 und 100 Prozent haben sich experimentell als sinnvoll erwiesen. Feinere Abstufungen sind auf Grund des groben RSSI-Rasters nicht möglich.

Es wird hier davon ausgegangen, dass die Ausbreitungsbedingungen der Signale sowohl in Sender–Empfänger- als auch in Empfänger–Sender–Richtung annähernd symmetrisch sind. Da nur die RSSI-Werte empfangener Pakete, die die Empfängerstation gesendet hat wie zum Beispiel Ack-Pakete, vom Sender ausgewertet werden. Die Tendenzen der Entwicklungen der RSSI-Werte lassen sich aber auch bei nicht ganz symmetrischen Ausbreitungsbedingungen nutzen, um durch angepasste Datenraten Paketverluste zu verringern.

Für Stationen, die nicht direkt gehört werden können, die also nur als Empfänger von mitgehörten Paketen in Erscheinung treten, wird die Wahrscheinlichkeit eines Paketverlustes auf 100 Prozent gesetzt, da davon ausgegangen werden kann, dass Pakete, die an diese Stationen gesendet werden, nicht ankommen werden. Es handelt sich dabei um Hidden-Nodes (siehe auch S. 23).

3.2 In-Range-Kollisionen

Für die Abschätzung der Wahrscheinlichkeit von Paketverlusten durch In-Range-Kollisionen werden die Anzahl der direkten Nachbarstationen und

die aktuelle Größe des Contention-Windows, aus der der Backoff berechnet wird, benötigt. Die Anzahl der direkten Nachbarstationen kann dem vorhandenem Click-Element HiddenNodeDetection entnommen werden. Den Wert des aktuell verwendeten Contention-Windows findet man in den Strukturen des vorhandenen Click-Elements BRN2Device.

Bei der Berechnung der Wahrscheinlichkeit von Paketverlusten durch In-Range-Kollisionen wird angenommen, dass alle direkten Nachbarstationen sich gegenseitig hören können, das heißt, dass zwischen den einzelnen Nachbarstationen kein Hidden-Node-Szenario (siehe S. 15) oder Exposed-Node-Szenario (siehe S. 16) auftritt. Weiterhin wird angenommen, dass jeder Nachbarstation zu jedem Zeitpunkt Daten zum Senden vorliegen.

Die Wahrscheinlichkeit für Paketverluste infolge von In-Range-Kollisionen lässt sich mit Hilfe des Geburtstagsparadoxons berechnen. Nach [KV08] wird die Wahrscheinlichkeit für In-Range-Kollisionen mit der Formel 3.2.1 berechnet:

$$\text{In-Range-Kollision: } 1 - \prod_{i=0}^{n-1} \frac{c-i}{c} \tag{3.2.1}$$

c: Contention-Windows-Größe, n: Anzahl der Stationen

Diese Schätzung ist recht pessimistisch, da davon ausgegangen werden kann, dass in der Realität nicht alle Stationen gleichzeitig Daten zu senden haben. Damit deckt diese Schätzung aber den schlechtesten Fall ab.

In der Grafik 3.1 sieht man, dass bei konstanter Anzahl von Stationen mit größer werdendem Contention-Window, die Wahrscheinlichkeit für Kollisionen sinkt und bei gleichbleibendem Contention-Window und steigender Anzahl von Stationen, die Wahrscheinlichkeit für Kollisionen zunimmt.

3.3 Hidden-Node

Die Schwierigkeit Paketverluste auf Grund von Hidden-Nodes zu prognostizieren liegt darin, dass sich die Hidden-Nodes nur indirekt aufspüren lassen. Hinweise auf Hidden-Nodes erhält man, indem man die Zieladressen der von den Nachbarstationen empfangenen Pakete mit der Liste der direkt erreichbaren Nachbarstationen vergleicht. Enthält ein Netzwerkpaket eine Adresse, die nicht in dieser Liste der Nachbarstationen zu finden ist, könnte es sich um einen Hidden-Node handeln.

Die Anzahl der Nachbarn lässt sich wieder mit den vorhandenem Click-Element HiddenNodeDetection ermitteln. Für die Abschätzung der Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes wäre es von Vorteil, zu Wissen wie viele Datenpakete in einer bestimmten Zeit vom Hidden-Node zur Nachbarstation gesendet wurden. Für eine grobe Abschätzung lassen sich die Ack-Pakete, die zum Hidden-Node gesendet werden, mitzählen und damit die gesendete Paketanzahl vom Hidden-Node zur Nachbarstation ermitteln. Ein Schwachpunkt dieser Methode liegt darin, dass es nicht möglich ist, die Hidden-Nodes eindeutig den Nachbarstationen zuzuordnen, da mehr Nachbarstationen den Hidden-Node hören könnten, aber bisher keine Pakete zwischen diesen Stationen und dem Hidden-Node gesendet wurden.

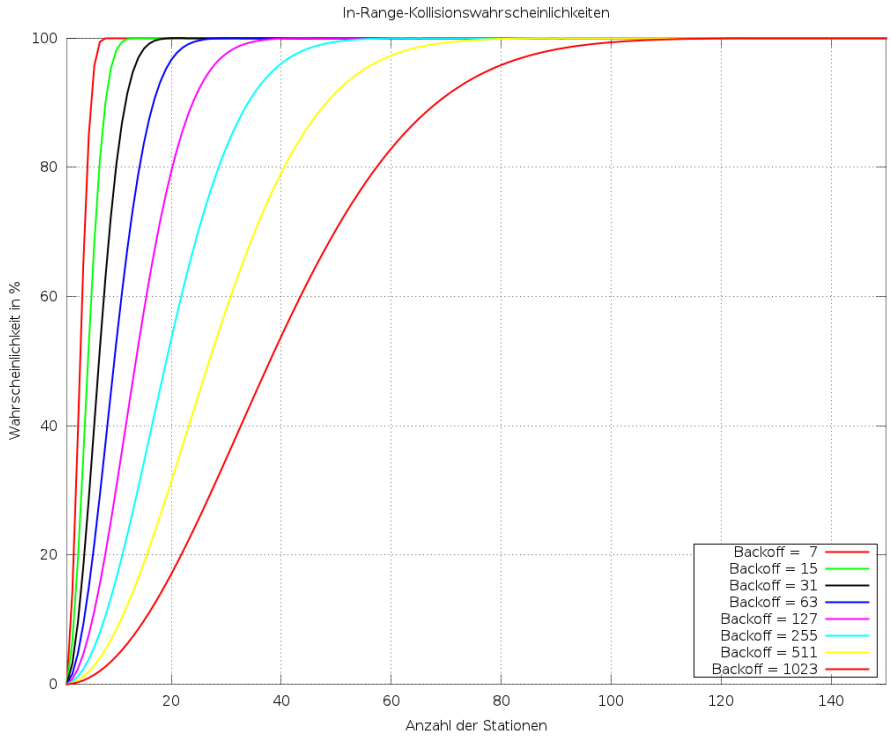

Abbildung 3.1: Kollisionswahrscheinlichkeit für verschiedene Contention-Window-Größen

Die Dauer der Belegung des Mediums hängt direkt von der gewählten Datenrate ab. Je geringer die Datenrate ist, desto länger dauert die Übertragung eines Paketes. Ack-Pakete werden immer mit der Basisdatenrate (1 MBit/s für 802.11b, 6 MBit/s für 802.11a) gesendet [G+07]. Da die Datenrate der gesendeten Ack-Pakete keine Rückschlüsse auf die Datenrate, mit der der Hidden-Node in der Lage ist zu senden, zulässt, wird für die Berechnung der Auslastung des Mediums angenommen, dass die Datenpakete nur mit 1 MBit/s (für 802.11b) vom Hidden-Node gesendet werden. Mit Hilfe der Formel 2.1.1 lässt sich die Auslastung des Mediums zwischen Hidden-Node und Nachbarstation für die Basisdatenrate von 1 MBit/s abschätzen. Dazu kommen noch die vom Hidden-Node zur Nachbarstation gesendeten Ack-Pakete, die wie in 3.3.1 zu sehen ist, 0,29 ms benötigen.

$$\begin{aligned} 1\,MBit/s &= 1048576\,Bit/s \\ \frac{304\,Bits}{1048576\,Bit/s} &= 0,29\,ms \end{aligned} \tag{3.3.1}$$

Eine wesentlich pessimistischere Abschätzung geht davon aus, dass jeder Versuch Daten zu senden, durch einen Versuch des Hidden-Nodes, Daten zu senden, zunichte gemacht wird, wie in Abbildung 3.2 zu sehen ist, da der Carrier-Sense-Mechanismus,

der Kollisionen vermeiden soll, bei einem Hidden-Node-Szenario nicht funktioniert. Daraus ergibt sich eine Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes von 100 Prozent und jede Datenübertragung sollte dann durch RTS-CTS abgesichert werden. Dieser Fall tritt ein, wenn keinerlei Informationen, wie Anzahl der gesendeten Pakete, über den entdeckten Hidden-Node vorliegen.

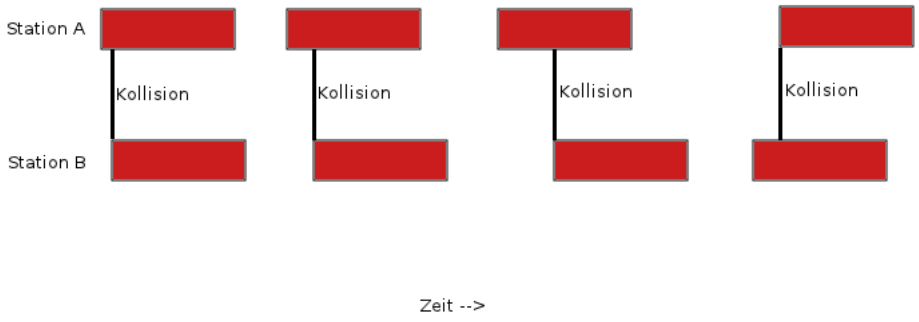

Abbildung 3.2: Kollisionen durch Hidden Nodes

Um Informationen über das Umfeld der Nachbarstationen zu bekommen und damit die Wahrscheinlichkeit für Paketverluste genauer schätzen zu können, bietet sich eine Kooperation der benachbarten Stationen an. Dazu senden die Stationen gesammelte Statistiken über ihre Nachbarstation an alle Nachbarstationen. Diese Statistik enthält die Adresse der Nachbarstation, die Anzahl der von dieser Station empfangen Datenpakete, die übertrage Byte-Menge, sowie die Dauer der Kanalbelegung durch die Nachbarstation. Mit Hilfe eines weiteres Click-Elements, welches die gesammelten Informationen in ein Datenpaket verpackt, werden diese Informationen periodisch nach einer einstellbaren Zeit per Broadcast an alle Nachbarn übertragen, welche dann diese Informationen auswerten können.

Mit Hilfe dieser Informationen, lassen sich die einzelnen Hidden-Nodes eindeutig den jeweiligen Nachbarn zuordnen. Weiterhin lassen sich mit den Informationen über die Belegungszeit des Mediums die Wahrscheinlichkeit einer Kollision besser als ohne Kooperation abschätzen, in dem die maximal zur Verfügung stehende Zeit auf dem Medium in Relation zur Auslastung gesetzt wird.

Der Nachteil der Kooperation ist, dass zusätzliche Daten-Pakete zwischen den Stationen ausgetauscht werden müssen. Dadurch wird die Auslastung des Netzes weiter erhöht und es kann durch die zusätzlichen Daten-Pakete zu weiteren Kollisionen kommen.

Die Statistik für eine Nachbarstation benötigt 31 Byte an Daten. Sendet eine Station die Statistiken von sechs Nachbarstationen, werden 186 Byte Daten erzeugt, die in ein 802.11-Datenframe verpackt werden müssen (siehe Kapitel 2.1.2). Das heißt, der resultierende Datenframe hat eine Größe von 1968 Bit.

3.4 Non-Wifi

Die einfachste Möglichkeit Störungen, die durch Non-Wifi-Quellen wie Mikrowellenherde verursacht werden, zu entdecken, ist die Hilfe eines Spektrumsanalysators

in Anspruch zu nehmen. Da dieser bei gängiger WLAN-Hardware nicht zur Verfügung steht, müssen die Informationen, die über die Treiber der WLAN-Hardware zugänglich sind, genutzt werden.

Wie schon in der Einleitung erwähnt, wird in [RPB11] erfolgreich ein WLAN-Chip für die Erkennung von Störungen durch Non-Wifi-Quellen eingesetzt. Allerdings ist auf Grund der Funktionsweise des Click-Frameworks und des Treibers zur Zeit kein Zugriff auf die Subcarrier möglich. Daher konnte diese Idee leider nicht aufgegriffen werden.

Das Problem der Erkennung von Non-Wifi-Signalen liegt, wie in [RPB11] beschrieben, darin, dass es nicht einfach ist, Non-Wifi-Geräte mit 802.11-Hardware zu erkennen. Es ist unter anderem nicht möglich protokollspezifische Detektoren einzusetzen, da die Treiber der WLAN-Hardware nur eingeschränkte Informationen über das empfangene Signal zur Verfügung stellen bzw. die Hardware verändert werden müsste, um mehr Informationen zu erhalten. Auch ist die Auflösung der Samples mit 312.5 kHz im Vergleich mit weniger als 1 kHz bei Spektrumsanalysatoren ziemlich grob, genauso wie die zeitliche Auflösung mit $2500\frac{\text{samples}}{\text{s}}$ recht gering ist.[RPB11]

Non-Wifi-Störungen lassen sich aber teilweise über den Vergleich von erkannten Signalen und empfangenen Paketen aufdecken. Wie in [HMS10] beschrieben lassen sich die Register für empfangene Signale und dekodierte Signale auslesen und diese Werte in Beziehung setzen. Dazu wird wieder das Click-Element ChannelStats genutzt und die Struktur airtime-stats ausgelesen. Darin befinden sich die Werte der Busy- RX- und TX-Register für die PHY-Schicht und die MAC-Schicht. Diese Register werden in [HMS10] detailliert beschrieben ist.

Die Werte der Busy-Register der beiden Schichten werden in Beziehung gesetzt und dann die Wahrscheinlichkeit für den Empfang einer Störung ermittelt.

Die Unterscheidung der verschiedenen Non-Wifi-Klassen, wie sie auf Seite 18 aufgeführt sind, ist nur bedingt möglich. Breitbandige Signale, die mehr als einen Kanal belegen, sind nur durch den Scan der Nachbarkanäle zu erkennen. Ein Kanalwechsel ist jedoch bei gängiger Hardware unpraktisch, da der Kanalwechsel einige Zeit in Anspruch nimmt [RPB11] und während dieser Zeit keine Daten auf dem eigentlichen Arbeitskanal empfangen werden können. Das würde wiederum zu Paketverlusten und erneuten Übertragung der Daten führen, was eigentlich vermieden werden sollte.

Die Unterscheidung in kooperative und nicht-kooperative Signalquellen lässt sich ebenfalls nicht umsetzen, da ein Carrier-Sense-Mechanismus sich nicht aus den Signalen ableitet und die Non-Wifi-Signalquellen nicht eindeutig zugeordnet werden können, wodurch eine Statistik, die eventuell einen Carrier-Sense-Mechanismus entdecken könnte, schwer zu realisieren ist.

3.5 Datenspeicherung

Die ermittelten Wahrscheinlichkeiten werden in einer Baumstruktur abgelegt (siehe Abb. 3.4). In den jeweiligen Blättern des Baumes wird die Wahrscheinlichkeit für Paketverluste für die beobachtete Ursache als Prozentwert gespeichert. Die beiden Hauptäste des Baums sind in Interferenz und Fading unterteilt. Der Interferenz-Ast wird nochmals in Wifi und Non-Wifi aufgeteilt, wobei unter dem Zweig Wifi der

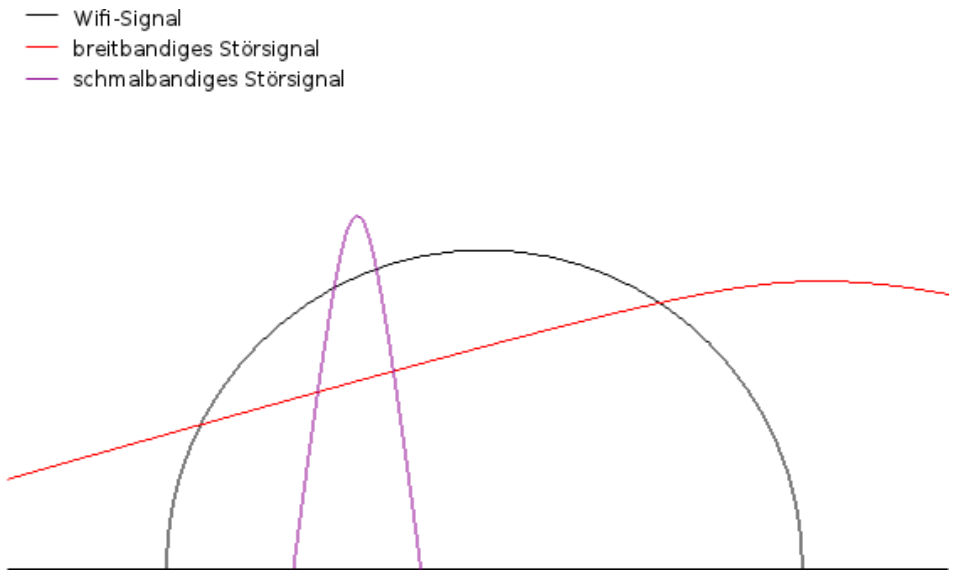

Abbildung 3.3: Schmal- und breitbandige Störsignale

Co-Channel-Zweig und darunter die Blätter In-Range und Hidden-Node zu finden sind.

Im Non-Wifi-Zweig finden sich noch die Zweige für Narrow- und Broadband mit jeweils den Cooperative- und Non-Cooperative-Blättern. Auf Grund der oben genannten Unterscheidungsschwierigkeiten von Non-Wifi-Signalen, werden alle Werte im Knoten Non-Wifi abgelegt und die Blätter nicht genutzt.

Pro Nachbar wird ein Baum erstellt, in dem die ermittelten Werte in den jeweiligen Blättern abgelegt werden und für die Auswertung zur Verfügung stehen.

Für die Auswertung werden die gesammelten Wahrscheinlichkeiten in eine XML-Struktur überführt. Dabei werden nicht nur die aktuellen Wahrscheinlichkeiten, sondern ebenfalls ein gleitender arithmetischer Mittelwert über 20 bzw. 200 Werte für die spätere Auswertung ausgegeben.

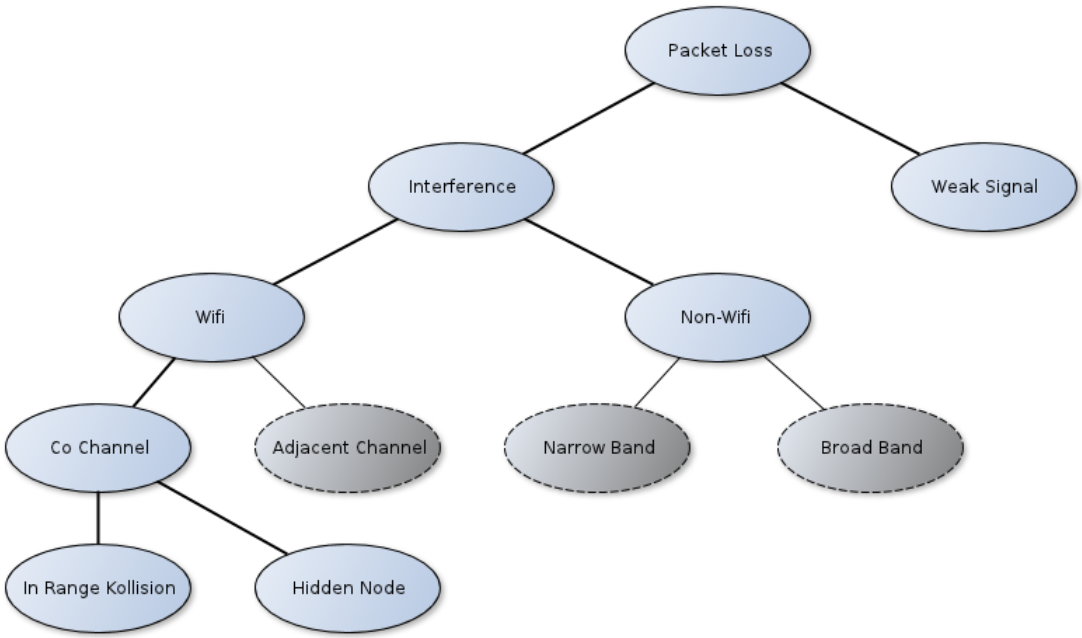

Abbildung 3.4: Baum zur Speicherung der Wahrscheinlichkeiten von Paketverlustursachen

4 Evaluierung

In diesem Kapitel werden die im vorherigem Kapitel behandelten Fehlerarten in verschiedenen Szenarien im Simulator realisiert und getestet. Als Simulator wird der Network Simulator 2 (NS-2) [Ins12] eingesetzt. NS-2 stellt drei unterschiedliche Modelle der Funkwellenausbreitung zur Verfügung: das Free-Space-Model, das Two-Ray-Ground-Reflection-Model und das Shadowing-Model.

Mit diesen Modellen wird der Pfadverlust, also der „Verlust an elektromagnetischer Leistung [...] zwischen einem Sender und einem Empfänger“[Wik12], ermittelt. Die Details der Implementierung sind in [Ins11] zu finden.

In den folgenden Szenarien werden das Two-Ray-Ground-Reflection-Model und das Shadowing-Model verwendet. Die Signalstärke ist beim Two-Ray-Ground-Reflection-Model nur vom Abstand der Stationen voneinander abhängig. Dies simuliert eine Idealumgebung, wie sie in der Praxis kaum zu finden sein wird. Für die Simulation zur Überprüfung, ob die provozierten Fehler erkannt werden, ist das Two-Ray-Ground-Reflection-Model deshalb gut geeignet.

Das Shadowing-Model dagegen simuliert Abschattungen und Mehrwegeausbreitung der Signale und erzeugt dadurch unterschiedlich starke Signale. Damit lassen sich die Szenarien in einer mehr an die Wirklichkeit angepassten Simulationsumgebung testen. Dadurch lässt sich auch abschätzen, ob die Erkennung der provozierten Fehler in realistischeren Umgebungen funktioniert. Für alle Simulation mit dem Shadowing-Model ist der Pfadverlustexponent gleich zwei und die Standardabweichung beträgt 2 dB.

In der Auswertung der folgenden Simulationen und Messungen werden nicht nur die einzelnen geschätzten Wahrscheinlichkeiten betrachtet, sondern ebenfalls ein gleitender Mittelwert über 20 und 200 Werte gebildet. Durch diese gleitenden Durchschnitte ist es möglich trotz Schwankungen der Einzelwerte Trends zu ermitteln. Der gleitende Mittelwert über 20 Werte lässt dabei Änderungen schneller sichtbar werden, der gleitende Mittelwert über 200 Werte zeigt den langfristigen Trend wenig beeinflusst von Änderungen an.

4.1 Paketverluste durch schwache Signale (Weak-Signal)

Für die Evaluierung der Wahrscheinlichkeitsberechnung von Paketverlusten auf Grund von zu schwachen Signalen werden unterschiedliche Szenarien, mehrere stationäre und dynamische, entwickelt, um verschiedene Weak-Signal-Situationen zu testen. Dabei wird die Anzahl der gesendeten Pakete pro Sekunde so gering gewählt, dass das Medium nicht zu stark ausgelastet wird und damit Kollisionen als Paketverlustursache vermieden werden.

4.1.1 Stationäre Szenarien

Die stationären Szenarien sollen zeigen, dass es grundsätzlich möglich ist, Paketverluste auf Grund von Weak-Signal zu erkennen. Dazu werden zwei Stationen in unterschiedlichen Entfernungen positioniert und Datenpakete an die jeweilige andere Station gesendet.

Jeder der Durchläufe wird zuerst mit dem Two-Ray-Ground-Reflection-Model und danach mit dem Shadowing-Model durchgeführt. Danach werden die RSSI-Werte und die geschätzten Wahrscheinlichkeiten für Paketverluste auf Grund von Weak-Signal ausgewertet.

Two-Ray-Ground-Reflection-Model

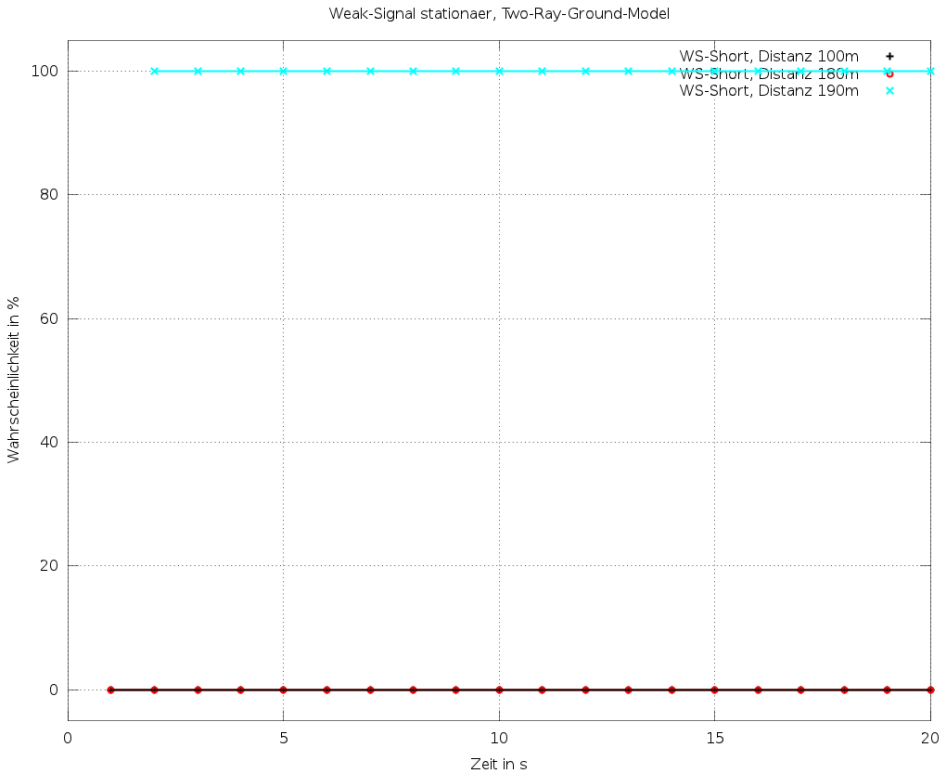

Abbildung 4.1: Stationäre Weak-Signal-Auswertung, Wahrscheinlichkeiten für die Distanzen 100 m, 180 m, 190 m

Im ersten stationären Weak-Signal-Szenario beträgt der Abstand zwischen Station eins und zwei zuerst 100 m. Nachdem der erste Simulationslauf beendet ist, wird der Abstand dann auf 180 m und nach einem weiteren Simulationslauf auf 190 m vergrößert. Alle drei Simulationen verwenden dabei das Two-Ray-Ground-Reflection-Model als Pfadverlustmodell.

Auf Grund des Two-Ray-Ground-Reflection-Model wird erwartet, dass die RSSI-Werte nicht schwanken und die Wahrscheinlichkeit für Paketverluste der ersten zwei simulierten Distanzen bei null Prozent liegt, da die Standardabweichung (siehe Seite 22) auf Grund des gleichen Erwartungswertes immer gleich ist. Die Simulationszeit beträgt auf Grund der erwarteten konstanten Ergebnisse 20 Sekunden. Die weiteren Simulationen mit dem Shadowing-Model und mit Mobilität haben eine längere Simulationszeit. Die letzte simulierte Distanz von 190 m liegt leicht außerhalb der Sendereichweite und so wird der RSSI-Wert null betragen und die Wahrscheinlichkeit für Paketverluste auf Grund von zu schwachen Signalen 100 Prozent ergeben.

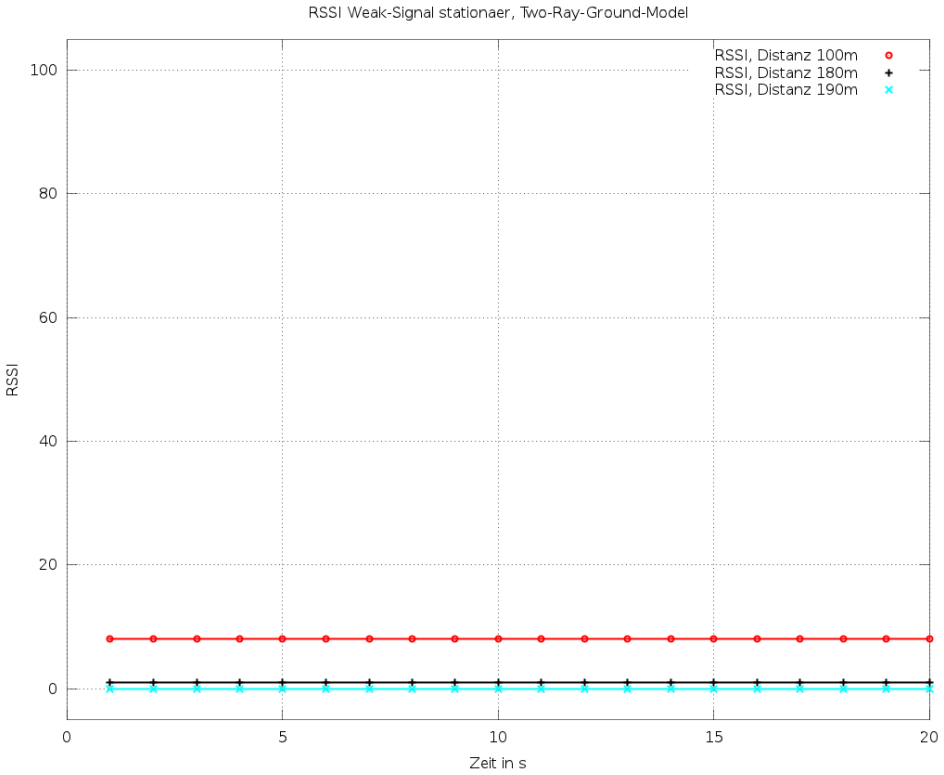

Abbildung 4.2: Stationäre Weak-Signal-Auswertung, RSSI-Werte für die Distanzen 100 m, 180 m, 190 m

In der Abbildung 4.1 sind die verschiedenen Wahrscheinlichkeiten (in der Abbildung als WS-Short bezeichnet) für die unterschiedlichen Distanzen der zwei Stationen gut zu erkennen. Die ersten beiden Simulationen zeigen eine Paketverlustwahrscheinlichkeit von null Prozent und die letzte Simulation mit der Entfernung von 190 m eine Paketverlustwahrscheinlichkeit von 100 Prozent. Auf die Darstellung der gleitenden Durchschnitte der Werte über 20 bzw. 200 Sekunden wird hier verzichtet, da der gleitende Durchschnitt über konstante Werte ebenfalls konstant ist und die gleichen Werte ergibt.

Die RSSI-Werte der Simulationen können aus der Abbildung 4.2 entnommen werden. Die Werte der ersten Simulation liegen dabei noch deutlich über null, die der zweiten Simulation ganz knapp über null und für die dritte Simulation, wie durch Abbildung 4.1 nicht anders zu erwarten, sind die RSSI-Werte genau null. Die Anzahl der Kollisionen beträgt ebenfalls null und die Rate der wiederholt übertragenen Pakete (Wiederholungsrate) liegt bei null Prozent, das heißt, dass kein Paket verloren ging.

Shadowing-Model

In den nächsten Simulationen wird das Shadowing-Model verwendet, um die Weak-Signal-Schätzung in einem Szenario mit Abschattungen und Mehrwegeausbreitung simulieren zu können. Dafür müssen die Distanzen zwischen den Stationen verringert werden. Die Distanz zwischen den zwei Stationen beträgt für den ersten Simulationslauf 30 m. Für den zweiten Simulationslauf wird die Distanz auf 60 m vergrößert und für den dritten Simulationslauf auf 90 m. Der vierte Simulationslauf wird dann zum Schluss mit einer Distanz von 120 m gestartet.

Durch das Shadowing-Model schwanken die RSSI-Werte und damit auch die Wahrscheinlichkeiten. Je nach Abstand der zwei Stationen von einander fallen die Schwankungen der Wahrscheinlichkeiten unterschiedlich stark und unterschiedlich häufig aus.

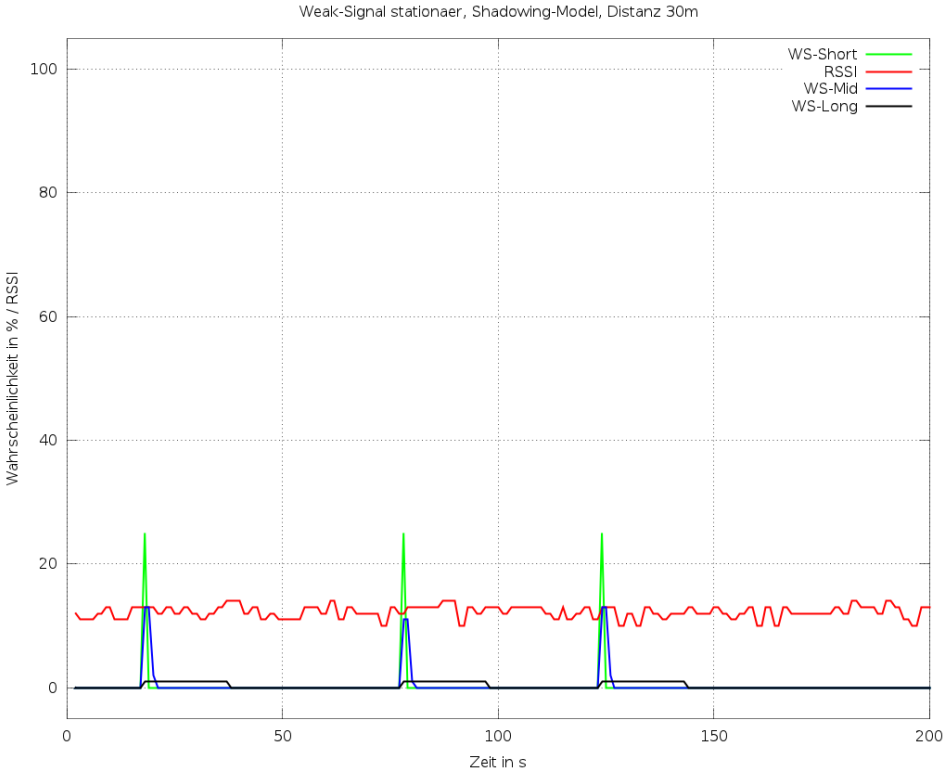

Abbildung 4.3: Stationäre Weak-Signal-Auswertung, Wahrscheinlichkeiten und RSSI-Werte für eine Distanz von 30 m

Stations-Distanz 30 m In Abbildung 4.3 sind die RSSI-Werte, hier rot dargestellt, deutlich über null. Die Wahrscheinlichkeit für Paketverluste, hier grün dargestellt und als WS-Short gekennzeichnet, steigt nur drei Mal auf 25 Prozent, ausgelöst durch vereinzelte Pakete, deren RSSI-Wert sehr niedrig war.

Der gleitende Durchschnitt der Werte über je 20 (blau, WS-Mid) und 200 (schwarz, WS-Long) Sekunden zeigt, dass die kurzen Anstiege der Wahrscheinlichkeit keine große Bedeutung haben. Die Anzahl der Kollisionen liegt bei null und die Wiederholungsrate ist mit 0,02 % klein.

Abbildung 4.4: Stationäre Weak-Signal-Auswertung, Wahrscheinlichkeiten und RSSI-Werte für eine Distanz von 60 m

Stations-Distanz 60 m Bei einer Distanz von 60 m schwanken die RSSI-Werte zwischen 3 und 6, wie in Abbildung 4.4 zu sehen ist. Die Wahrscheinlichkeit für Paketverluste schwankt in großen Teilen zwischen 25 und 50 Prozent, hat aber ein paar Ausreißer nach unten. Beim gleitenden Mittelwert über 20 Sekunden (WS-Mid) folgt die Paketverlustwahrscheinlichkeit noch recht deutlich den Einzelwerten. Wird über 200 Sekunden gleitend gemittelt (WS-Long), schwankt die Wahrscheinlichkeit im Großen und Ganzen zwischen 25 und 40 Prozent. Die Anzahl der Kollisionen ist bei 4241 gesendeten Paketen weiterhin null, die Wiederholungsrate hat sich durch vereinzelt verlorengegangene Pakete auf knapp 4 % erhöht.

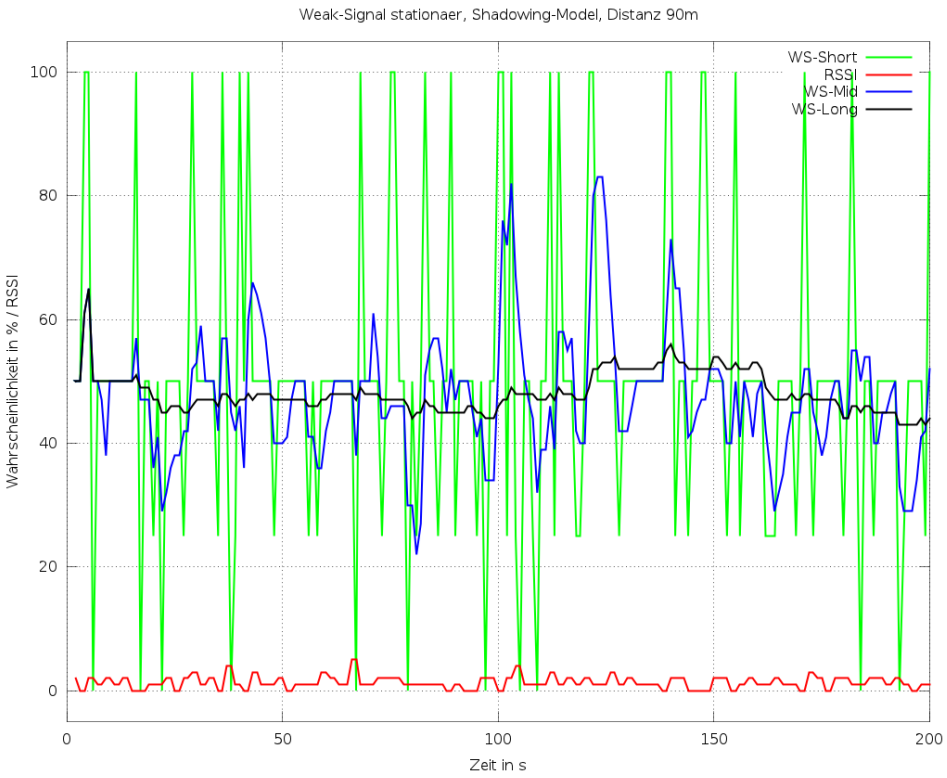

Abbildung 4.5: Stationäre Weak-Signal-Auswertung, Wahrscheinlichkeiten und RSSI-Werte für eine Distanz von 90 m

Stations-Distanz 90 m Wird die Distanz auf 90 m vergrößert (Abbildung 4.5) sinken die RSSI-Werte wie erwartet weiter, teilweise bis auf null. Die Paketverlustwahrscheinlichkeit schwankt sehr stark zwischen null und 100 Prozent.

Schaut man sich den gleitenden Mittelwert an, sind über einen Zeitraum von 20 Sekunden (WS-Mid) die Wahrscheinlichkeiten für Paketverluste wesentlich deutlicher zu sehen. Die Extremwerte von null und 100 Prozent werden weggemittelt und es ergeben sich Werte von knapp über 20 Prozent Wahrscheinlichkeit bis hin zu über 80 Wahrscheinlichkeit von Paketverlusten.

Bei einem gleitenden Durchschnitt der Werte über 200 Sekunden (WS-Long), liegt die Wahrscheinlichkeit um die 50 Prozent. Dieses Ergebnis korreliert sehr gut mit der Wiederholungsrate von 49,56 %. Die Anzahl der Kollisionen ist bei 3331 gesendeten Paketen weiterhin null. Die Anzahl der erfolgreich gesendeten Pakete nimmt im Vergleich zu den vorherigen Simulationen ab.

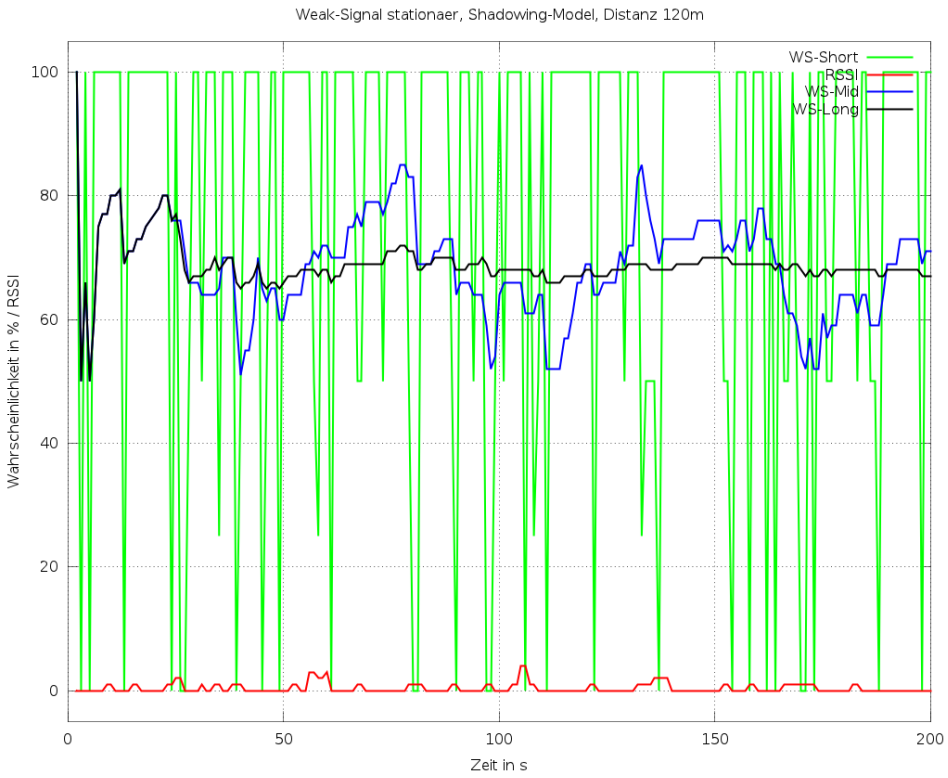

Abbildung 4.6: Stationäre Weak-Signal-Auswertung, Wahrscheinlichkeiten und RSSI-Werte für eine Distanz von 120 m

Stations-Distanz 120 m Im letzten Durchgang der Simulation wird die Entfernung zwischen den beiden Stationen auf 120 m vergrößert. Abbildung 4.6 zeigt, dass die RSSI-Werte ab und zu über null steigen. Dies schlägt sich auch in der Paketverlustwahrscheinlichkeit (WS-Short) nieder, die meist zwischen 50 und 100 Prozent liegt, aber auch Werte zwischen 50 und null Prozent aufweist.

Der gleitende Durchschnitt über 20 Sekunden bewegt sich zwischen 50 und knapp über 80 Prozent. Wird über 200 Sekunden gleitend gemittelt, liegt die Wahrscheinlichkeit für Paketverluste recht konstant bei etwa 75 Prozent. Die Wiederholungsrate ist auf gut 79 % geklettert und bestätigt die geschätzten Werte der Paketverlustwahrscheinlichkeit. Die Anzahl der Kollisionen bleibt bei 2540 gesendeten Paketen bei null.

Auswertung

Die Auswertung der Simulationen hat gezeigt, dass bei steigender Entfernung die errechneten Wahrscheinlichkeiten für Paketverluste auf Grund von schwachen Signalen zunehmen. Da die einzelnen Wahrscheinlichkeitswerte gerade bei größeren Entfernungen stark schwanken, ergibt sich erst durch die gleitenden Durchschnitte der Werte eine kontinuierliche Tendenz der zu erwartenden Wahrscheinlichkeiten für Paketverluste, die aber recht gut mit den Wiederholungsraten der einzelnen Simulationen korrelieren. Bei stark schwankenden Werten zeigen gleitende Durchschnitte über größere Bereiche den Trend besser. Schwanken die Werte dagegen weniger stark, werden kleine Änderungen der einzelnen Werte von gleitenden Mittelwerten über große Bereiche nicht sichtbar gemacht.

4.1.2 Szenario mit Mobilität, Verkleinerung der Distanz

Das zweite Szenario ist dynamisch, dass heißt, eine Station bewegt sich und zwar in diesem Fall auf die andere Station zu. Die Anfangspositionen der zwei Stationen liegen dabei möglichst weit auseinander. Damit soll getestet werden, ob die Erkennung von Paketverlusten durch zu schwache Signale mit sich stark verändernden Signalen zurecht kommt beispielsweise Stationen, die die Ausgangsleistung drosseln. Es wird dabei mit verschiedenen Geschwindigkeiten gemessen.

Two-Ray-Ground-Reflection-Model

Für das Two-Ray-Ground-Reflection-Model beträgt die Distanz zwischen den zwei Stationen 250 m. Nach zehn Sekunden, fängt die zweite Station an, sich auf die erste Station zu zu bewegen, sodass sich die Distanz zwischen beiden Stationen immer weiter verringert, bis sich beide Stationen bis auf 30 m angenähert haben.

Dabei müsste zu beobachten sein, dass der RSSI-Wert kontinuierlich steigt und die Wahrscheinlichkeit für Paketverluste dementsprechend kontinuierlich sinkt, je geringer die Distanz zwischen den beiden Stationen wird.

Geschwindigkeit 2 m/s Zuerst wird nur eine geringe Geschwindigkeit von 2 Metern pro Sekunde untersucht, um die Änderungen der Werte deutlich sichtbar zu machen.

Bei der Geschwindigkeit von 2 Metern pro Sekunde (Abbildung 4.7) dauert es einige Zeit bis Station zwei in den Empfangsbereich von Station eins eintritt. Die ersten Pakete werden, wie erwartet mit einem niedrigen RSSI-Wert (hier rot dargestellt) empfangen und die Paketverlustwahrscheinlichkeit (grün, WS-Short) liegt bei 100 Prozent. Kurz darauf steigen die RSSI-Werte durch die weitere Annäherung der Stationen an und die Wahrscheinlichkeit für Paketverluste sinkt auf null Prozent. Die gleitenden Mittelwerte der Wahrscheinlichkeiten zeigen den längerfristigen Trend an und sinken ebenfalls gegen null. Die Anzahl der Kollisionen liegt bei null. Gesendet wurden 4018 Pakete, wobei 8,26 % erneut übertragen werden mussten. Die Wiederholungsrate ist allerdings in dieser dynamischen Simulation wenig aussagekräftig, da die Auswirkungen der Distanzveränderungen zwischen den Stationen sich nicht in dem Wert widerspiegeln.

Geschwindigkeit 5 m/s Bei einer höheren Geschwindigkeit der Station zwei, wie in Abbildung 4.8 zu sehen, von 5 Metern pro Sekunde, ähneln die Ergebnisse denen der vorherigen Simulation mit einer Geschwindigkeit von 2 Metern pro Sekunde. Beide Stationen werden zu Anfang auf die gleichen Positionen wie bei der vorherigen Simulation gesetzt und Station 2 bewegt sich wieder nach 10 Sekunden auf Station 1 zu. Die Zeit bis zum Empfang des ersten Paketes ist allerdings wesentlich kürzer und der Anstieg der RSSI-Werte steiler, sowie das Sinken der Wahrscheinlichkeiten schneller, da sich Station zwei wesentlich schneller mit 2,5-facher Geschwindigkeit bewegt. Die Anzahl der Kollisionen liegt bei 4147 gesendeten Paketen bei null und die Wiederholungsrate ist durch die schnellere Bewegung von Station zwei auf 4,65 % gesunken.

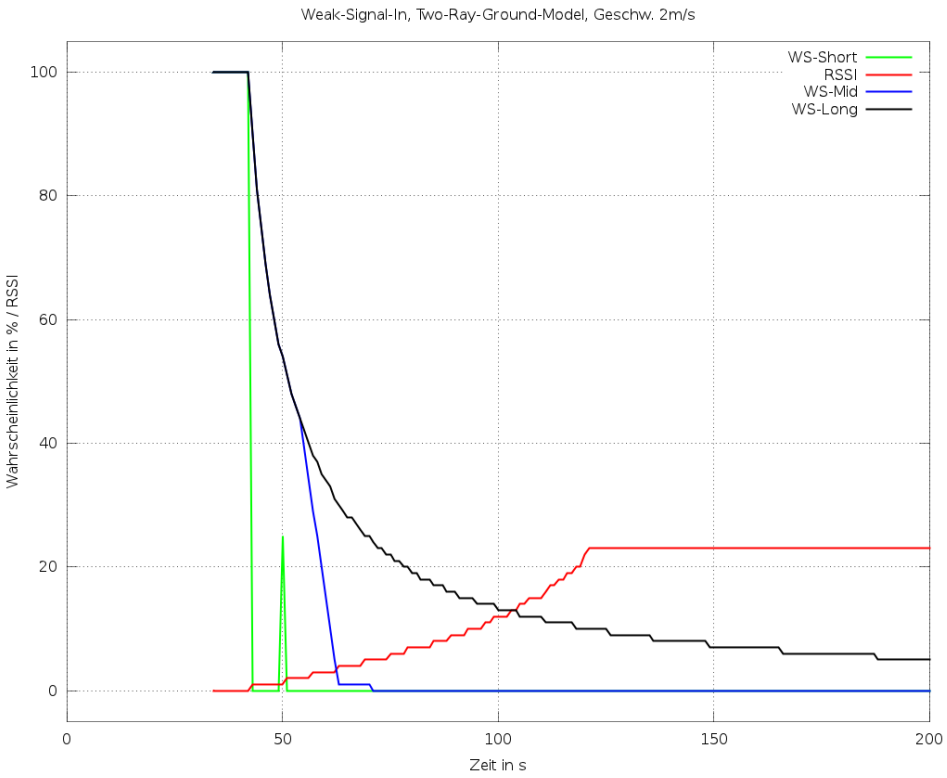

Abbildung 4.7: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Two-Ray-Ground-Reflection-Model, dynamisch-in, Geschw. 2 m/s

Shadowing-Model

Das Shadowing-Model erfordert wieder eine geringere Entfernung zwischen den zwei Stationen. Die Distanz zum Anfang beträgt 140 m und wie in den zwei vorhergehenden Simulationen bewegt sich Station zwei nach 10 Sekunden auf Station eins zu, bis die Distanz zwischen den zwei Stationen auf 30 m geschrumpft ist. Wieder soll ermittelt werden, ob die Weak-Signal-Erkennung auch mit den Signaleigenschaften des Shadowing-Model, dieses Mal in einer dynamischen Simulation, zurecht kommt.

Die Ergebnisse dieser Simulation sollten den Ergebnissen der Simulation mit dem Two-Ray-Ground-Reflection-Model ähneln, wobei die Werte auf Grund der Eigenschaften des Shadowing-Model stärker schwanken werden.

Geschwindigkeit 2 m/s Wie in Abbildung 4.9 zu sehen ist, werden schon nach kurzer Zeit die ersten Pakete mit niedrigem RSSI-Wert (rot dargestellt) empfangen. Wie schon auf Seite 33 zu sehen war, schwanken die RSSI-Werte und sinken trotz weiterer Annäherung der beiden Stationen anfangs immer wieder auf null. Dementsprechend stark schwankt die Wahrscheinlichkeit (grün dargestellt und als WS-Short gekennzeichnet) am Anfang noch zwischen null und 100 Prozent und

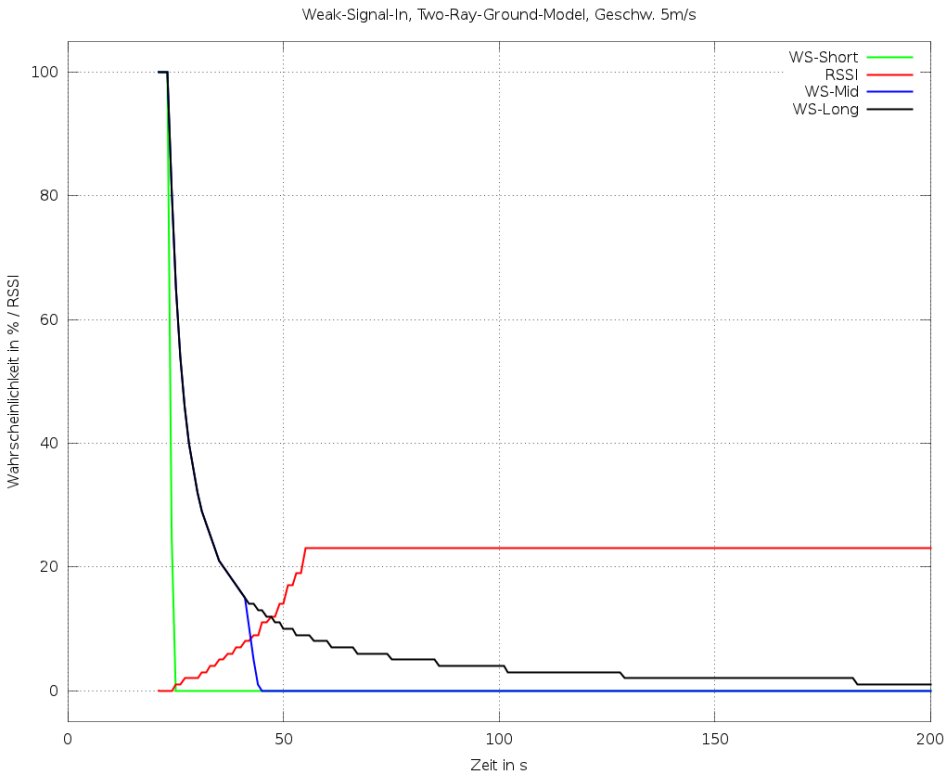

Abbildung 4.8: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Two-Ray-Ground-Reflection-Model, dynamisch-in, Geschw. 5 m/s

später zwischen 50 und 25 Prozent. Zum Schluss sinkt die Wahrscheinlichkeit bis auf wenige Ausreißer auf null Prozent.

Die gleitenden Durchschnitte der Wahrscheinlichkeiten (in der Abbildung als WS-Mid und WS-Long gekennzeichnet) pendeln sich kurz von 100 Prozent auf um die 50 Prozent ein und sinken dann beim gleitenden Durchschnitt über 20 Sekunden recht schnell auf annähernd null Prozent. Die Kollisionsanzahl liegt bei 3445 gesendeten Paketen bei null und die Wiederholungsrate bei 27,90 %.

Geschwindigkeit 5 m/s Wird die Geschwindigkeit der Station zwei um das 2,5-fache auf 5 Meter pro Sekunde erhöht, wie in Abbildung 4.10 zu sehen, ergibt sich wie zu erwarten ein ähnlicher Trend wie bei der vorherigen Simulation mit niedrigerer Geschwindigkeit. Bemerkenswert ist der schnelle Anstieg der RSSI-Werte und die schnell sinkende Paketverlustwahrscheinlichkeit im Vergleich zur vorherigen Simulation. Die gleitenden Durchschnitte der Werte (hier blau und schwarz) pendeln sich nicht auf einem Niveau ein, sondern sinken kontinuierlich auf null Prozent.

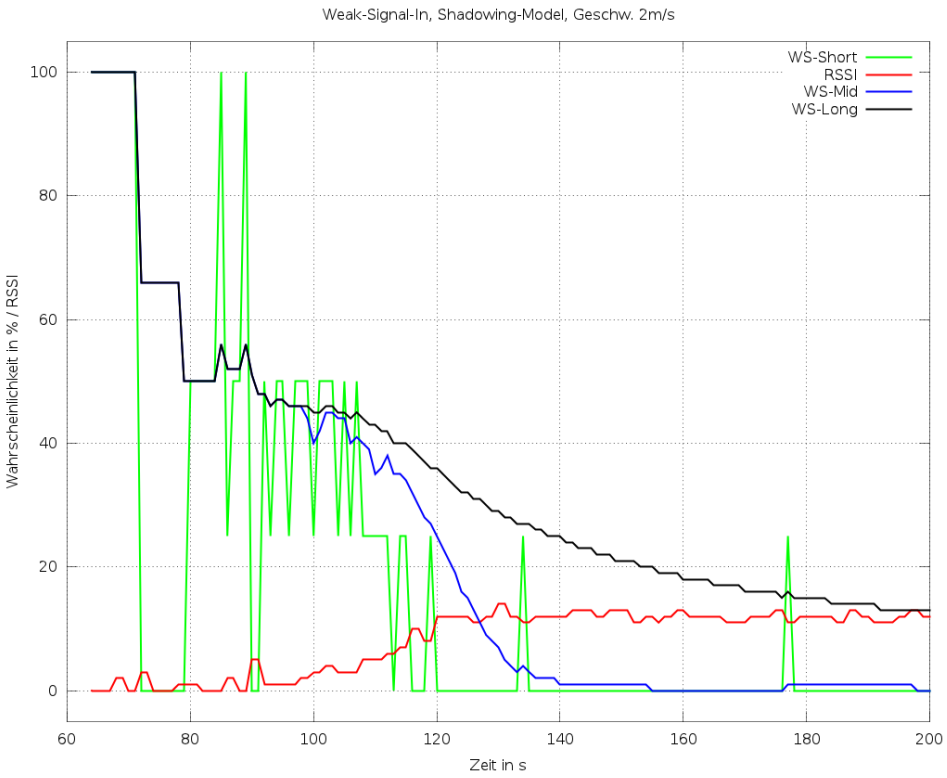

Abbildung 4.9: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Shadowing-Model, dynamisch-in, Geschw. 2 m/s

Insgesamt wurden 3918 Pakete gesendet und es gab wieder keine Kollisionen. Die Wiederholungsrate hat sich mit gut 11 % mehr als halbiert und korreliert mit der 2,5-fachen Geschwindigkeit von Station zwei gegenüber der vorherigen Simulation, auch wenn die Wiederholungsrate in diesem Szenario wenig aussagekräftig ist.

Auswertung

Anhand dieser Simulationen konnte deutlich gezeigt werden, dass die Weak-Signal-Erkennung bei Verringerung der Distanz zwischen den zwei Stationen plausible Wahrscheinlichkeiten abschätzt. Durch die wenig feingranularen RSSI-Werte sind gerade die Einzelwahrscheinlichkeiten beim Einsatz des Shadowing-Model großen Schwankungen unterworfen, sodass die gleitenden Durchschnitte der Wahrscheinlichkeiten notwendig sind, um diese Schwankungen zu glätten und Tendenzen besser abschätzen zu können.

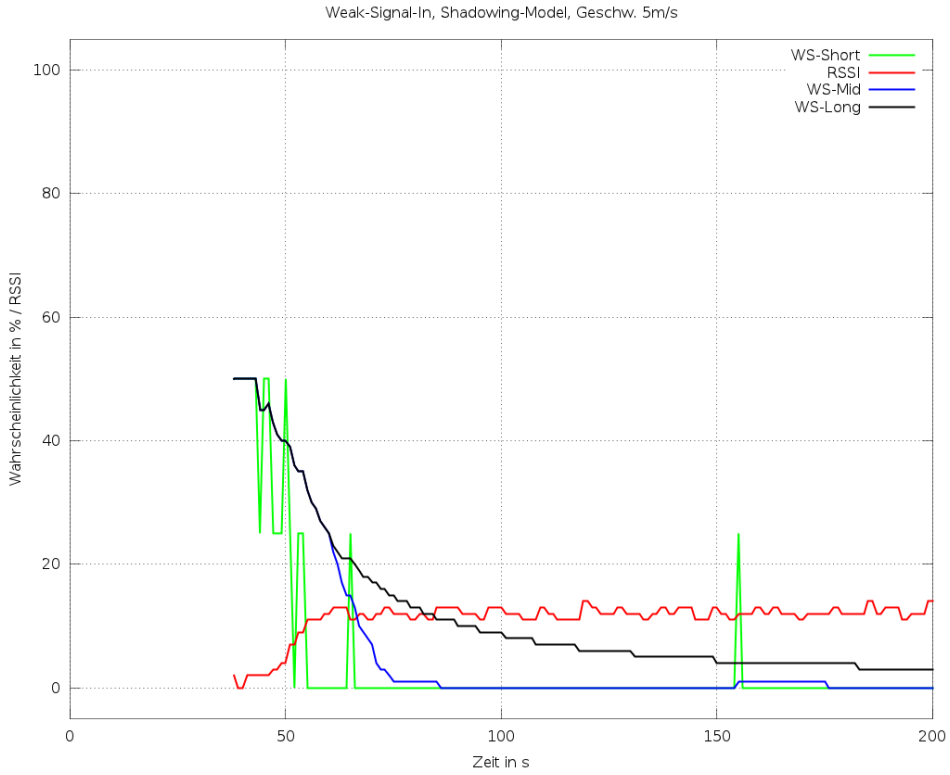

Abbildung 4.10: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Shadowing-Model, dynamisch-in, Geschw. 5 m/s

4.1.3 Szenario mit Mobilität, Vergrößerung der Distanz

Das dritte Szenario ist ebenfalls dynamisch, jedoch bewegt sich eine Station von der anderen Station weg, und zwar so, dass sie sich aus deren Empfangsbereich herausbewegt. Damit soll die Weak-Signal-Erkennung unter den entgegengesetzten Bedingungen zu den vorherigen Simulationen getestet werden.

Two-Ray-Ground-Reflection-Model

Als erstes wird wieder das Two-Ray-Ground-Reflection-Model eingesetzt und die Stationen in Empfangsreichweite positioniert. Die Distanz zwischen beiden Stationen beträgt am Anfang 30 m. Nach 10 Sekunden bewegt sich Station zwei geradlinig von Station ein weg, bis die Entfernung zwischen beiden Stationen auf 300 m gestiegen ist. Diese Positionen liegt außerhalb des Empfangs- und Sendebereiches von Station eins.

Nach einiger Zeit sollte der RSSI-Wert bis auf null sinken und, sobald dieser null erreicht hat, die Wahrscheinlichkeit für Paketverluste auf 100 Prozent steigen.

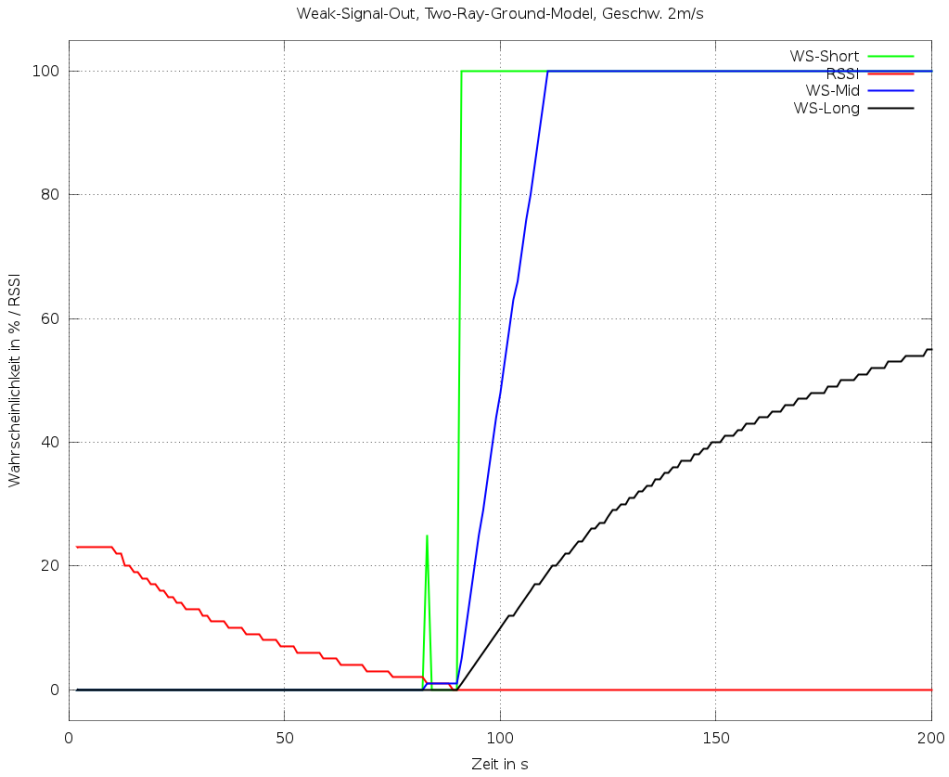

Abbildung 4.11: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Two-Ray-Ground-Reflection-Model, dynamisch-out, Geschw. 2 m/s

Geschwindigkeit 2 m/s Mit einer Geschwindigkeit von 2 Metern pro Sekunde sinkt der RSSI Wert, wie in Abbildung 4.11 zu sehen, recht langsam auf null. Kurz vor Erreichen der Null-Marke ist ein Anstieg der Paketverlustwahrscheinlichkeit auf 25 Prozent zu beobachten. Sobald der RSSI-Wert null erreicht hat, steigt, wie prognostiziert, die Wahrscheinlichkeit auf 100 Prozent. Die gleitenden Durchschnitte der Wahrscheinlichkeiten (WS-Mid und WS-Long in der Abbildung) steigen ebenfalls, allerdings langsamer, auf 100 Prozent.

Bei 4336 gesendeten Pakete und keinen Kollisionen liegt die Wiederholungsrate bei vernachlässigbaren 0,02 %.

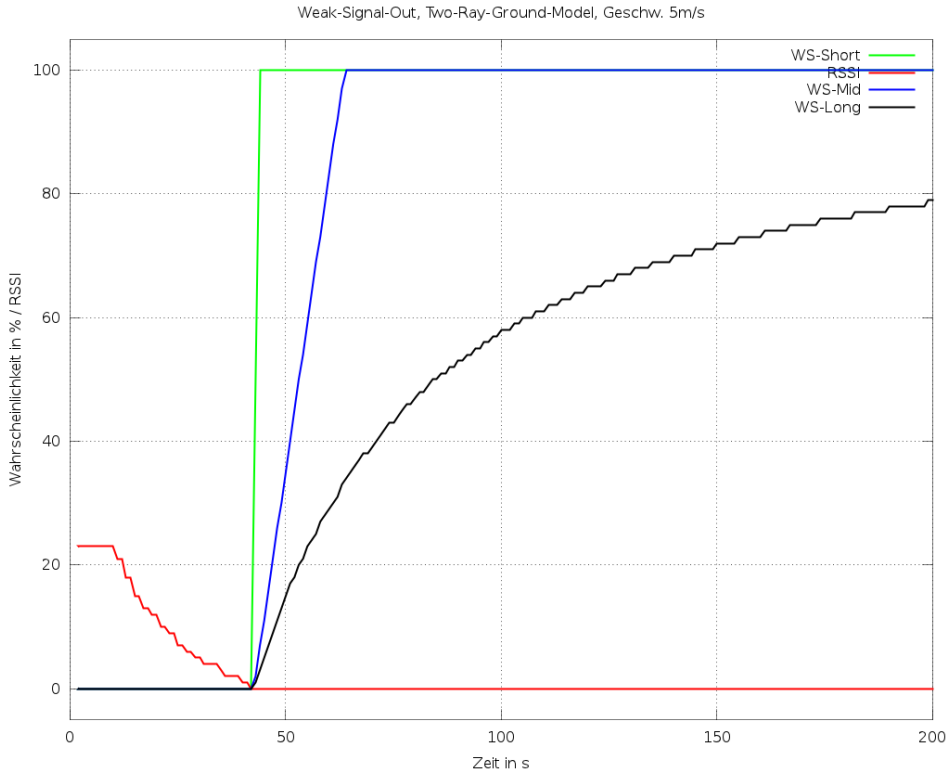

Abbildung 4.12: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Two-Ray-Ground-Reflection-Model, dynamisch-out, Geschw. 5 m/s

Geschwindigkeit 5 m/s Wird die Geschwindigkeit auf 5 Meter pro Sekunde bei gleicher Start- und Zielentfernung erhöht, siehe Abbildung 4.12, ergibt sich ein ähnliches Bild wie in der Simulation zuvor. Allerdings sind die zeitlichen Abläufe auf Grund der 2,5-fachen Geschwindigkeit deutlich gestrafft. Sobald der RSSI-Wert auf null abgesunken ist, steigt die Wahrscheinlichkeit auf 100 Prozent und die gleitenden Durchschnitte der Wahrscheinlichkeiten folgen je nach Anzahl der gemittelten Werte langsamer ebenfalls auf 100 Prozent.

Die Wiederholungsrate liegt bei null Prozent und die Anzahl der Kollisionen ist bei 4342 gesendeten Paketen ebenfalls null.

Shadowing-Model

Nach der Simulation mit dem Two-Ray-Ground-Reflection-Model wird jetzt das Shadowing-Model eingesetzt. Dieses Mal müssen die Distanzen zu Beginn nicht angepasst werden. Ebenfalls kann die Distanz von 300 m zum Ende der Simulation beibehalten werden, da diese Entfernung größer als die Empfangs- und Sendereichweite ist.

Im Gegensatz zum Two-Ray-Ground-Reflection-Model werden die Wahrscheinlichkeiten auf Grund der zu erwartenden Schwankungen des RSSI-Wertes schon vor dem Absinken des RSSI-Wertes auf null ansteigen. Tendenziell sollten die Ergebnisse denen der Simulation mit dem Two-Ray-Ground-Reflection-Model ähneln.

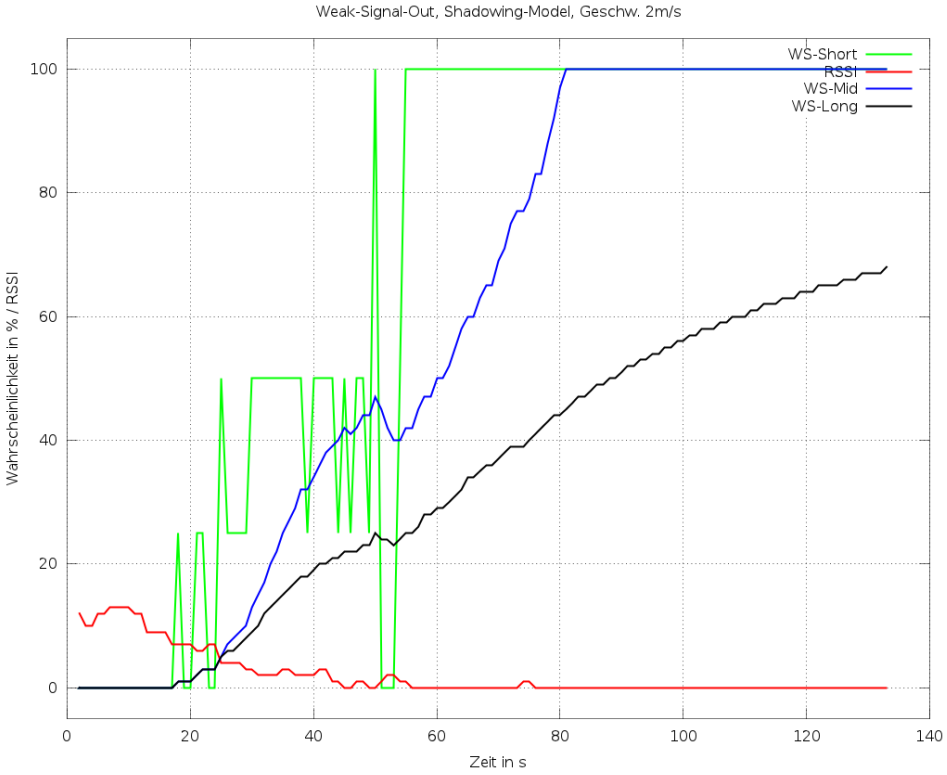

Abbildung 4.13: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Shadowing-Model, dynamisch-out, Geschw. 2 m/s

Geschwindigkeit 2 m/s Trotz der langsamen Geschwindigkeit von 2 Metern pro Sekunde steigt die Paketverlustwahrscheinlichkeit im Vergleich zur Simulation mit

dem Two-Ray-Ground-Reflection-Model sehr zeitig an, wie in Abbildung 4.13 zu sehen ist. Anfangs pendelt die Wahrscheinlichkeit noch zwischen null und 25 Prozent, steigt dann aber dauerhaft auf Werte zwischen 25 und 50 Prozent, um 100 Prozent zu erreichen. Ein kurzer Anstieg des RSSI-Wertes lässt die Wahrscheinlichkeit kurzzeitig auf null Prozent sinken, liegt danach aber dauerhaft bei 100 Prozent. Wenn man die gleitenden Mittelwerte der Wahrscheinlichkeiten über 20 Sekunden (WS-Mid in der Abbildung) betrachtet, kann der Anstieg auf knapp 50 Prozent gut verfolgt werden, ebenso der kurze Anstieg des RSSI-Wertes. Nach einiger Zeit, bedingt durch den gleitenden Durchschnitt, werden dann die 100 Prozent Paketverlustwahrscheinlichkeit erreicht.

Die Anzahl der Kollisionen beträgt bei 2734 gesendeten Paketen null, die Anzahl der Retries liegt mit 60,50 % recht hoch, lässt aber auf Grund der Dynamik in der Simulation wenig Rückschlüsse zu, außer das viele Pakete verloren gehen, wenn Station zwei sich immer weiter entfernt.

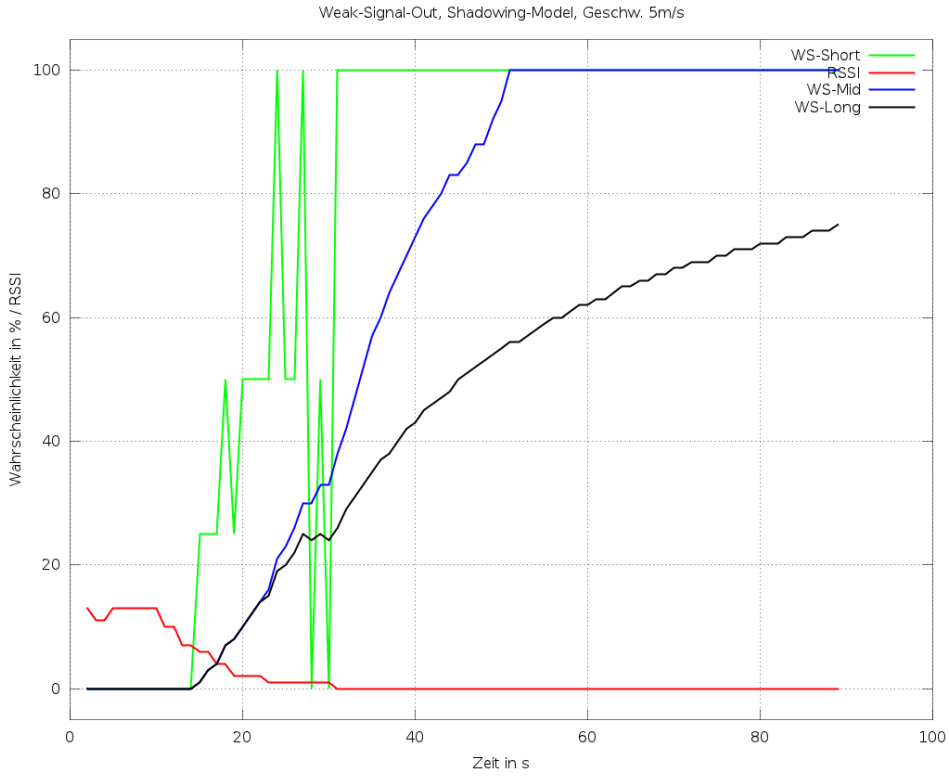

Abbildung 4.14: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Shadowing-Model, dynamisch-out, Geschw. 5 m/s

Geschwindigkeit 5 m/s Wie in Abbildung 4.14 zu erkennen ist, steigt die Paketverlustwahrscheinlichkeit schon nach kurzer Zeit auf 100 Prozent. Die RSSI-Werte

sinken innerhalb von 30 Sekunden auf null. Der Verlauf Paketverlustwahrscheinlichkeit ist durch die 2,5-fache Geschwindigkeit geradliniger als in der Simulation zuvor. Es gibt einen kleinen Bereich, in der die Wahrscheinlichkeit nochmals kurz auf null Prozent absinkt, um danach aber dauerhaft auf 100 Prozent zu verweilen.

Es wurden 2557 Pakete gesendet, die Anzahl der Kollisionen verharrt weiter auf null. Die Wiederholungsrate hat sich auf 71,29 % erhöht, was im Vergleich zur 2,5-fachen Geschwindigkeit der Station zwei, recht gering ist.

Auswertung

Die verschiedenen Simulationen zur Erhöhung der Distanz zeigen die Abschätzung plausibler Wahrscheinlichkeiten für Paketverluste auf Grund von zu schwachen Signalen. Auch hier schwanken die Werte der Einzelwahrscheinlichkeiten gerade bei der Simulation mit dem Shadowing-Model recht stark, sodass eine Glättung durch gleitende Mittelwerte angebracht ist.

4.2 Paketverluste durch In-Range-Kollisionen

Um die Abschätzung der Paketverlustwahrscheinlichkeit verursacht durch In-Range-Kollisionen zu testen, wurden vier Szenarien mit unterschiedlich vielen Nachbarstationen entwickelt. Je höher die Anzahl der Nachbarstationen ist, desto höher sollte die Paketverlustwahrscheinlichkeit sein.

4.2.1 Zwei Nachbarn

Zuerst werden zwei Nachbarstationen simuliert, dass heißt insgesamt sind drei Stationen an diesem Szenario beteiligt. Die erste Station wird auf den Koordinaten (0 15 0) positioniert und fungiert als Beobachter-Station. Station zwei wird auf die Koordinaten (0 0 0) gesetzt und Station drei auf die Koordinaten (0 10 0). Alle drei Stationen befinden sich damit innerhalb der Sende- und Empfangsreichweiten der jeweiligen anderen Stationen.

Der erste Simulationslauf wird mit dem Two-Ray-Ground-Reflection-Model gestartet. Da sich die Wahrscheinlichkeit der Paketverluste aus der Anzahl der Nachbarstationen und dem Contention-Window errechnet (siehe S. 13), wird die Wahrscheinlichkeit bei gleichbleibendem Contention-Window und gleichbleibender Anzahl von Nachbarn ebenfalls gleich bleiben.

Two-Ray-Ground-Reflection-Model

In Abbildung 4.15 ist gut zu erkennen, dass sich bei einem gleichbleibendem Contention-Window-Wert (in der Abbildung als CW gekennzeichnet) und gleichbleibender Anzahl der Nachbarn wie prognostiziert die Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision (in der Abbildung als Inrange-Short bezeichnet) nicht ändert.

Es wurden insgesamt 110588 Pakete versendet, wobei es zu 523 Kollisionen kam. Die Wiederholungsrate liegt bei vernachlässigbaren 0,47 % und liegt damit unter den zwei Prozent Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen.

Interessant ist, dass die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen (in der Abbildung als Non-Wifi-Short bezeichnet) bei rund acht Prozent liegt. Bei der vorhergehenden Weak-Signal-Simulationen mit dem Two-Ray-Ground-Reflection-Model beträgt die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen nur null bis zwei Prozent. Vermutlich werden Pakete, die auf Grund der In-Range-Kollision kaputt gehen, zwar nicht mehr als 802.11-konforme Signale empfangen, aber die Energieerkennung registriert das Paket trotzdem. Durch die unterschiedliche Anzahl von Empfangenen Signalen und als 802.11-konform erkannten Signalen, steigt die geschätzte Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi.

Shadowing-Model

Als nächstes wird die Simulation mit der Shadowing-Model wiederholt. Die Stationen bleiben auf den oben genannten Koordinaten. Zu erwarten ist eine gleichbleibende Wahrscheinlichkeit für Paketverluste auf Grund von

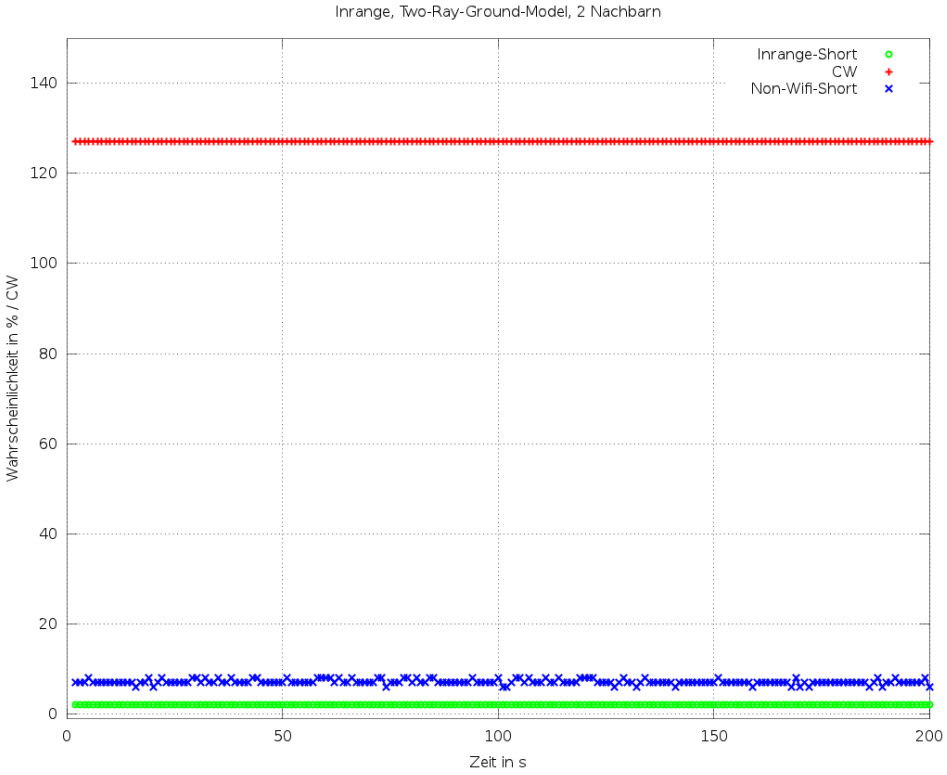

Abbildung 4.15: Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Two-Ray-Ground-Reflection-Model, 2 Nachbarn

In-Range-Kollision, die sich von der In-Range-Kollisionswahrscheinlichkeit mit dem Two-Ray-Ground-Reflection-Model nicht unterscheiden dürfte.

Auf Grund der Eigenschaften der Shadowing-Model sollte die Wahrscheinlichkeit für Non-Wifi-Paketverluste höher liegen, als bei der eben durchgeführten Simulation.

Wie in Abbildung 4.16 zu beobachten ist, ist die Paketverlustwahrscheinlichkeit für In-Range-Kollisionen (Inrange-Short in der Abbildung) wie vorhergesagt im Vergleich zum Two-Ray-Ground-Reflection-Model gleich geblieben. Die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen ist dagegen auf Werte von 13 bzw. 14 Prozent gestiegen. Diese Werte sind im Vergleich zur stationären Weak-Signal-Simulation mit dem Shadowing-Model deutlich erhöht. Bei der Weak-Signal-Simulation mit einer Distanz von 30 liegen die Non-Wifi-Werte lediglich bei eins. Bei 148613 gesendeten Paketen gab es 418 Kollisionen. Die Wiederholungsrate liegt bei 0,37 %, was unter der Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen von zwei Prozent liegt.

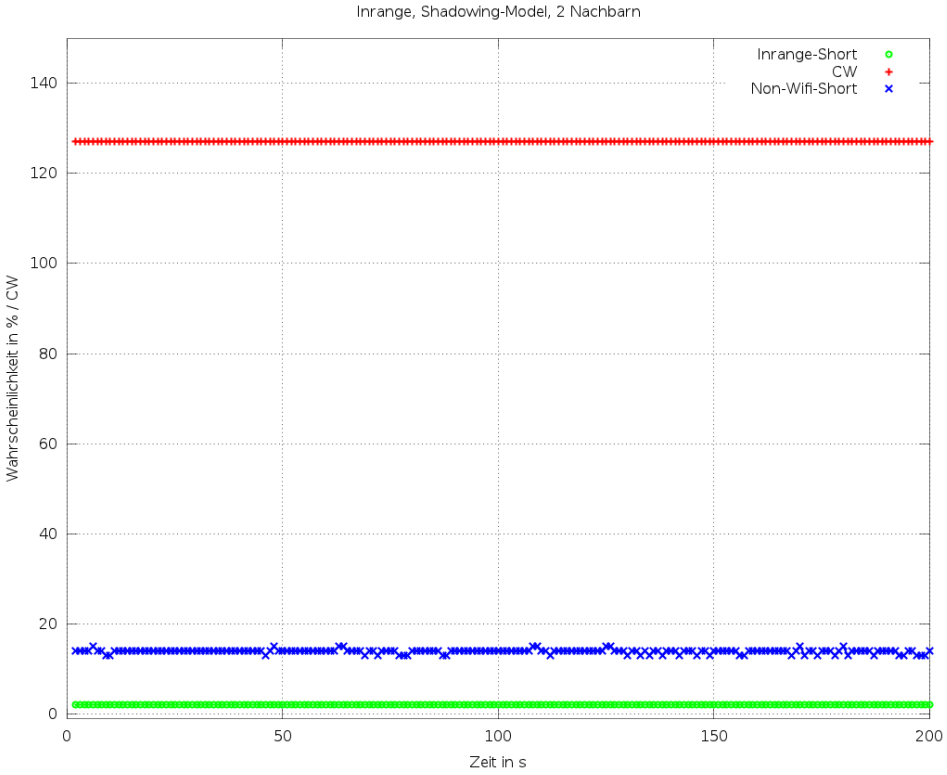

Abbildung 4.16: Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 2 Nachbarn

4.2.2 Fünf Nachbarn

In der nächsten Simulation werden fünf Nachbarn simuliert. Station eins ist wieder der Beobachter und wird auf den Koordinaten (0 15 0) platziert. Die Stationen zwei bis sechs werden auf den Koordinaten (0 0 0), (0 10 0), (0 14 0), (0 20 0) und (0 25 0) platziert. Da die geschätzten Paketverlustwahrscheinlichkeiten auf Grund von In-Range-Kollisionen in diesem Szenario nicht von den Antenneneigenschaften abhängen, und die ermittelten Werte bei Simulationen mit dem Two-Ray-Ground-Reflection-Model und dem Shadowing-Model bei gleicher Anzahl von Nachbarstationen und gleichem Contention-Window gleich sind, wird stellvertretend nur die Simulation mit dem Shadowing-Model ausgewertet, da die Entwicklung der Paketverluste auf Grund von Non-Wifi-Signalen deutlicher zu sehen sein wird.

Bei fünf Nachbarn ist eine höhere Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen zu erwarten und damit einhergehend auch eine Erhöhung der Wahrscheinlichkeit von Paketverlusten auf Grund von Non-Wifi-Signalen.

Wie in Abbildung 4.17 beobachtet werden kann, liegt die In-Range-Kollisionswahrscheinlichkeit bei 11 Prozent und damit höher, als bei zwei Nachbarstationen.

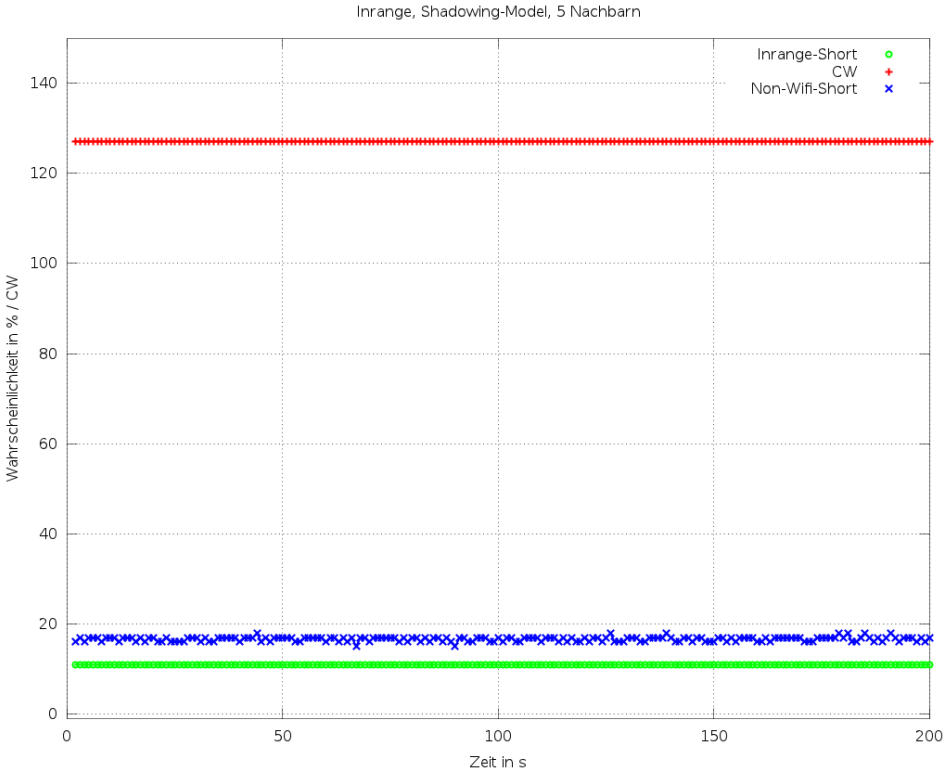

Abbildung 4.17: Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 5 Nachbarn

Wie vorhergesagt, ist auch die Wahrscheinlichkeit für Non-Wifi-Paketverluste gestiegen, und zwar auf Werte von 16 bzw. 17 Prozent. Die Anzahl der Kollisionen ist bei 173162 gesendeten Paketen auf 2491 Kollisionen gestiegen und die Wiederholungsrate liegt bei 2,11 % und damit unter der geschätzten In-Range-Kollisionswahrscheinlichkeit von 11 Prozent.

4.2.3 Zehn Nachbarn

Als nächstes wird die Anzahl der Nachbarstationen auf zehn verdoppelt. Die fünf weiteren Stationen werden in der Nähe der sechs Stationen der vorherigen Simulation platziert. Erwartet wird ein weiterer Anstieg der Wahrscheinlichkeiten für Paketverluste auf Grund von In-Range-Kollisionen und Non-Wifi-Signalen.

Abbildung 4.18 zeigt, dass sich die Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen auf 35 Prozent erhöht hat. Die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen ist dabei nur auf Werte zwischen 18 und 21 Prozent gestiegen. Die Kollisionsanzahl ist bei 183838 gesendeten Paketen auf 6359 gestiegen, die Wiederholungsrate liegt bei 4,71 % und

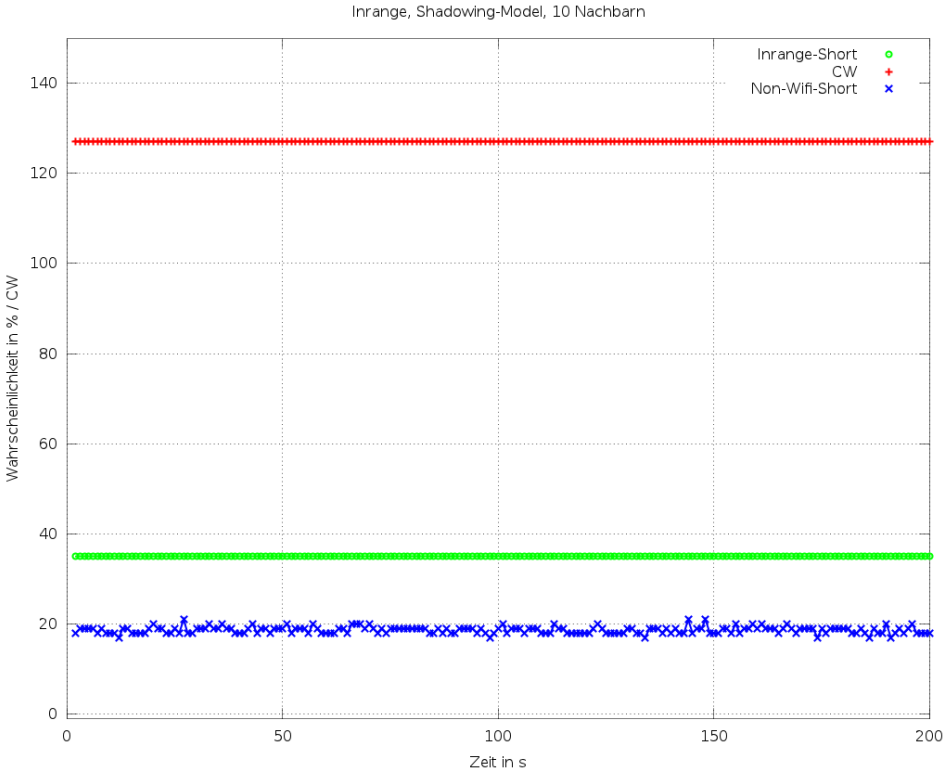

Abbildung 4.18: Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 10 Nachbarn

damit wie in den beiden vorherigen Simulationen weit unter der geschätzten In-Range-Paketverlustwahrscheinlichkeit.

4.2.4 Zwanzig Nachbarn

Als letzte Simulation zum Test der Schätzung von Paketverlustwahrscheinlichkeiten auf Grund von In-Range-Kollisionen wird die Anzahl der Nachbarstationen auf 20 erhöht. Die zusätzlichen zehn Stationen werden wieder in der Nähe der aus der vorherigen Simulationen stammenden 11 Stationen platziert.

Die Wahrscheinlichkeiten für Paketverluste werden sowohl für die durch In-Range-Kollisionen verursachten als auch die Non-Wifi-Signale verursachten weiter steigen.

Zu beobachten sind in Abbildung 4.19 eine Steigerung der Paketverlustwahrscheinlichkeiten auf Grund von In-Range-Kollisionen auf über 80 Prozent, was bei einem Contention-Window-Wert von 128 plausibel ist. Die Wahrscheinlichkeit für Non-Wifi-Signale als Paketverlustursache ist dagegen moderat auf Werte zwischen 20 und 24 Prozent gestiegen. Bei 191297 gesendeten Paketen traten 16806 Kollisio-

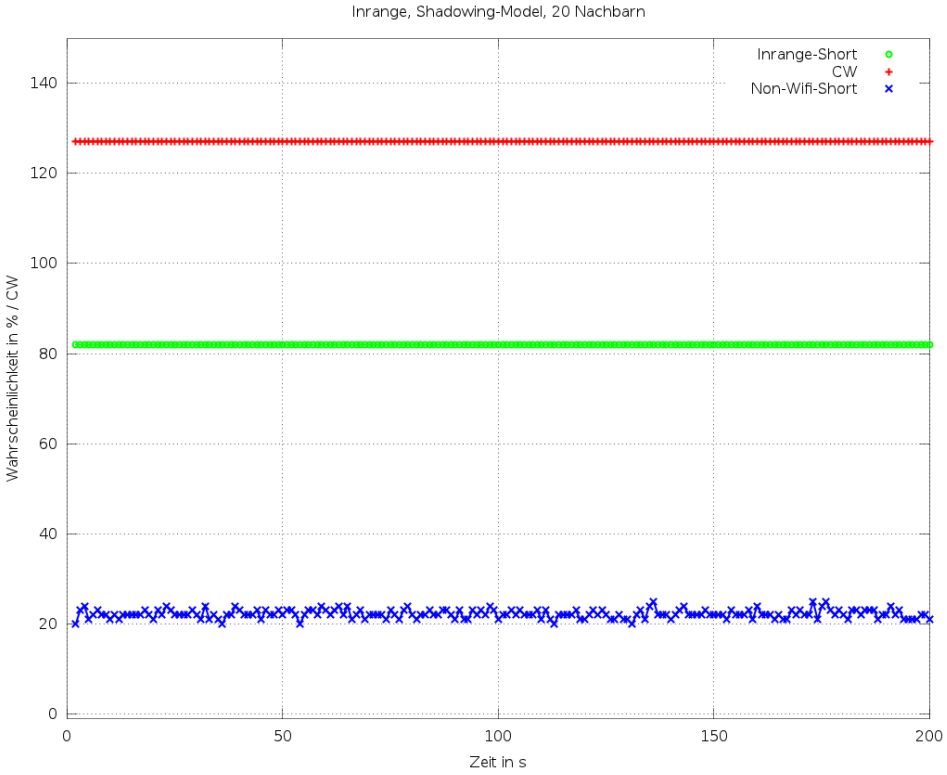

Abbildung 4.19: Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 20 Nachbarn

nen auf. Die Wiederholungsrate liegt bei lediglich 10,83 % und beträgt damit gerade ein achtel der auf 80 Prozent geschätzten In-Range-Paketverlustwahrscheinlichkeit.

4.2.5 Auswertung

In den beiden Abbildungen 4.20 und 4.21 sind noch einmal die Wahrscheinlichkeiten für Paketverluste auf Grund von In-Range-Kollisionen und Non-Wifi-Signalen für zwei, fünf, zehn und 20 Nachbarstationen zusammengefasst worden. Wobei Abbildung 4.20 die Simulationen mit dem Two-Ray-Ground-Reflection-Model und Abbildung 4.21 die Simulationen mit dem Shadowing-Model zeigt.

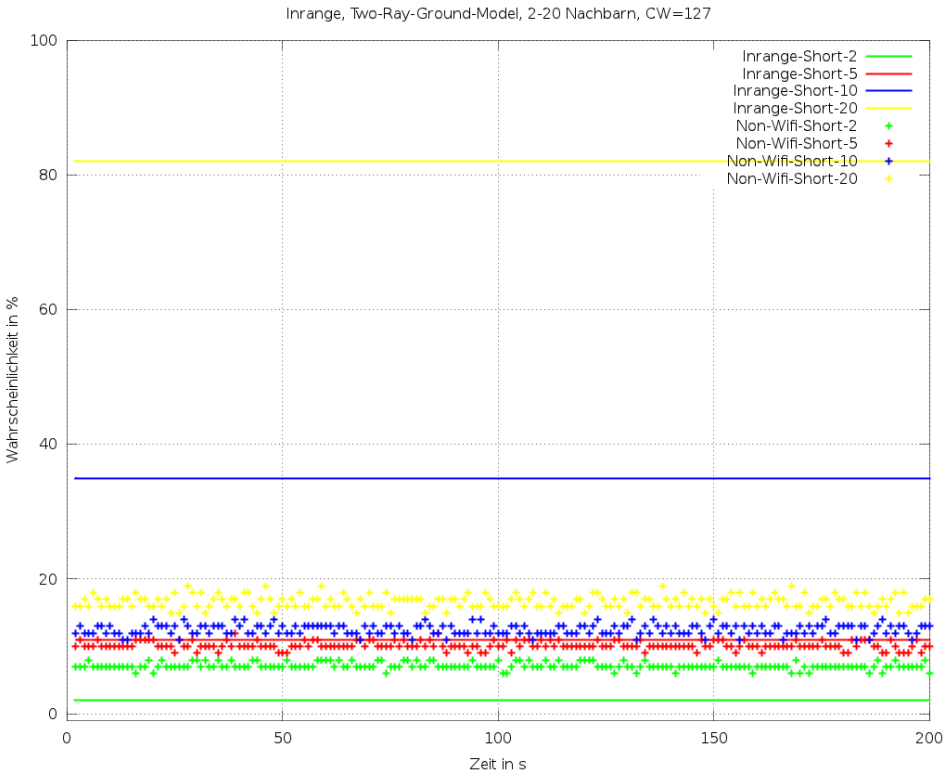

Abbildung 4.20: Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Two-Ray-Ground-Reflection-Model, 2 bis 20 Nachbarn

Es ist deutlich zu sehen, dass die Wahrscheinlichkeit für Paketverluste auf Grund von In-Range-Kollisionen mit zunehmender Anzahl der Nachbarstationen steigt, unabhängig von den Eigenschaften des gewählten Pfadverlustmodells.

Die durch die In-Range-Kollisionen zerstörten Pakete sind der Grund für die erhöhten Wahrscheinlichkeiten von Paketverlusten auf Grund von Non-Wifi-Signalen. Dabei steigt diese Wahrscheinlichkeit wesentlich langsamer, als die der In-Range-Paketverluste an.

Auch sind Unterschiede zwischen den beiden Pfadverlustmodellen feststellbar. Die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen ist bei der Simulation mit dem Shadowing-Model etwas höher.

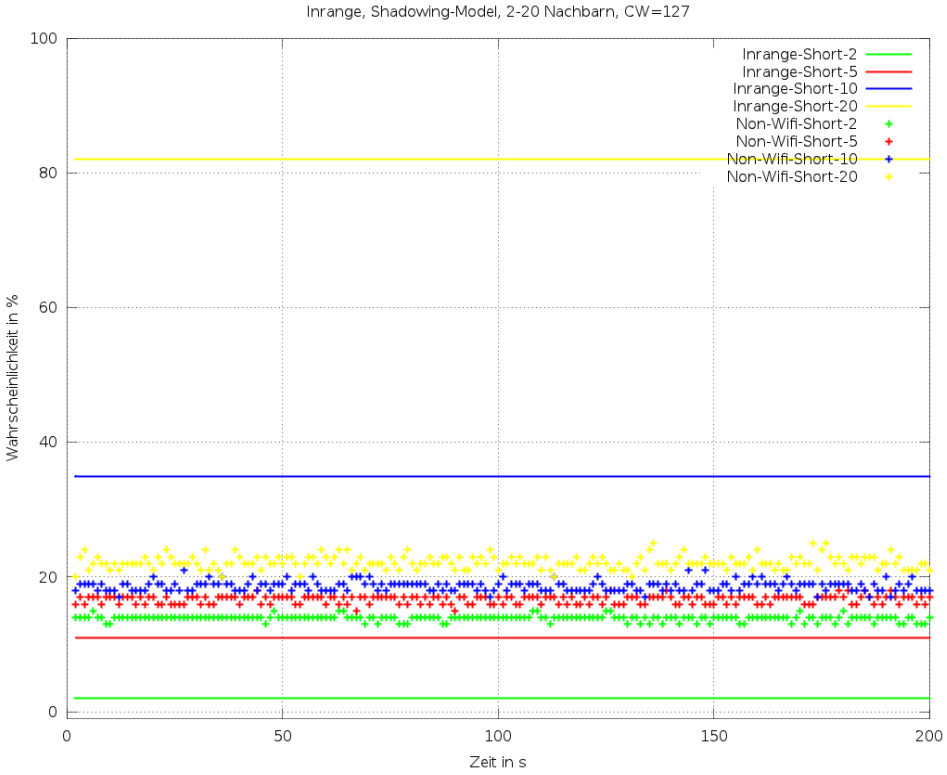

Abbildung 4.21: Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 2 bis 20 Nachbarn

Die geschätzten Werte für Paketverluste auf Grund von In-Range-Kollisionen scheinen im Vergleich zur Anzahl der beobachteten Kollisionen und der Wiederholungsrate zu hoch zu sein. Mögliche Gründe dafür sind nicht ganz ausgelastete Sender und ein durch die Simulation verursachter häufiger asynchroner Start der Signalaussendung.

4.3 Paketverluste durch Hidden-Nodes

Zum Test der Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes sind drei Szenarien mit ein, zwei und vier Hidden-Nodes entwickelt worden.

4.3.1 Ein Hidden-Node

Als erstes wird nur ein Hidden-Node simuliert. Dazu werden drei Stationen benötigt, die in einer Linie platziert werden. Die erste Station wird auf den Koordinaten (0 50 0) platziert. Die zweite Station wird in einer Entfernung von 150 m von der ersten Station auf die Koordinaten (150 50 0) gesetzt. Die dritte Station befindet sich auf den Koordinaten (300 50 0) und damit 300 m von der ersten Station entfernt. Station eins und drei können nicht miteinander kommunizieren, da sie jeweils außerhalb ihrer Sende- bzw. Empfangsreichweiten liegen. Einzig Station zwei liegt innerhalb der Empfangs- und Sendereichweite der Stationen eins und drei. Die Simulation wird zweimal ohne Kooperation zwischen den Stationen und zweimal mit Kooperation zwischen den Stationen ausgeführt.

Two-Ray-Ground-Reflection-Model, nicht-kooperativ

Der erste Simulationslauf wird mit dem Two-Ray-Ground-Reflection-Model gestartet. Wobei eine recht gleichmäßige Verteilung der Wahrscheinlichkeit erwartet wird.

Wie in Abbildung 4.22 gut zu sehen ist, schwankt die Wahrscheinlichkeit für Paketverluste verursacht durch Hidden-Nodes (in der Abbildung als Hidden-Node Short gekennzeichnet) zwischen 40 und 60 Prozent. Wird der gleitende Durchschnitt über 20 Sekunden diese Werte betrachtet (Hidden-Node Mid in der Abbildung), ergeben sich Werte von ungefähr 48 Prozent. Während der Simulation gab es bei 31829 versendeten Paketen 599 Kollisionen. 6,19 % der gesendeten Pakete mussten erneut übertragen werden.

Shadowing-Model, nicht-kooperativ

Als nächstes wird die Simulation mit dem Shadowing-Model gestartet. Vorher müssen die Stationen zwei und drei neu positioniert werden. Sie befinden sich für die folgende Simulation mit einer Distanz von 90 und 180 m zur Station eins auf den Positionen (90 50 0) und (180 50 0).

Die Paketverlustwahrscheinlichkeiten für die kommende Simulation werden im Vergleich zur letzten Simulation wahrscheinlich weniger gleichmäßig sein.

In Abbildung 4.23 ist zu sehen, dass die Wahrscheinlichkeit für Paketverluste verursacht durch Hidden-Nodes (Hidden-Node Short in der Abbildung) für einige Sekunden auf null fällt. Dies kommt dadurch zu Stande, dass auf Grund der Eigenschaften des Shadowing-Model immer wieder einzelne Pakete der Station drei von Station eins empfangen werden. Sobald dies geschieht, ist wird aus dem Hidden-Node ein direkter Nachbar, wodurch die Wahrscheinlichkeit auf null sinkt.

Die Wahrscheinlichkeit schwankt zwischen den eben erwähnten null Prozent und knapp über 20 Prozent. Wird der gleitende Durchschnitt über 20 Sekunden gebildet (Hidden-Node Mid in der Abbildung), liegen die Werte zwischen sechs und 14

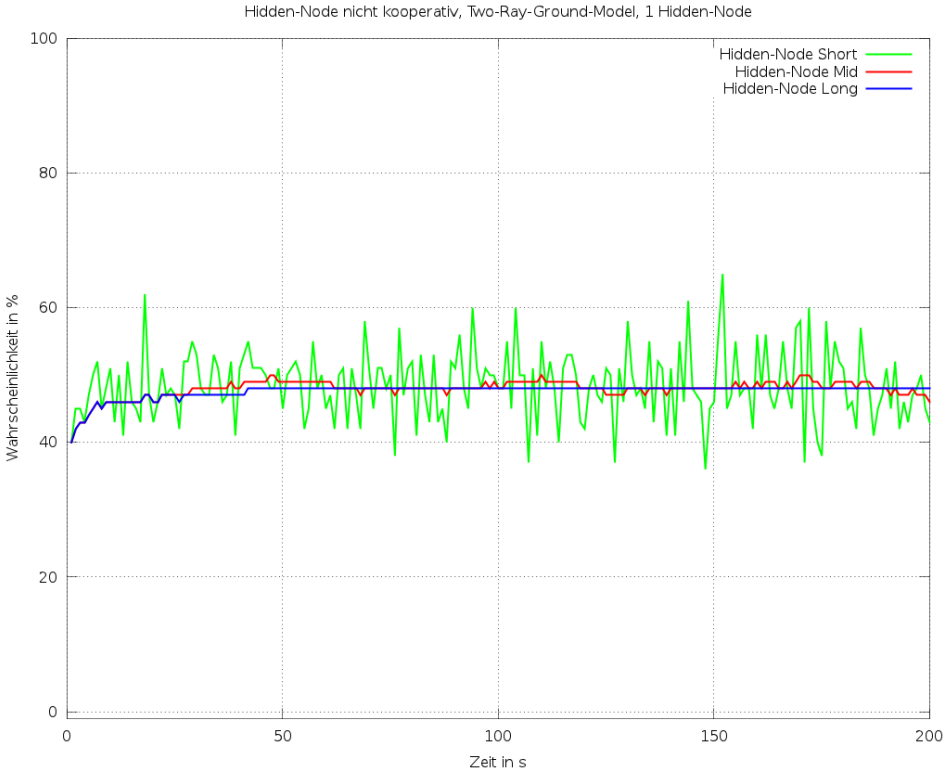

Abbildung 4.22: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 1 Hidden-Node, nicht-kooperativ

Prozent. Mit nur 36 Kollisionen bei 24147 gesendeten Paketen ist die Kollisionsrate sehr niedrig im Vergleich zur Berechnung. Allerdings liegt die Rate der wiederholten Pakete bei 32,31 %.

Bemerkenswert ist die sehr hohe Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen (Non-Wifi Short in der Abbildung). Im vorherigen Simulationslauf mit dem Two-Ray-Ground-Reflection-Model lag die Wahrscheinlichkeit bei konstant null Prozent.

Die als Non-Wifi-Signale klassifizierten Signale sind Störungen des Hidden-Nodes. Die Erkennung eines Signals wird noch angesprochen, allerdings lassen sich die Informationen des empfangenen Signals nicht mehr dekodieren, wodurch dieses Paket als nicht-802.11-konform eingestuft wird.

Two-Ray-Ground-Reflection-Model, kooperativ

In dieser Simulation kooperieren die Nachbarstationen miteinander, indem sie regelmäßig Statistiken über ihre Nachbarstationen austauschen. Dabei werden Daten wie Anzahl der gesendeten Pakete und Dauer der Übertragung gesendet.

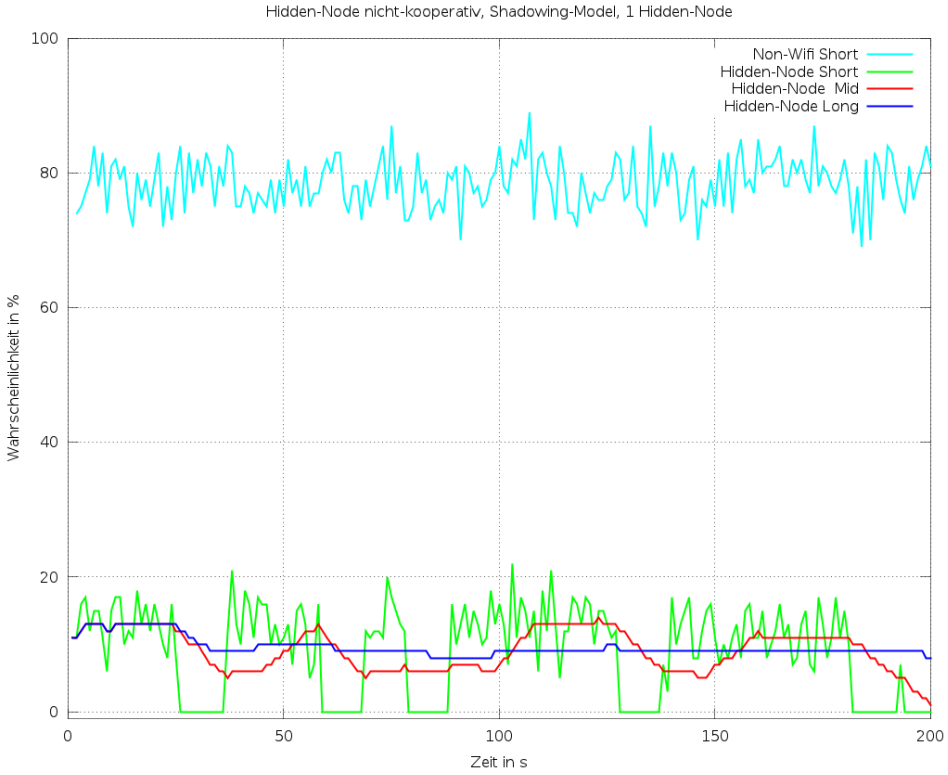

Abbildung 4.23: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 1 Hidden-Node, nicht-kooperativ

Das führt natürlich zu zusätzlichem Datenaufkommen, aber möglicherweise wird die Erkennung von Hidden-Nodes verbessert.

Die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes liegt knapp über 40 Prozent, wie man in Abbildung 4.24 erkennen kann, und damit ein wenig niedriger als in der Simulation ohne Kooperation mit dem Two-Ray-Ground-Reflection-Model. Die Anzahl der Kollisionen hat sich bei 31882 gesendeten Paketen auf 1730 im Vergleich zur nicht-kooperativen Simulation mit dem Two-Ray-Ground-Reflection-Model fast verdreifacht. Dies ist vermutlich auf die zusätzlich gesendeten Statistiken zurückzuführen. Die Wiederholungsrate ist mit 8,15 % annähernd gleich geblieben.

Shadowing-Model, kooperativ

Als nächstes wird die Kooperation beibehalten, aber das Shadowing-Model verwendet. Die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes sollten höher liegen als in der gleichen Simulation ohne Kooperation.

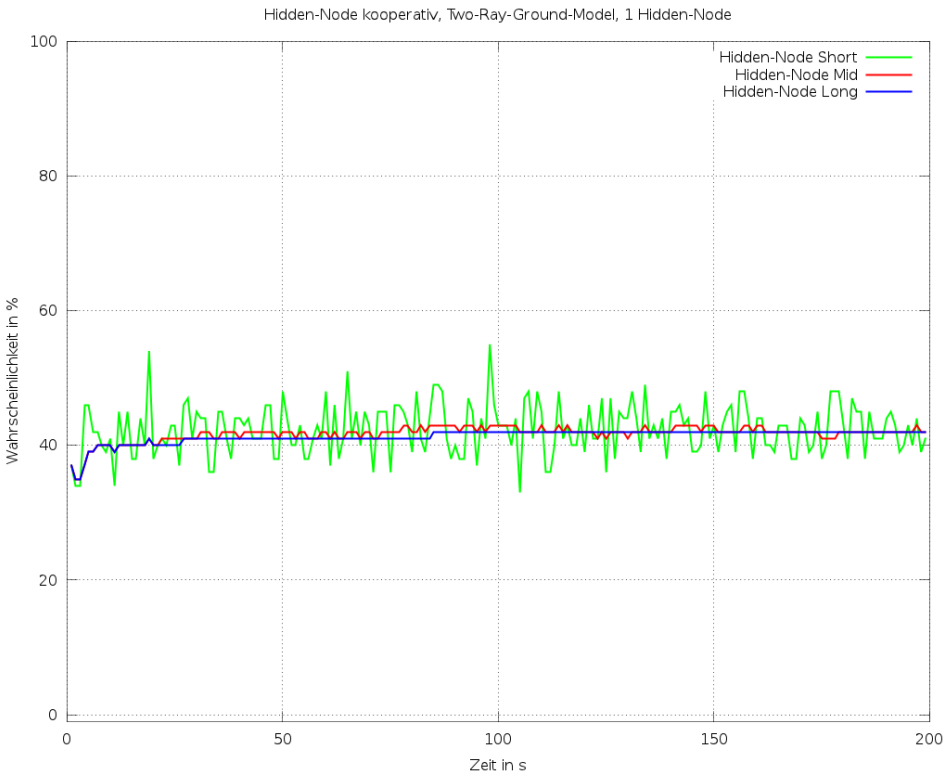

Abbildung 4.24: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 1 Hidden-Node, kooperativ

Im Gegensatz zu den Simulationen mit dem Two-Ray-Ground-Reflection-Model, unterscheiden sich die Ergebnisse deutlich. Schwankt die Wahrscheinlichkeit für Paketverluste verursacht durch Hidden-Nodes in der nicht-kooperativen Simulation im gleitenden Mittel zwischen sechs und 20 Prozent, liegt der gleitende Durchschnitt der Werte der kooperativen Simulation nach der Anfangsphase zwischen 14 und 30 Prozent. Nicht geändert hat sich die hohe Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen, die weiterhin bei etwa 80 Prozent liegt.

Abbildung 4.25: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 1 Hidden-Node, kooperativ

4.3.2 Zwei Hidden-Nodes

In der nächsten Simulation wird die Anzahl der Hidden-Nodes auf zwei erhöht. Station eins wird auf die Koordinaten (0 15 0), Station zwei auf die Koordinaten (150 15 0), Station drei auf die Koordinaten (300 10 0) und Station vier auf die Koordinaten (300 30 0) gesetzt. Die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes sollte sich deutlich erhöhen, da jetzt zwei Hidden-Nodes Datenpakete senden.

Two-Ray-Ground-Reflection-Model, nicht-kooperativ

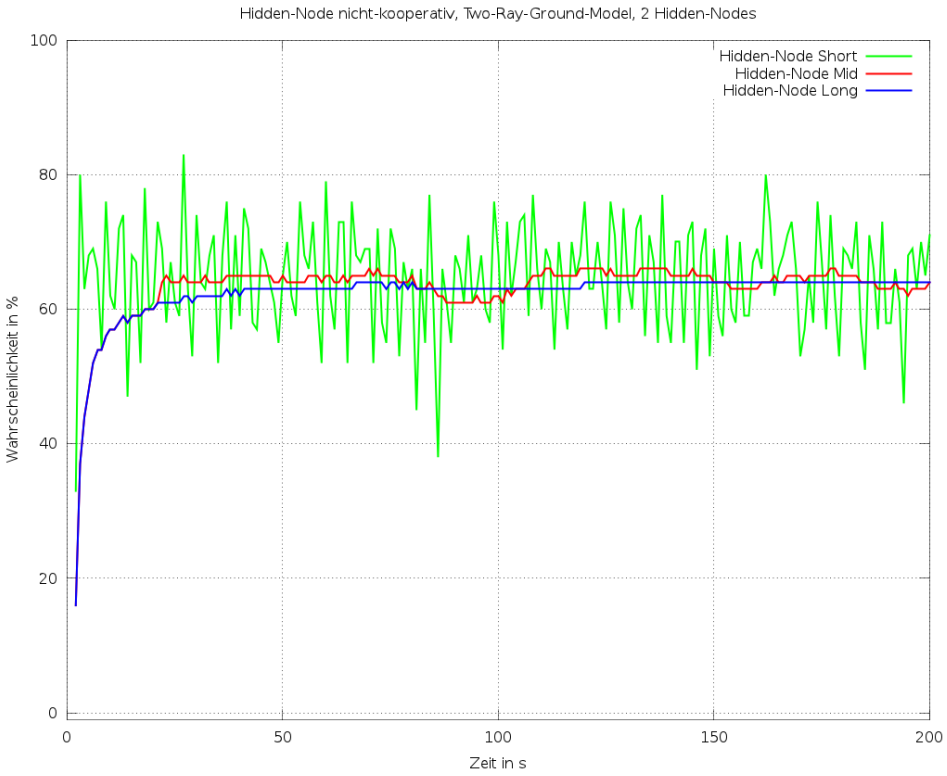

Abbildung 4.26: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 2 Hidden-Nodes, nicht-kooperativ

Die Paketverlustwahrscheinlichkeit für Hidden-Node ist, wie in Abbildung 4.26 zu sehen ist, entgegen der Prognose nur um knapp 15 Prozent gestiegen. Die recht geringe Steigerung der Wahrscheinlichkeit liegt an der Anzahl von empfangenen Ack-Paketen, die wahrscheinlich durch eine In-Range-Situation zwischen den Stationen zwei, drei und vier ausgelöst wird.

Die Anzahl der Kollisionen ist von 599 auf 4885 bei 32018 gesendeten Paketen recht deutlich gestiegen. Die Wiederholungsrate liegt bei 15,39 %.

Shadowing-Model, nicht-kooperativ

Als nächstes wird die Simulation mit dem Shadowing-Model gestartet. Dazu werden die Stationen neu positioniert. Station eins bleibt auf den Koordinaten (0 15 0). Station zwei wird auf die Koordinaten (85 15 0), Station drei auf die Koordinaten (175 10 0) und Station vier auf die Koordinaten (175 30 0) gesetzt.

Die Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes wird wie bei der Simulation mit dem Two-Ray-Ground-Reflection-Model wahrscheinlich nicht so stark ansteigen. Die Paketverlustwahrscheinlichkeit auf Grund von Non-Wifi-Signalen wird auf einem ähnlich hohen Niveau, wie bei einem Hidden-Node bleiben.

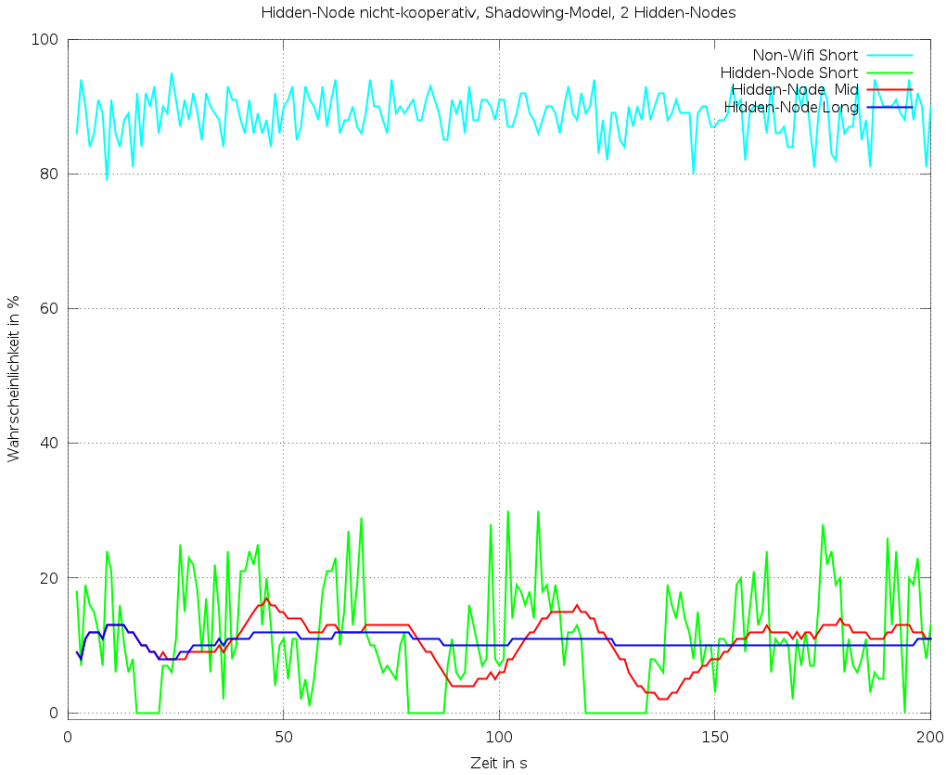

Abbildung 4.27: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 2 Hidden-Nodes, nicht-kooperativ

Abbildung 4.27 zeigt, dass die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes, wie vermutet, wenig gestiegen ist. Durch einige von Station eins empfangene Pakete sinkt die Wahrscheinlichkeit wieder auf null. Die Paketverlustwahrscheinlichkeit auf Grund von Non-Wifi-Signalen liegt zwischen 80 und 90 Prozent.

Die Anzahl der Kollisionen hat sich auf 623 erhöht, ist aber bei 24401 gesendeten Paketen immer noch recht niedrig. Mit fast 48 % Retries ist deutlich sichtbar,

dass durch die Hidden-Nodes Paketverluste auftreten, mehr als die Berechnung vorhersagt.

4.3.3 Vier Hidden-Nodes

Für die letzte Simulation werden insgesamt sechs Stationen benötigt, vier davon sind Hidden-Nodes. Die Station eins ist auf den Koordinaten (0 15 0) und die Station zwei auf den Koordinaten (150 15 0) zu finden. Station drei wird auf den Koordinaten (300 10 0), Station vier auf den Koordinaten (300 30 0), Station fünf auf den Koordinaten (300 0 0) und Station sechs auf den Koordinaten (300 40 0) positioniert.

Die Simulation wird wieder zuerst mit dem Two-Ray-Ground-Reflection-Model gestartet. Die Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes wird wieder nur leicht steigen.

Two-Ray-Ground-Reflection-Model, nicht-kooperativ

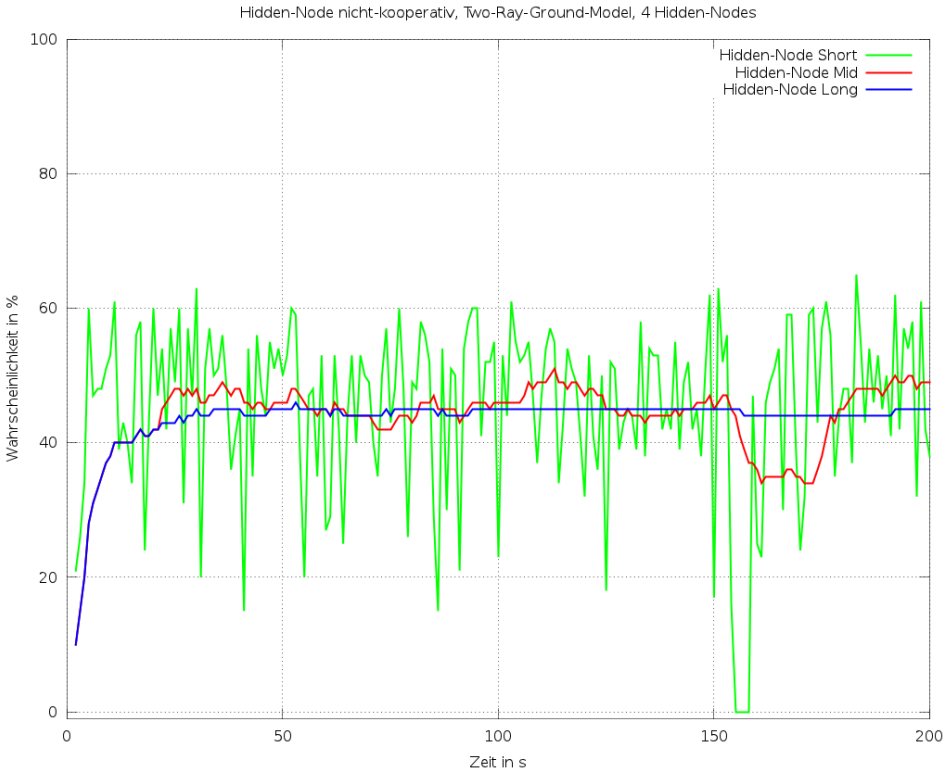

Abbildung 4.28: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 4 Hidden-Nodes, nicht-kooperativ

Wie in Abbildung 4.28 zu sehen ist, ist die Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes überraschender Weise gesunken, obwohl sich Anzahl der Hidden-Nodes verdoppelt hat. Die Wahrscheinlichkeit hat allerdings eine recht hohe Schwankungsbreite und liegt zwischen 15 und 63 Prozent. Wobei sie für kurze Zeit bis auf null absinkt. Der gleitende Durchschnitt der Werte über 20 Sekunden liegt meist zwischen 40 und 50 Prozent, wobei durch das Absinken auf null, der gleitende Mittelwert einen Minimalwert von 34 in diesem Bereich erreicht.

Die Anzahl der Kollisionen ist bei 33601 Paketen auf 11775 Kollisionen gestiegen. Die Wiederholungsrate liegt bei 37,28 %.

Vermutlich ist das Absinken der Wahrscheinlichkeit auf In-Range-Kollisionen zwischen den Stationen zwei bis sechs zurückzuführen. Die hohe Kollisionsrate lässt darauf schließen.

Shadowing-Model, nicht-kooperativ

Als nächstes wird die Simulation mit dem Shadowing-Model gestartet. Station eins bleibt dafür auf der vorherigen Position und Station zwei wird auf die Koordinaten (85 15 0) gesetzt. Die Stationen drei, vier, fünf und sechs werden auf die Koordinaten (175 10 0), (175 30 0), (175 0 0) und (175 40 0) gesetzt.

Durch die In-Range-Kollisionen, die in der Simulation mit dem Two-Ray-Ground-Reflection-Model beobachtet werden konnten und der Tatsache, dass immer wieder Pakete von den Hidden-Nodes Station eins erreichen, wird die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes recht gering ausfallen. Die Paketverlustwahrscheinlichkeit auf Grund von Non-Wifi-Signalen wird dagegen unverändert hoch sein.

Abbildung 4.29 zeigt, dass die Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes wie vorhergesagt gefallen ist. Sie geht recht häufig auf null zurück. Auffällig ist, dass die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen stark zwischen 90 und 95 Prozent einerseits und null Prozent andererseits schwankt.

Die Kollisionen sind bei 26110 gesendeten Paketen auf 3337 im Vergleich zu zwei Hidden-Nodes zurückgegangen, die Wiederholungsrate ist auf 63 Prozent gestiegen.

Two-Ray-Ground-Reflection-Model, kooperativ

Die folgende Simulation verwendet wieder das Two-Ray-Ground-Reflection-Model, dieses Mal kooperieren die Stationen miteinander. Die Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes sollte sich ähnlich entwickeln, wie in der Simulation ohne Kooperation, da die In-Range-Kollisionen der Hidden-Nodes zu ähnlichen Ergebnissen führen werden.

Im Gegensatz zur nicht-kooperativen Simulation mit dem Two-Ray-Ground-Reflection-Model, schwanken die Werte, wie in Abbildung 4.30 zu sehen ist, weniger stark. Der gleitende Durchschnitt der Wert über 20 Sekunden, schwankt um die 50 Prozent und liegt damit nur wenig höher als in der Simulation ohne Kooperation. Bei 33746 gesendeten Paketen, traten 13027 Kollisionen auf, die Wiederholungsrate liegt bei 38,68 %. Damit gab es mehr Kollisionen, als bei der nicht-kooperativen Simulation, was auf die zusätzlichen Datenpakete für den Austausch der Statistiken zwischen den Stationen zurückzuführen sein dürfte.

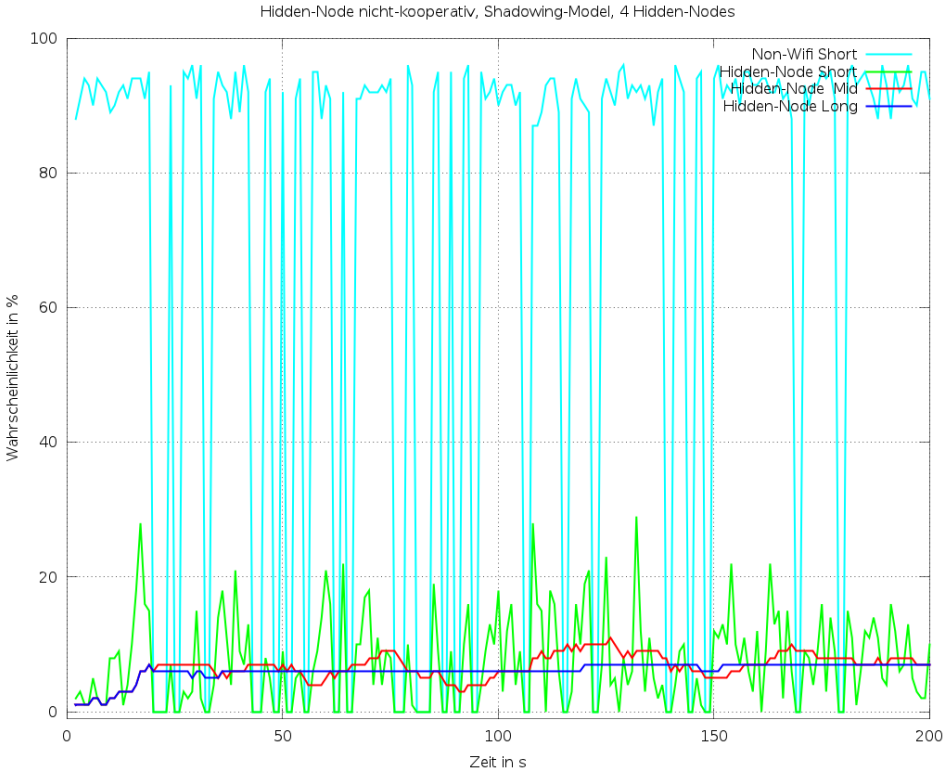

Abbildung 4.29: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 4 Hidden-Nodes, nicht-kooperativ

Shadowing-Model, kooperativ

Zuletzt wird wiederum das Shadowing-Model eingesetzt, dieses Mal mit eingeschalteter Kooperation. Die Erkennung der Hidden-Nodes sollte durch die Kooperation deutlich besser sein, als ohne Kooperation. Das wird durch die gestiegene Wahrscheinlichkeit für Paketverluste verursacht durch Hidden-Nodes zum Ausdruck kommen. Die Paketverlustwahrscheinlichkeit auf Grund von Non-Wifi-Signalen wird ähnlich hoch sein, wie bei der Simulation mit dem Shadowing-Model ohne Kooperation.

Wie erwartet, liegt die Wahrscheinlichkeit für Paketverluste verursacht durch Hidden-Nodes mit Werten zwischen 18 und 25 Prozent höher als bei der Simulation mit dem Shadowing-Model, wie Abbildung 4.31 zeigt, wenn gleich nicht so hoch wie bei den Simulationen mit dem Two-Ray-Ground-Reflection-Model. Es wurden 3680 Kollisionen bei 26336 gesendeten Paketen registriert und die Retry-Rate liegt bei knapp 63 %. Damit ist die Anzahl der Kollisionen höher als bei der Simulation ohne Kooperation. Wie bei der Simulation mit dem Two-Ray-Ground-Reflection-Model ist die erhöhte Anzahl von Kollisionen auf die zusätzlichen Statistik-Pakete, die zwischen den Stationen ausgetauscht werden, zurückzuführen.

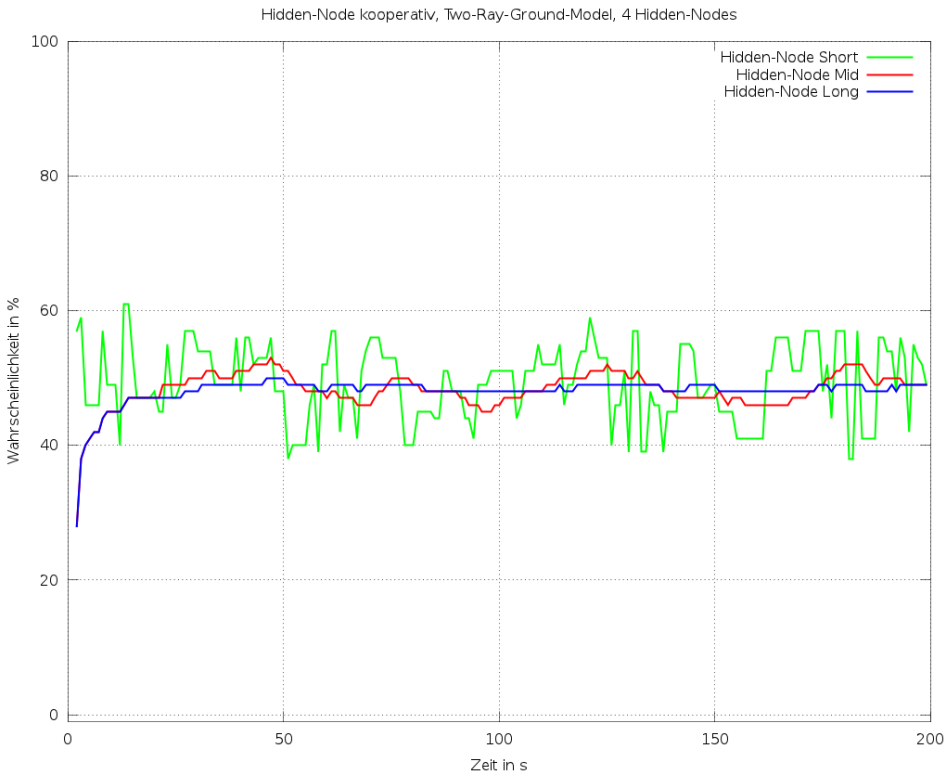

Abbildung 4.30: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 4 Hidden-Nodes, kooperativ

Die Paketverlustwahrscheinlichkeit auf Grund von Weak-Signal-Signalen ist wie erwartet annähernd gleich geblieben.

4.3.4 Auswertung

Die Hidde-Node-Szenarien haben sich als recht komplex herausgestellt. Während die Vorhersagen bei den Simulationen mit dem Two-Ray-Ground-Reflection-Model mit und ohne Kooperation noch in einem akzeptablen Bereich liegen, sind die Vorhersagen für das Shadowing-Model ohne Kooperation nicht zutreffend. Das Problem der Vorhersagen liegt in der Tatsache, dass sich ein reines Hidden-Node-Szenario nicht konstruieren lässt. Es treten immer In-Range-Kollisionen zwischen den Hidden-Nodes auf und durch kaputte bzw. zu schwache Signale, die nicht mehr als 802.11-konform erkannt werden, werden immer Non-Wifi-Signale registriert. Für das Shadowing-Model hat die Kooperation eine leichte Verbesserung der Ergebnisse gebracht, die Ergebnisse der Simulation mit dem Two-Ray-Ground-Reflection-Model wurden dagegen nur marginal verbessert.

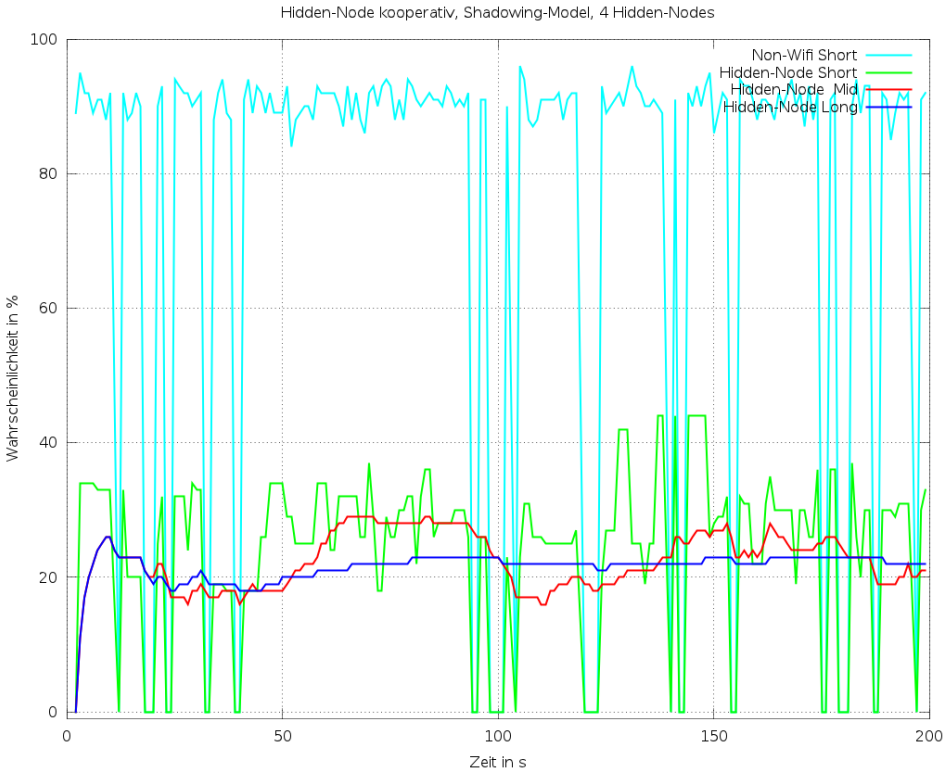

Abbildung 4.31: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 4 Hidden-Nodes, kooperativ

4.4 Paketverluste durch Non-Wifi-Störungen

Für den Test von Non-Wifi-Paketverlusten wurde ein Szenario entworfen, welches aus drei Stationen besteht. Zwei Stationen, die Pakete austauschen und einer Station dazwischen, ein sogenannter Jammer, die kaputte Pakete ohne Carrier-Sensing-Mechanismus sendet.

Station eins wird für die erste Simulation mit dem Two-Ray-Ground-Reflection-Model auf die Koordinaten (0 50 0) gesetzt, Station zwei, der Jammer, auf die Koordinaten (50 50 0) und Station drei auf die Koordinaten (100 50 0) gesetzt.

Die Wahrscheinlichkeit für Paketverluste verursacht durch Non-Wifi-Signale wird recht hoch sein.

4.4.1 Two-Ray-Ground-Reflection-Model

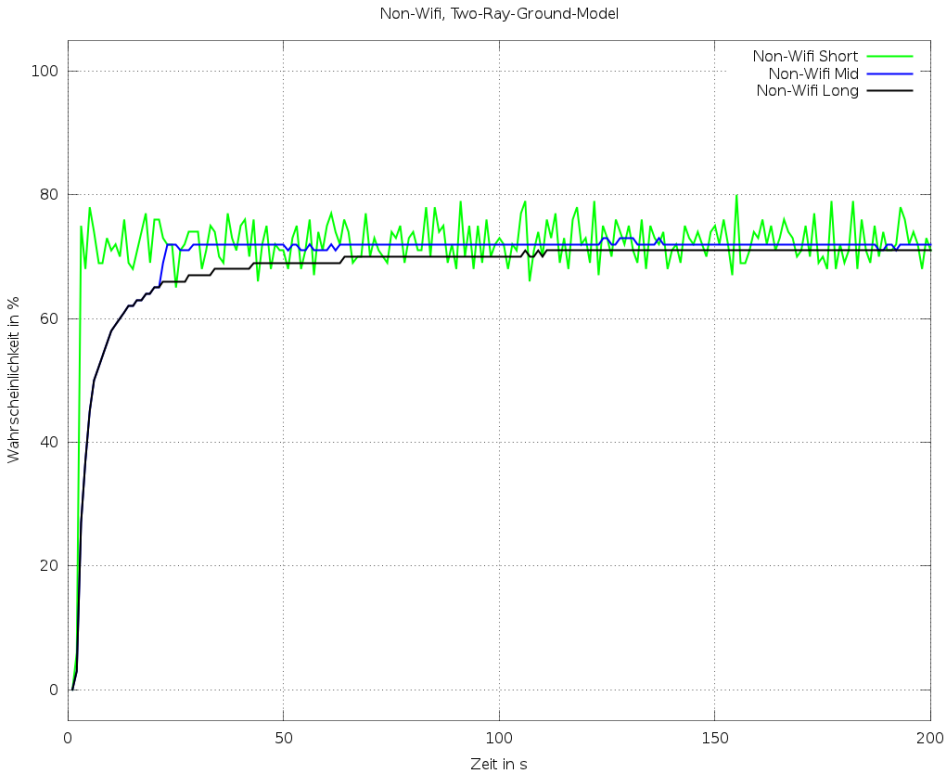

Abbildung 4.32: Wahrscheinlichkeit von Paketverlusten auf Grund von Non-Wifi-Signalen, Two-Ray-Ground-Reflection-Model

Wie in Abbildung 4.32 zu sehen ist, pendelt sich die Paketverlustwahrscheinlichkeit auf Grund von Non-Wifi-Signalen auf Werte zwischen 70 und 80 Prozent ein. Bei 20140 gesendeten Pakete werden 11592 Kollisionen verzeichnet und eine

Wiederholungsrate von null Prozent. Dies ist in diesem Fall allerdings irreführend, da Non-Wifi-Signale in Click Pakete sind, die als Non-Wifi-Signale gekennzeichnet sind. Dadurch kommt die hohe Kollisionsrate zu Stande.

4.4.2 Shadowing-Model

Als nächstes wird die Simulation noch mit der Shadowing-Model gestartet. Die Stationen werden auf den bisherigen Positionen belassen. Auf Grunde der Eigenschaften der Shadowing-Model wird die Paketverlustwahrscheinlichkeit verursacht durch Non-Wifi-Signale etwas höher liegen, als bei der Simulation mit dem Two-Ray-Ground-Reflection-Model.

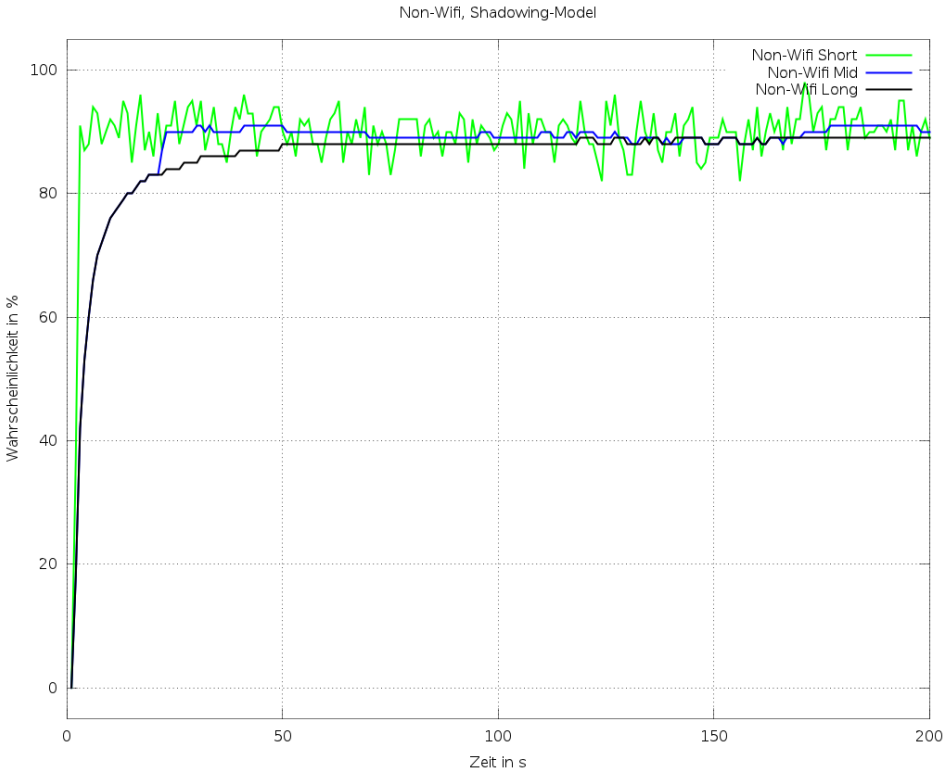

Abbildung 4.33: Wahrscheinlichkeit von Paketverlusten auf Grund von Non-Wifi-Signalen, Shadowing-Model

Wie prognostiziert und in Abbildung 4.33 gut zu erkennen, liegt die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen noch höher als in der vorherigen Simulation. Die Anzahl der Kollisionen, die hier ebenfalls irreführend ist, liegt mit 7549 bei 20208 gesendeten Paketen niedriger als bei der Simulation mit dem Two-Ray-Ground-Reflection-Model. Die Wiederholungsrate liegt wie bei der vorherigen Simulation bei null Prozent.

4.4.3 Auswertung

Mit diesem Szenario konnte gezeigt werden, dass die Abschätzung der Paketverluste durch Non-Wifi-Signale in der Simulation grundsätzlich funktioniert. Da innerhalb des Click-Frameworks bzw. des Network-Simulator-2 Non-Wifi-Signale durch annotierte Pakete simuliert werden, kann nur grundsätzlich gezeigt werden, dass eine Erkennung möglich ist, da beispielsweise schmalbandige Störsignale nicht simuliert werden können.

4.5 Szenarien mit Mobilität

Mit den folgenden drei Szenarien sollen komplexere Konstellationen und verschiedene Effekte untersucht werden. Jedes der folgenden Szenarien besteht aus drei Stationen, von denen zwei stationär sind und die dritte sich in unterschiedlicher Weise gleichmäßig bewegt.

4.5.1 Hidden-Node zu In-Range

In diesem Szenario soll sich eine Station zwei anderen Stationen so nähern, dass aus einem Hidden-Node-Szenario ein In-Range-Szenario wird. Dazu werden die Stationen eins und zwei auf die Koordinaten (0 15 0) und (150 15 0) gesetzt. Die dritte Station, sich bewegende Station, wird auf den Koordinaten (300 15 0) platziert und bewegt sich nach 10 Sekunden mit einer Geschwindigkeit von 2 Metern pro Sekunde auf die Koordinaten (140 30 0) zu. Dadurch mutiert Station drei für Station eins von einem Hidden-Node zu einem direkten Nachbarn.

Two-Ray-Ground-Reflection-Model, nicht-kooperativ

Die Simulation wird zuerst mit dem Two-Ray-Ground-Reflection-Model durchgeführt. Anfangs wird sich die Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes in einem ähnlichem Niveau wie in der Simulation mit einem Hidden-Node befinden, um dann auf null abzusinken. Gleichzeitig wird die Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen geringfügig steigen.

Wie in der Abbildung 4.34 zu sehen ist, fällt die Wahrscheinlichkeit für Paketverluste verursacht durch Hidden-Nodes nach einiger Zeit, wie prognostiziert, auf null. Gleichzeitig steigt die Wahrscheinlichkeit für Paketverluste verursacht durch In-Range-Kollisionen ein wenig an.

Kurz bevor die Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes abfällt, steigt die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen deutlich auf etwa 50 Prozent an, um dann bis auf null abzufallen und sich dann später auf einem Wert von circa 10 Prozent einzupendeln. Der Abfall dieses Wahrscheinlichkeitswertes geht mit einem Anstieg der Paketverlustwahrscheinlichkeit auf Grund von Weak-Signal bestimmt für die Station drei einher.

Dieses Verhalten zeigt deutlich, dass die Störungen des Hidden-Nodes immer mehr zunehmen, bis die ersten schwachen Signale dekodiert werden können.

Die Anzahl der Kollisionen beträgt bei 32077 gesendeten Paketen 120 und die Wiederholungsrate liegt bei 3,49 %, was auf Grund der Dynamik der Simulation nur wenig aussagekräftig ist.

Shadowing-Model, nicht-kooperativ

Für den Einsatz des Shadowing-Model für die Simulation müssen die Stationen zwei und drei neu positioniert werden. Station zwei befindet sich für die Simulation mit dem Shadowing-Model auf den Koordinaten (70 15 0) und Station drei auf den Startkoordinaten (200 15 0). Station drei bewegt nach 10 Sekunden mit einer Geschwindigkeit von 2 Metern pro Sekunde zu den Koordinaten (30 30 0). Die Paketverlustwahr-

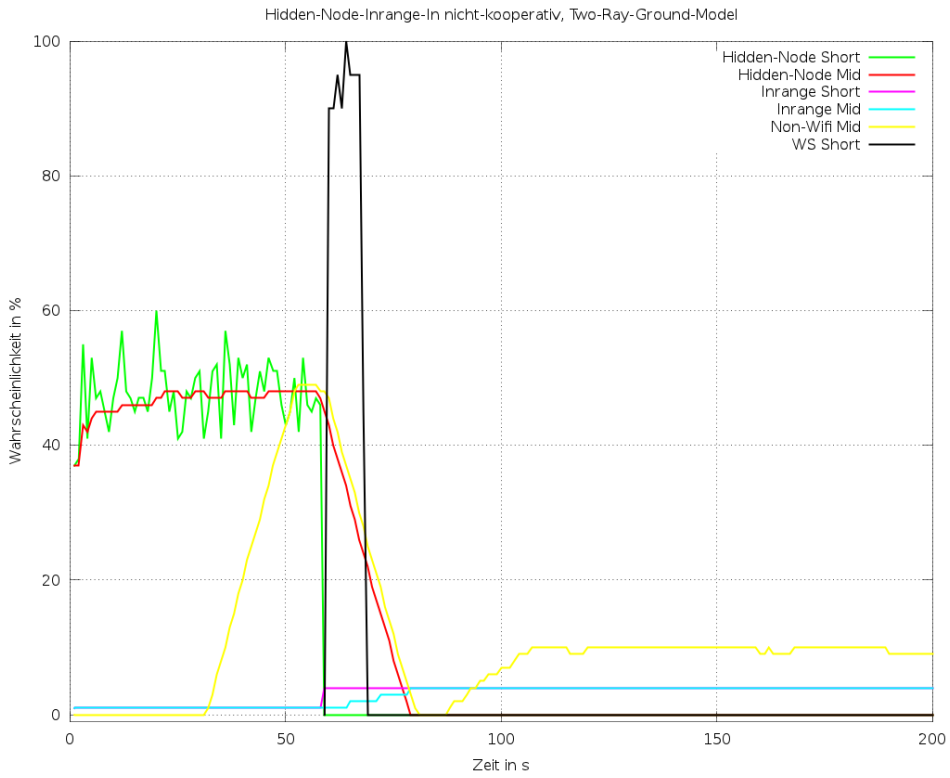

Abbildung 4.34: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR, Two-Ray-Ground-Reflection-Model, nicht-kooperativ

scheinlichkeit auf Grund von Hidden-Nodes wird ausgehend von den Erfahrungen mit dem Shadowing-Model in den Hidden-Node-Szenarien am Anfang weniger hoch sein, als bei der Simulation mit dem Two-Ray-Ground-Reflection-Model. Sobald Station drei die Empfangsbereich von Station eins erreicht wird wie in der vorherigen Simulation die Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes auf null sinken und die Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen minimal steigen.

Abbildung 4.35 zeigt deutlich den vorhergesagten Abfall der Wahrscheinlichkeit von Paketverlusten verursacht durch Hidden-Nodes und den gleichzeitigen Anstieg der In-Range-Kollisionswahrscheinlichkeit.

Die Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen steigt bis auf über 60 Prozent an und fällt nach dem Erreichen der Empfangsreichweite von Station eins langsam auf Werte um die 15 Prozent. Gleichzeitig steigt die Paketverlustwahrscheinlichkeit auf Grund von Weak-Signal für Station drei bis auf 100 Prozent an um dann langsam bis auf null Abzusinken.

Es wurden 29796 Pakete gesendet, mit einer Wiederholungsrate von knapp 10 % und 148 Kollisionen. Im Vergleich zur Simulation mit dem Two-Ray-Ground-Reflection-Model sind Wiederholungsrate und Kollisionen

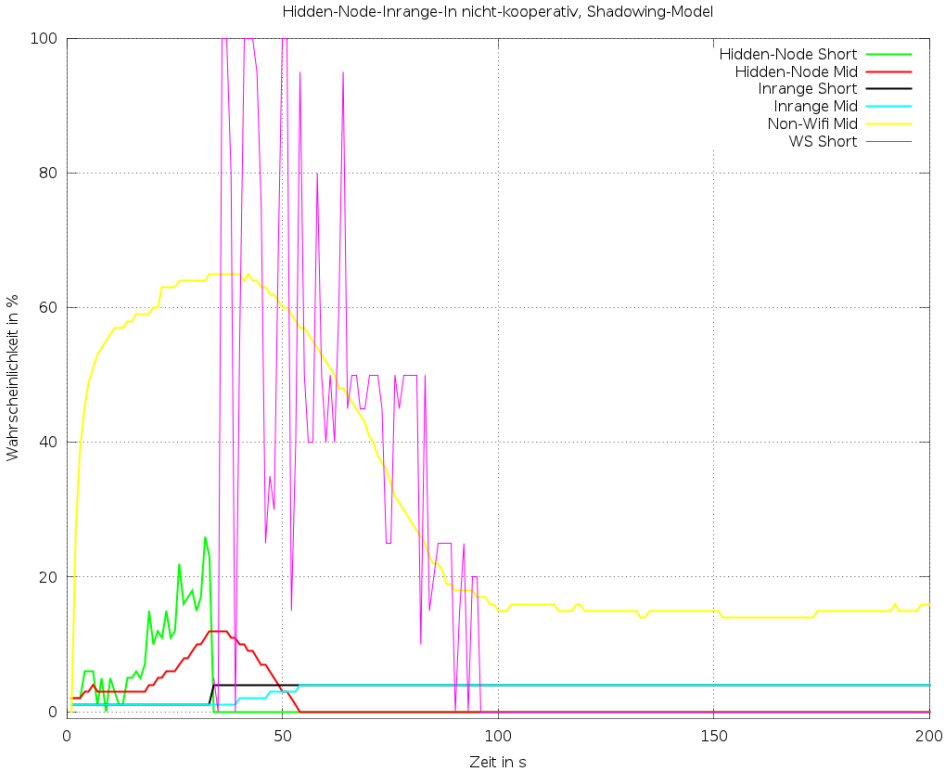

Abbildung 4.35: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR, Shadowing-Model, nicht-kooperativ

etwas höher, was auf die unterschiedlichen Eigenschaften der beiden Antennen zurückzuführen ist.

Shadowing-Model, kooperativ

Die folgende Simulation wird wieder mit dem Shadowing-Model gestartet, jetzt allerdings mit eingeschalteter Kooperation. Dadurch sollte die Erkennung des Hidden-Nodes deutlicher erfolgen, als bei der Simulation ohne eingeschaltete Kooperation, was an einem deutlichen Anstieg der Wahrscheinlichkeit für Paketverluste verursacht durch Hidden-Nodes erkennbar sein wird.

Abbildung 4.36 zeigt deutlich, dass die erwartete Verbesserung der Hidden-Node-Erkennung ausgeblieben ist. Anfangs liegt die Wahrscheinlichkeit für Paketverluste verursacht durch Hidden-Nodes in ähnlichen Bereichen wie ohne Kooperation, um dann aber auf null abzufallen. Lediglich ein kurzer Anstieg über 30 Prozent Wahrscheinlichkeit ist ein Indiz dafür, dass Paketverluste durch Hidden-Nodes verursacht werden könnten.

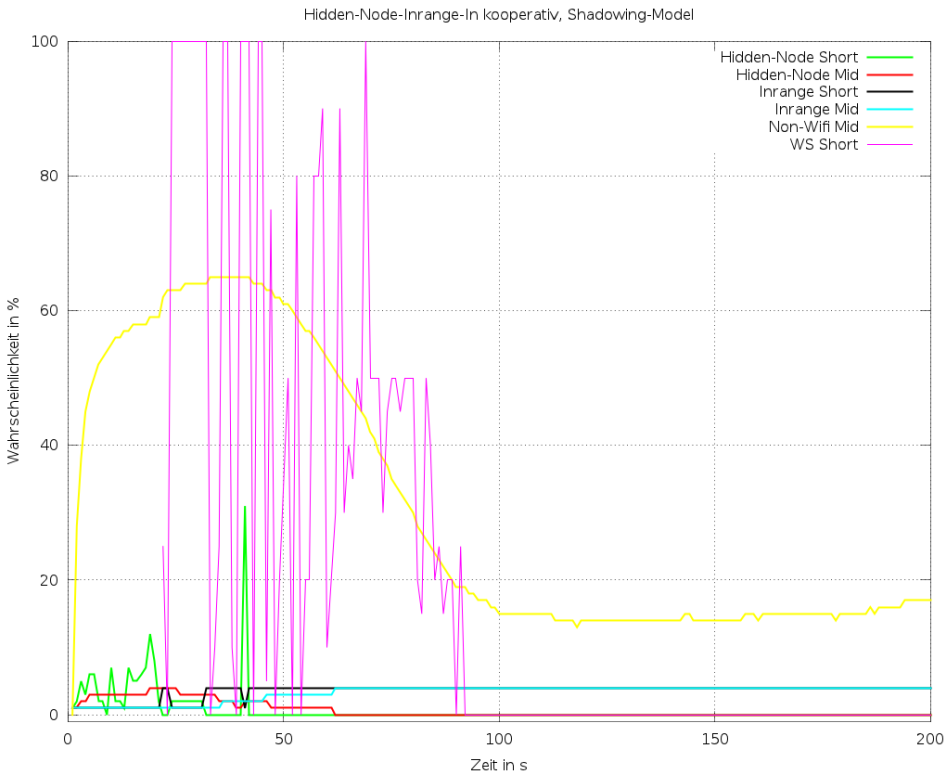

Abbildung 4.36: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR, Shadowing Model, kooperativ

Die Anzahl der Kollisionen ist durch die zusätzlichen Statistik-Pakete wieder erhöht. Es wurden bei 30162 gesendeten Paketen 370 Kollisionen gezählt. Die Wiederholungsrate liegt fast unverändert bei 9,88 %.

Die schlechte Erkennung des Hidden-Node hängt vermutlich mit zu wenigen empfangenen Statistik-Paketen zusammen und der Tatsache, das die sich bewegende Station recht schnell als direkter Nachbar erkannt wird.

Der Verlauf der Wahrscheinlichkeiten für Paketverluste auf Grund von Non-Wifi-Signalen unterscheidet sich im Vergleich zur nicht-kooperativen Simulation kaum.

4.5.2 In-Range zu Hidden-Node

Im Gegensatz zum vorherigen Szenario bewegt sich Station zwei von Station eins und zwei weg, sodass ein anfängliches In-Range-Szenario sich in ein Hidden-Node-Szenario wandelt.

Two-Ray-Ground-Reflection-Model, nicht-kooperativ

Für die Simulation mit dem Two-Ray-Ground-Reflection-Model wird Station eins auf den Koordinaten (0 15 0) platziert und Station zwei auf den Koordinaten (150 15 0). Station drei bekommt die Startkoordinaten (140 15 0) und bewegt sich nach 10 Sekunden mit einer Geschwindigkeit von 2 Metern pro Sekunde zu den Koordinaten (399 15 0).

Zu erwarten ist, dass die Wahrscheinlichkeiten für Paketverluste auf Grund von Hidden-Nodes bzw. In-Range-Kollisionen sich genau anders herum verhalten werden als im vorherigen Szenario. Es wird die Wahrscheinlichkeit für In-Range-Kollisionen leicht abnehmen, sobald Station drei die Empfangsreichweite von Station eins verlässt und die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes ansteigen. Dies wird vermutlich mit einer Steigerung der Wahrscheinlichkeit für Non-Wifi-Paketverluste einhergehen, sowie einem Anstieg der Wahrscheinlichkeit für Paketverluste auf Grund von Weak-Signal auf 100 Prozent für die Station drei.

Wie prognostiziert steigen die Wahrscheinlichkeiten für Paketverluste auf Grund von Hidden-Nodes und Non-Wifi-Signalen an, wobei letztere schon vor dem Erreichen der Grenze der Empfangsreichweite von Station eins leicht zu steigen anfängt, wie in Abbildung 4.37 deutlich zu sehen ist. Nach einiger Zeit bewegt sich Station drei auch aus dem Empfangsbereich von Station zwei heraus, was deutlich am Absinken der Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes zu erkennen ist. Die Wahrscheinlichkeit für Paketverluste auf Grund von Störungen durch Non-Wifi-Signale sinken ebenfalls wieder langsam ab.

Es wurden 25350 Pakete mit einer Wiederholungsrate von 21,28 % gesendet und es traten 274 Kollisionen auf. Im Vergleich zum vorherigen Szenario sind diese Werte höher, bedingt durch das langsame Entfernen aus den Empfangsbereichen.

Shadowing-Model, nicht-kooperativ

Für die Simulation mit dem Shadowing-Model bleibt Station eins auf den Koordinaten (0 15 0). Station zwei wird auf den Koordinaten (30 15 0) platziert und die Startkoordinaten von Station drei sind (30 30 0). Station drei bewegt sich nach 10 Sekunden zu den Zielkoordinaten (399 15 0).

Die Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes wird bei Erreichen der Empfangsreichweite von Station eins vermutlich weniger stark ansteigen als bei der Simulation mit dem Two-Ray-Ground-Reflection-Model. Der Verlauf der Wahrscheinlichkeit für Paketverluste verursacht durch In-Range-Kollisionen wird dem der Simulation mit dem Two-Ray-Ground-Reflection-Model stark ähneln.

Die Wahrscheinlichkeit für Paketverluste verursacht durch Non-Wifi-Signale wird, ausgehend vom vorhergehenden Szenario, weit ansteigen und mit zunehmender Entfernung der Station drei wieder langsam absinken.

In Abbildung 4.38 lässt sich der Anstieg und das folgende langsame Absinken der Paketverlustwahrscheinlichkeit auf Grund von Non-Wifi-Signalen gut erkennen.

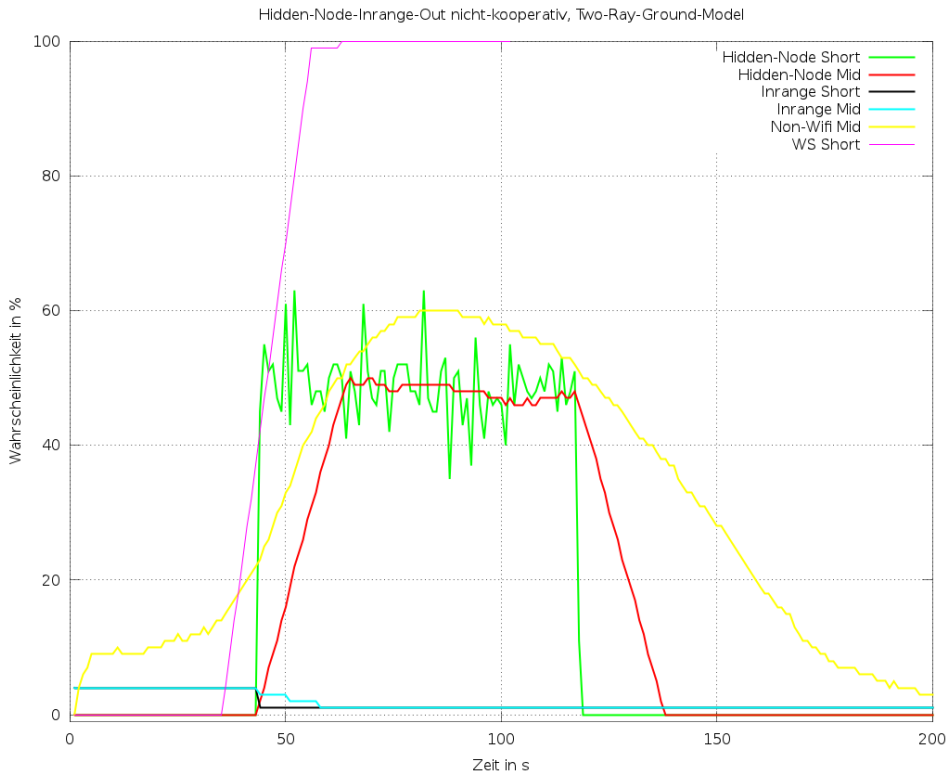

Abbildung 4.37: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, IR-HN, Two-Ray-Ground-Reflection-Model, nicht-kooperativ

Die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes steigt kaum merklich an, zeigt aber die gleichen Symptome, die in den Hidden-Szenarien mit dem Shadowing-Model beobachtet werden konnten. Die Paketverlustwahrscheinlichkeit für In-Range-Kollisionen verläuft wie vorhergesagt.

Die Wiederholungsrate ist im Gegensatz zur vorherigen Simulation mit 37,19 % höher, die Anzahl der Kollisionen hat bei 23070 gesendeten Paketen auf 83 abgenommen.

Shadowing-Model, kooperativ

Für die folgende Simulation wird die Kooperation dazugeschaltet und als Pfadverlustmodell wird weiter das Shadowing-Model verwendet. Durch die Kooperation der Stationen sollte die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes beim Verlassen des Empfangsbereiches von Station eins ansteigen. Die Verläufe der Paketverlustwahrscheinlichkeiten auf Grund von In-Range-Kollisionen und auf Grund von Non-Wifi-Signalen sollten sich im Vergleich zur Simulation ohne Kooperation nicht großartig unterscheiden.

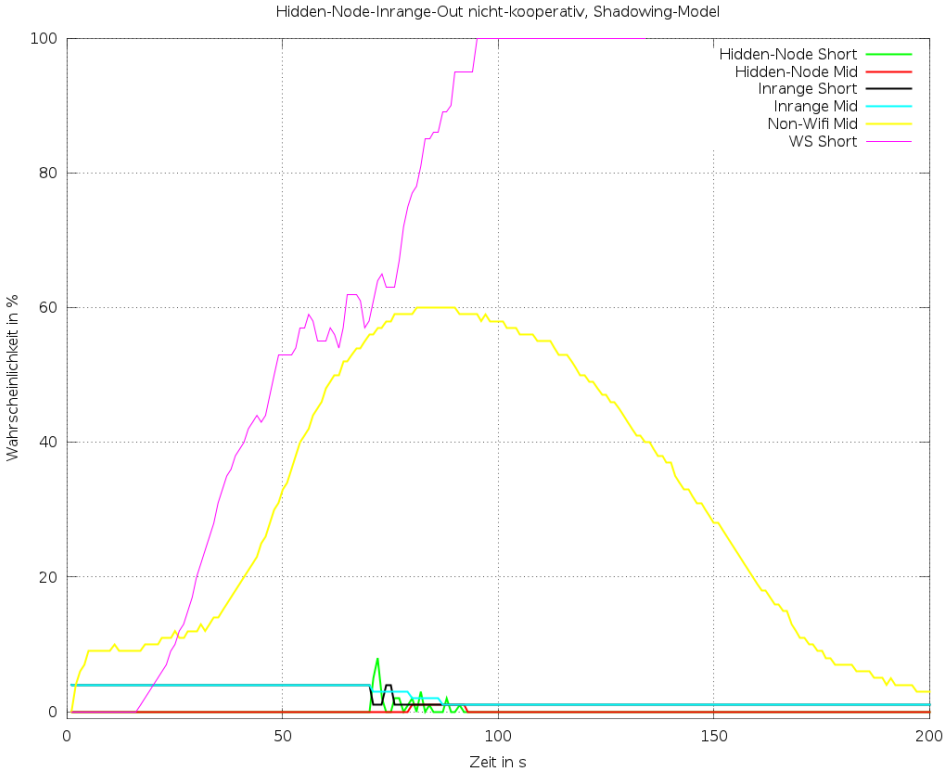

Abbildung 4.38: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, IR-HN, Shadowing-Model, nicht-kooperativ

In Abbildung 4.39 ist der Übergang vom direkten Nachbarn zum Hidden-Node der Station drei deutlich zu sehen. Der gleitende Durchschnitt der Werte über 20 Zyklen steigt auf 25 Prozent an.

Wie schon in den vorherigen kooperativen Simulationen ist die Anzahl der Kollisionen mit 234 bei 23418 gesendeten Paketen wieder höher, als bei der unkooperativen Simulation. Die Wiederholungsrate liegt mit 36,42 % nur geringfügig niedriger gegenüber der unkooperativen Simulation.

Wie erwartet sind die die Wahrscheinlichkeiten von Paketverlusten auf Grund von In-Range-Kollisionen sowie Non-Wifi-Signalen sehr ähnlich zur nicht-kooperativen Simulation.

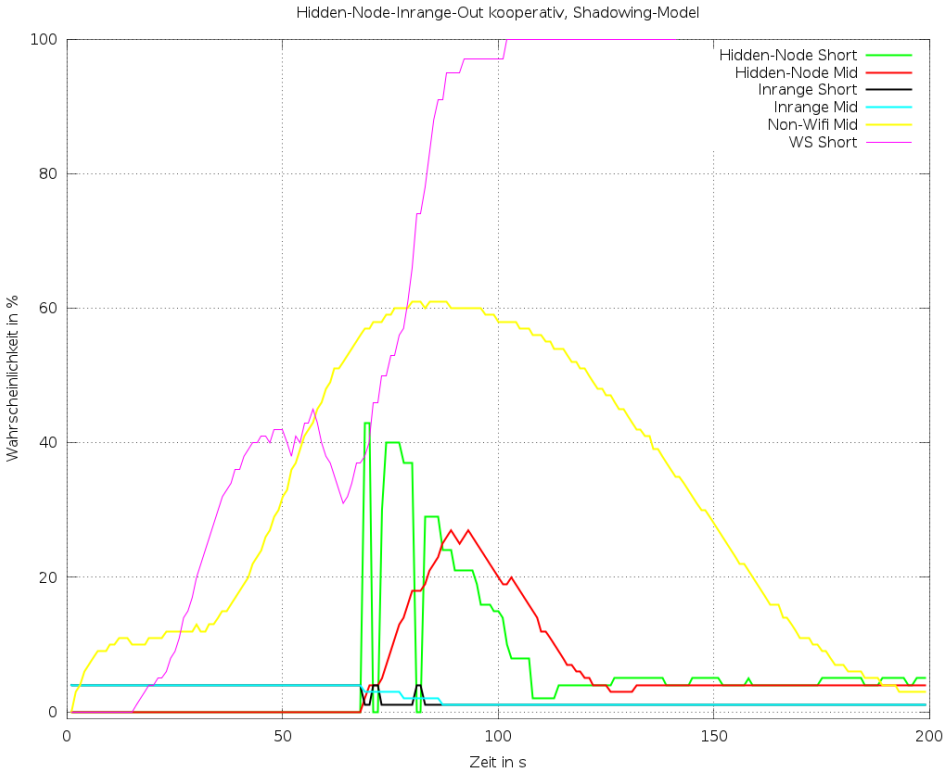

Abbildung 4.39: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, IR-HN, Shadowing-Model, kooperativ

4.5.3 Hidden-Node zu In-Range zu Hidden-Node

Dieses Szenario simuliert einen Transit einer Station durch den Empfangsbereich zweier weiterer Stationen. Dabei mutiert die sich bewegende Station von einem Hidden-Node zu einem direkten Nachbarn, um dann wieder zu einem Hidden-Node zu werden.

Two-Ray-Ground-Reflection-Model, nicht-kooperativ

Die erste Simulation wird mit dem Two-Ray-Ground-Reflection-Model durchgeführt dazu werden die Stationen eins und zwei auf den Koordinaten (0 255 0) und (50 255 0) platziert. Station drei wird auf die Startposition mit den Koordinaten (70 0 0) gesetzt und bewegt sich nach fünf Sekunden mit einer Geschwindigkeit von zwei pro Sekunde zur Position mit Koordinaten (70 449 0).

Am Anfang ist ein Anstieg der Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes zu erwarten, die, nachdem Station drei den Empfangsbereich von Station eins erreicht hat, dann auf null sinken wird und sobald Station drei den Empfangsbereich wieder verlässt wieder ansteigen wird. Die Wahrscheinlichkeit für Paketverluste auf Grund von In-Range-Kollisionen wird sich genau umgekehrt verhalten, sie wird erst ansteigen, wenn Station drei die Empfangsreichweite von Station eins erreicht und wieder fallen, sobald Station drei den Empfangsbereich wieder verlässt.

Abbildung 4.40 zeigt deutlich, wie zuerst die Wahrscheinlichkeit von Paketverlusten verursacht durch Non-Wifi-Signale zunimmt, um dann bei zunehmender Annäherung von Station drei an Station eins wieder abzunehmen. Nach der größten Annäherung beider Stationen steigt diese Paketverlustwahrscheinlichkeit wieder an.

Die Wahrscheinlichkeit von Paketverlusten verursacht durch Hidden-Nodes zeigt in Abbildung 4.40 zwei Spitzen, einmal zum Zeitpunkt an dem Station drei den Empfangsbereich von Station zwei erreicht und dann wieder nachdem Station drei den Empfangsbereich von Station eins verlassen hat.

Gut zu sehen ist auch der nicht sehr große Anstieg der Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen beim Erreichen des Empfangsbereichs von Station eins. Beim Verlassen des Bereichs sinkt die Wahrscheinlichkeit wieder auf das vorherige Niveau.

Die Wahrscheinlichkeit von Paketverlusten verursacht durch Weak-Signal für Station drei steigt, wie nicht anders erwartet erst kurz an, um dann bei größerer Annäherung an Station eins auf null zu sinken und später dann wieder auf 100 Prozent anzusteigen.

Es wurden 36398 Pakete empfangen, wobei die Wiederholungsrate bei 11,00 % lag und es 181 Kollisionen gab.

Shadowing-Model, nicht-kooperativ

Die Simulation mit dem Shadowing-Model kann ohne weitere Modifikation der Positionen der drei Stationen gestartet werden.

Im Gegensatz zur Simulation mit dem Two-Ray-Ground-Reflection-Model wird der Anstieg der Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes nur wenig steigen, wie auch schon in den Hidden-Node-Simulationen zu sehen war. (Siehe S. 58, 62 und 65)

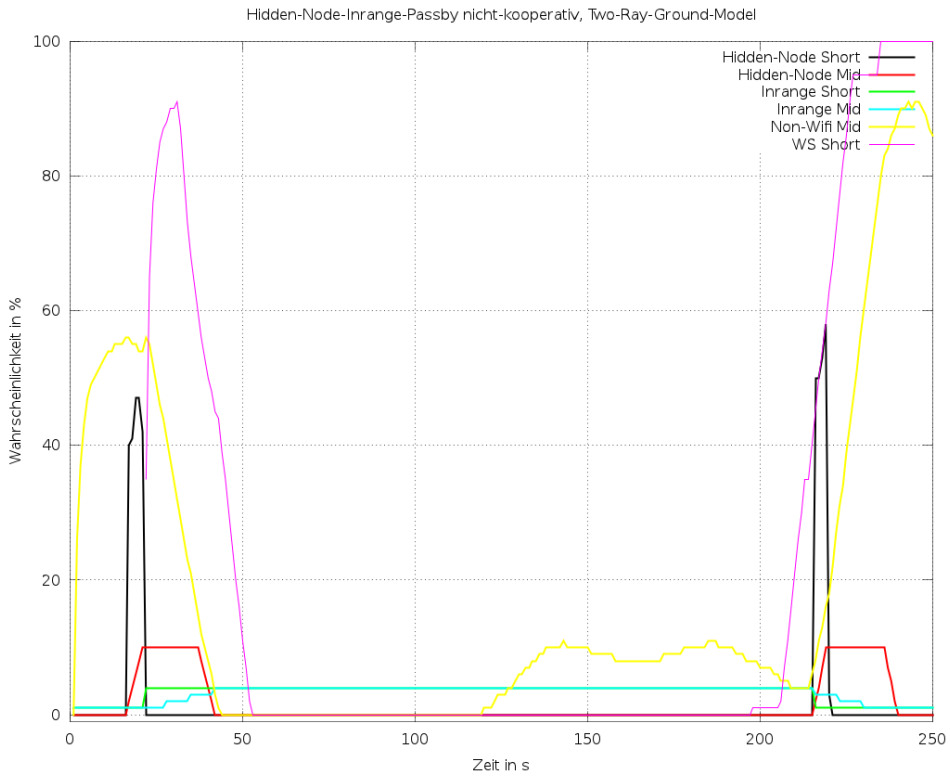

Abbildung 4.40: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR-HN, Two-Ray-Ground-Reflection-Model, nicht-kooperativ

Der Verlauf der Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen wird sich nicht wesentlich von der der vorherigen Simulation mit dem Two-Ray-Ground-Reflection-Model unterscheiden.

Wie vorhergesagt steigen die Werte für die Wahrscheinlichkeit von Paketverlusten verursacht durch Hidden-Nodes nur wenig an. Dies wird durch die in den Hidden-Node-Szenarien beschriebenen Ursachen ausgelöst. Der Verlauf der Paketverlustwahrscheinlichkeit auf Grund von In-Range-Kollisionen zeigt, wie prognostiziert, kaum Unterschiede zur Simulation mit dem Two-Ray-Ground-Reflection-Model.

Die Wahrscheinlichkeit von Paketverlusten auf Grund von Non-Wifi-Signalen entwickelt sich sehr ähnlich der der vorherigen Simulation. Einen Unterschied zur vorherigen Simulation gibt es im Verlauf der Paketverlustwahrscheinlichkeit auf Grund von Weak-Signal für Station drei. Nach dem Eintreten in den Empfangsbereich von Station eins steigt die Wahrscheinlichkeit auf über 80 Prozent, um dann während der Annäherungsphase bis auf über 40 Prozent zu sinken, wo sie dann während der größten Annäherung verharrt. Danach steigt die Wahrscheinlichkeit wieder langsam bis auf 100 Prozent.

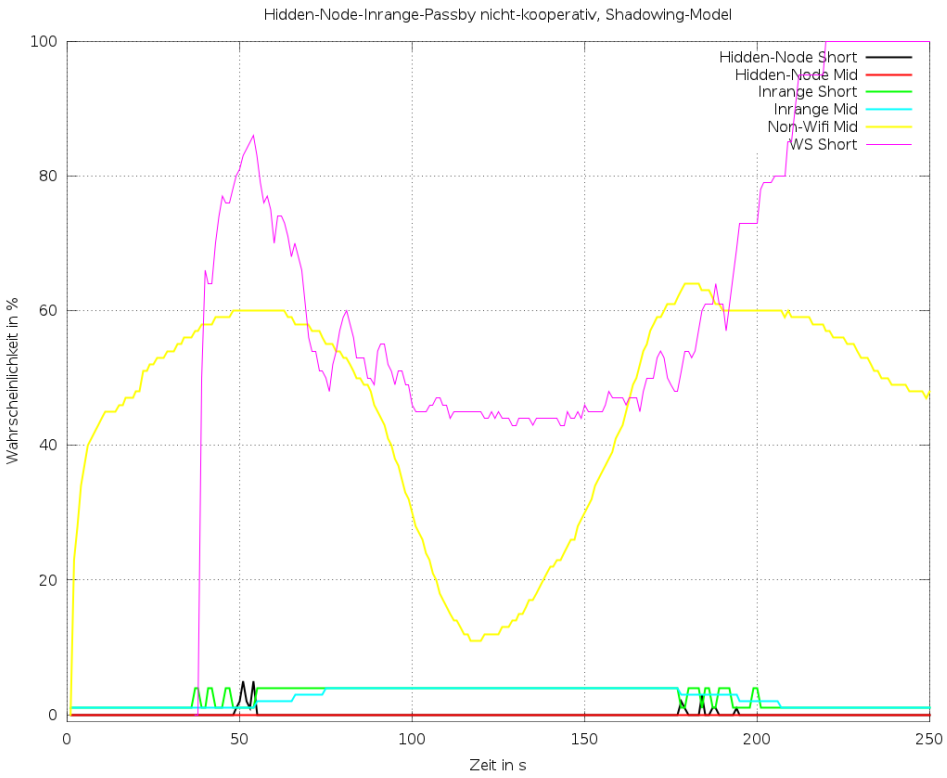

Abbildung 4.41: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR-HN, Shadowing-Model, nicht-kooperativ

Die Anzahl der Kollision liegt bei 27703 gesendeten Paketen bei 73 Kollisionen, was deutlich weniger als bei der Simulation mit dem Two-Ray-Ground-Reflection-Model ist. Die Wiederholungsrate ist dafür mit 34,54 % mehr als drei Mal so hoch.

Two-Ray-Ground-Reflection-Model, kooperativ

Die nächste Simulation nutzt wieder das Two-Ray-Ground-Reflection-Model, aber mit eingeschalteter Kooperation. Die Ergebnisse sollten sich im Vergleich zur Simulation mit dem Two-Ray-Ground-Reflection-Model ohne Kooperation nicht all zu groß unterscheiden, da die Simulation mit dem Two-Ray-Ground-Reflection-Model auch ohne Kooperation schon recht aussagekräftige Ergebnisse liefert.

Wie prognostiziert, unterscheiden sich die Verläufe der Wahrscheinlichkeiten für Paketverluste in allen Bereichen kaum, wie Abbildung 4.42 deutlich zeigt. Lediglich die schon bekannte Schwäche der Erkennung eines Hidden-Nodes beim Aufeinanderzubewegen der Stationen tritt erneut auf. Die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes steigt kurz an und fällt dann wieder

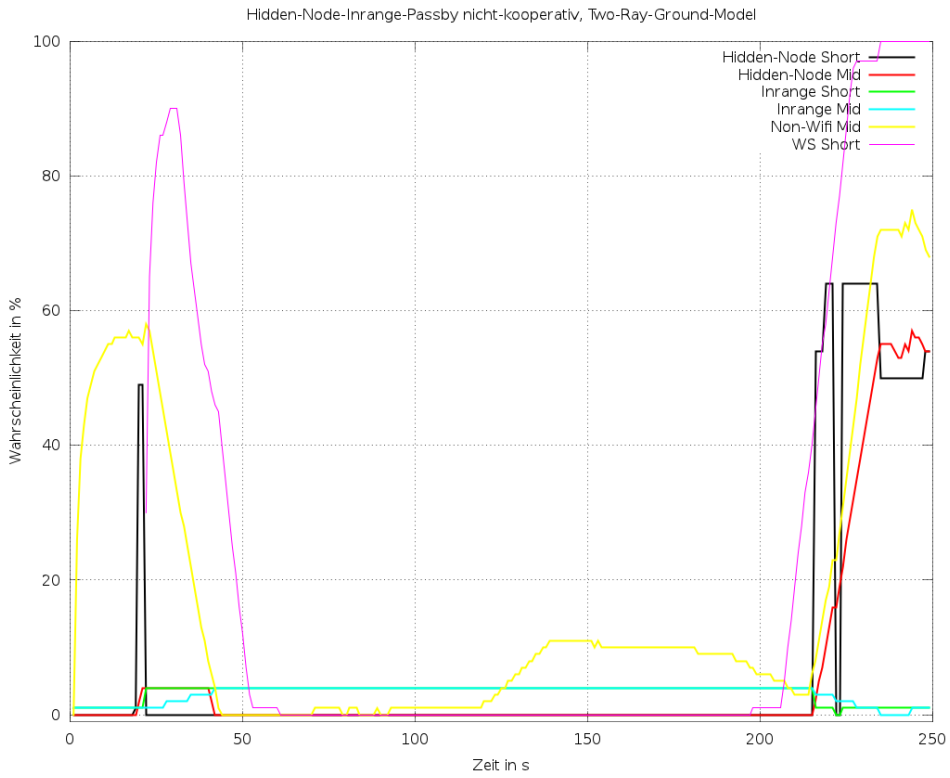

Abbildung 4.42: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR-HN, Two-Ray-Ground-Reflection-Model, kooperativ

auf null, wodurch der gleitende Durchschnitt über 20 Sekunden nicht einmal eine Wahrscheinlichkeit von 10 Prozent erreicht.

Dafür ist zum Ende der Anstieg der Paketverlustwahrscheinlichkeit auf Grund von Hidden-Nodes deutlich zu erkennen.

Verursacht durch die zusätzlichen Pakete der Kooperation zwischen den Stationen, ist die Kollisionsanzahl auf 612 bei 36742 gesendeten Paketen gestiegen. Die Wiederholungsrate liegt mit 10,46 % nur wenig niedriger, als bei der Simulation mit dem Two-Ray-Ground-Reflection-Model ohne Kooperation.

Shadowing-Model, kooperativ

Als letztes wird wieder das Shadowing-Model eingesetzt und dieses Mal die Kooperation eingeschaltet. Die Erkennung des Hidden-Node sollte im Vergleich zur Simulation mit dem Shadowing-Model ohne Kooperation, sobald Station drei den Empfangsbereich von Station eins verlässt, besser sein. Die Verläufe der anderen Wahrscheinlichkeiten sollten sich nur marginal unterscheiden.

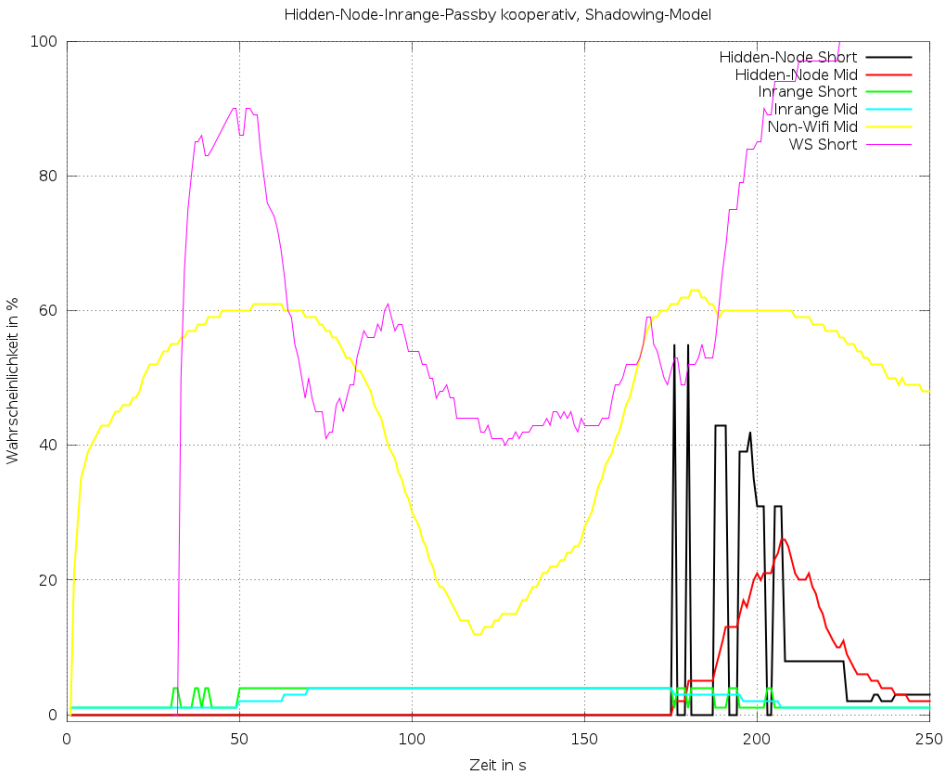

Abbildung 4.43: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR-HN, Shadowing-Model, kooperativ

Wie erwartet und wie auch schon in den vorherigen Simulationen zu erkennen war, zeigt Abbildung 4.43 deutlich, dass der Übergang vom Hidden-Node zum direkten Nachbarn nicht zu erkennen ist. Der umgekehrte Fall, der Übergang vom direkten Nachbarn zum Hidden-Node", ist dagegen wieder deutlich zu erkennen.

Die Verläufe der Paketverlustwahrscheinlichkeit verursacht durch In-Range-Kollisionen bzw. Non-Wifi-Signale gleichen weitgehend der Simulation mit dem Shadowing-Model ohne Kooperation.

Bei 28184 gesendeten Paketen traten 239 Kollisionen auf, was wieder auf die zusätzlichen Kooperationspakete zurückzuführen ist. Die RetryRate ist mit 33,55 % nur unbedeutend niedriger, im Vergleich zur nicht-kooperativen Simulation.

4.5.4 Auswertung

Die dynamischen Simulationen zeigen, dass sich mit dem Two-Ray-Ground-Reflection-Model die Ursachen für Paketverluste abschätzen lassen. Mit dem Shadowing-Model wird die Erkennung von Hidden-Nodes erschwert, da Hidden-Nodes Störungen verursachen, die die Pakete, welche Rückschlüsse

auf die Hidden-Nodes zulassen, durch Interferenzen der Signale, beeinträchtigen. Das lässt sich aus den hohen Wahrscheinlichkeiten für Paketverluste verursacht durch Non-Wifi-Signale ablesen.

Wird die Kooperation eingeschaltet, verbessert sich die Erkennung bei den Simulationen mit dem Two-Ray-Ground-Reflection-Model nicht, bei den Simulationen mit dem Shadowing-Mode dagegen teilweise schon. Die Erkennung von Hidden-Nodes, die sich auf andere Stationen zu bewegen, ist sehr schlecht. Der Grund wird der recht kurze Zeitraum sein, in dem die Station ein Hidden-Node ist. Sobald die Station sich weit genug bewegt hat, wird sie schnell als direkter Nachbar erkannt.

4.6 Testbed

Um die Ergebnisse der Simulationen zu prüfen, werden einige Messungen im Testbed vorgenommen. Dazu werden reale WLAN-Stationen des Lehrstuhls verwendet und die Software automatisch darauf installiert und die Messungen gestartet. Dabei wird im 2,4 GHz-Band auf Kanal sieben gemessen.

4.6.1 Weak-Signal-Messung

Als erstes erfolgt die Messung an Hand der Datenübertragung zweier stationärer Stationen. Dabei wird alle 10 Sekunden die Sendestärke der Station zwei verringert. Nachdem die Sendestärke auf zwei gesunken ist, wird zehn Sekunden später die Sendestärke bis auf eins abgesenkt. Dadurch sollte ein Anstieg der Paketverlustwahrscheinlichkeit auf Grund von Weak-Signal zu sehen.

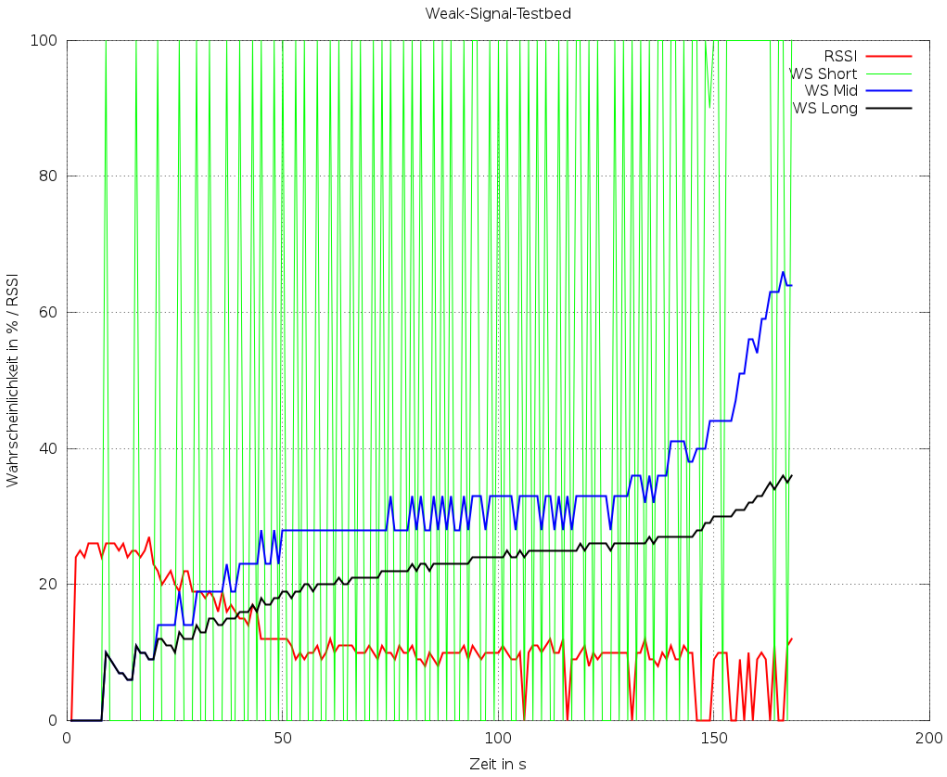

Abbildung 4.44: Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal im Testbed

Die Messung zeigt, dass der RSSI-Wert langsam auf Werte von zehn abfällt, wie in Abbildung 4.44 an der roten Linie zu erkennen ist. Später zeigen sich immer häufiger auftretende RSSI-Werte von null.

Die Wahrscheinlichkeit für Paketverluste auf Grund von Weak-Signal (in der Abbildung grün dargestellt) schwankt sehr stark zwischen Werten von null und 100 Prozent. Wird der gleitende Durchschnitt über 20 Sekunden betrachtet, steigt dieser von 10 Prozent auf Werte um die 30 Prozent und verharrt dort kurz um dann auf über 60 Prozent zu steigen.

4.6.2 In-Range-Messung

Als nächstes wird die Datenübertragung dreier benachbarter Stationen, die sich gegenseitig hören können, ausgewertet. Damit soll die In-Range-Erkennung getestet werden.

Da sich einige weitere Stationen in der Nähe der drei Stationen befinden, werden die Wahrscheinlichkeiten für Paketverluste auf Grund von In-Range-Kollisionen vermutlich höher ausfallen als bei drei Stationen erwartet.

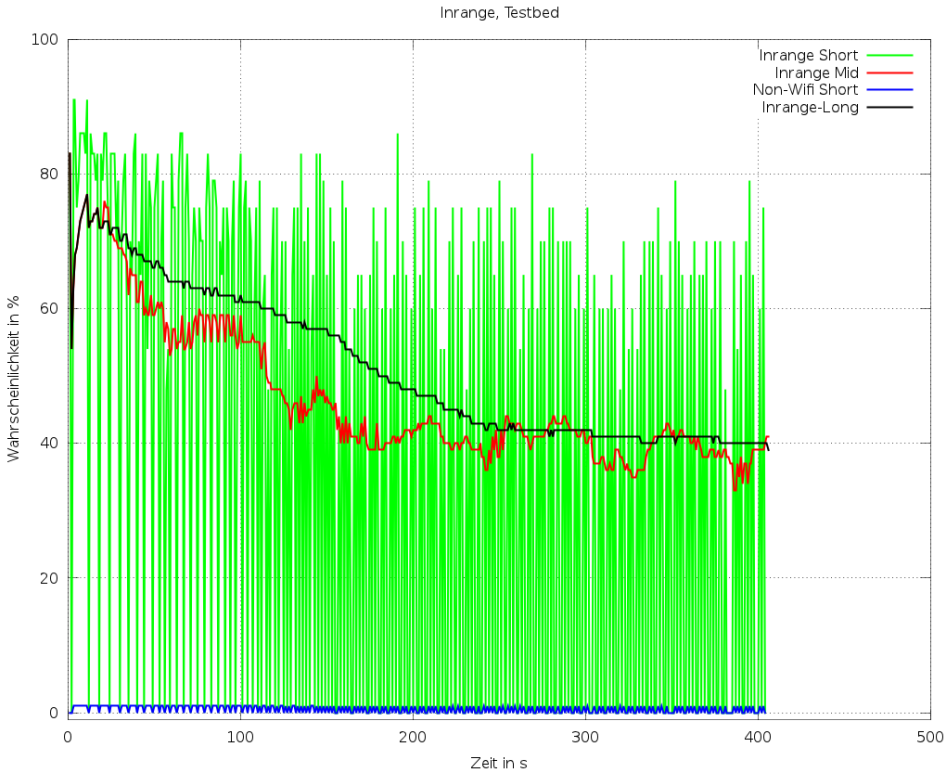

Abbildung 4.45: Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollisionen im Testbed

Die Abbildung 4.45 zeigt starke Schwankungen der In-Range-Kollisionswahrscheinlichkeit. Die Werte schwanken am Anfang zwischen null und 90 Prozent, später liegen die Maximalwerte bei knapp 80 Prozent. Die gleitenden Durchschnitte

über 20 Sekunden (in der Abbildung rot dargestellt) und über 200 Sekunden (in der Abbildung schwarz dargestellt) liegen am Anfang der Messung ungefähr 75 Prozent und fallen dann auf Werte um die 40 Prozent.

Die starken Schwankungen der In-Range-Kollisionswahrscheinlichkeit sind darauf zurückzuführen, dass einerseits innerhalb einer Messung keine Datenpakte von der beobachteten Station eingetroffen sind und somit keine Wahrscheinlichkeit angegeben werden konnte, andererseits die Anzahl der erkannten Nachbarstationen während einer Messung sehr niedrig war und dadurch die Wahrscheinlichkeit für In-Range-Kollisionen stark gesunken ist.

Dass immer wieder keine Datenpakete empfangen wurden, wird vermutlich an Kollisionen durch Interferenzen anderer Stationen liegen. Die schwankende Anzahl der erkannten Nachbarstationen liegt an der Häufigkeit, mit der diese Stationen Pakete senden. Werden von einer Station keine Pakete versendet, wird diese nicht als Nachbar erkannt und geht auch nicht in die Berechnung der In-Range-Kollisionswahrscheinlichkeit ein.

Vergleicht man die Messung mit den Simulationen, zeigt sich ein Bild wie bei den Simulationen von In-Range-Kollisionen von zehn bzw. 20 Nachbarn. Allerdings konnte der starke Anstieg der Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen nicht beobachtet werden. Das lässt eine recht geringe Anzahl von stattgefundenen Kollisionen vermuten.

4.6.3 Hidden-Node-Messungen

Als letztes werden Messungen von Hidden-Node-Szenarien durchgeführt. Dazu werden drei Stationen, ein Beobachter, dessen Nachbar und der Hidden-Node, der vom Beobachter nicht gesehen werden kann, aber von dessen Nachbarn, benötigt. Zuerst wird die Messung ohne Kooperation gestartet und danach mit eingeschalteter Kooperation.

Die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes sollte trotz vieler anderer Stationen im Testbed ansteigen. Außerdem sollte der Anstieg der Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen wie in den Simulationen zu sehen sein.

Nicht-kooperativ

Wie in Abbildung 4.46 zu sehen, steigt die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes nur gering auf Maximalwerte von 10 Prozent. Allerdings ist ein deutlicher Anstieg der Paketverlustwahrscheinlichkeit verursacht durch Non-Wifi-Signale zu erkennen. Der gleitende Durchschnitt über 20 Sekunden zeigt einen Anstieg auf Werte zwischen 30 und 40 Prozent.

Die Paketverlustwahrscheinlichkeit verursacht durch Hidden-Nodes sinkt dagegen im Verlauf der Messung. Da schon in der Simulation von Hidden-Nodes andere Störungen, wie In-Range-Kollisionen eine wichtige Rolle gespielt haben, können auch hier Interferenzen von Stationen, in der Nähe des Hidden-Nodes für das Absinken der Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes verantwortlich sein.

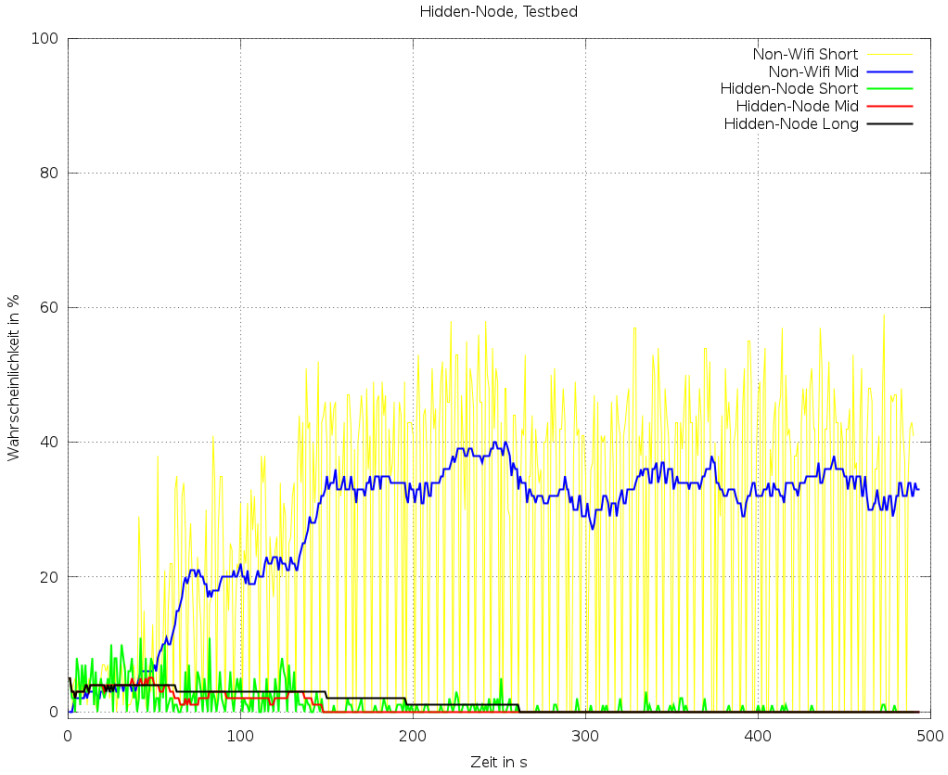

Abbildung 4.46: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes im Testbed, nicht-kooperativ

Kooperativ

Mit eingeschalteter Kooperation liegt die Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes etwas höher als ohne Kooperation, wie Abbildung 4.47 zeigt. Der gleitende Mittelwert über 20 Sekunden liegt am Anfang bei sieben Prozent und sinkt dann auf Werte von zwei Prozent. Nach einem kurzen Anstieg auf fünf Prozent sinkt der Wert dann dauerhaft auf ein Prozent ab. Der Anstieg der Paketverlustwahrscheinlichkeit verursacht durch Non-Wifi-Signale ist wie in der vorherigen Messung deutlich zu sehen. Auch bei dieser Messung steigt der gleitende Mittelwert über 20 Sekunden auf bis zu 40 Prozent Wahrscheinlichkeit.

4.6.4 Auswertung

Die Messungen im Testbed zeigen, dass die Ergebnisse der Simulationen ungefähr mit den Ergebnissen der Messungen übereinstimmen. Durch die vielen anderen WLAN-Stationen im Umfeld wurden die Messungen im Testbed allerdings beeinflusst. Hinzu kommt, dass die Messung von Non-Wifi-Einflüssen nicht ohne weiteres

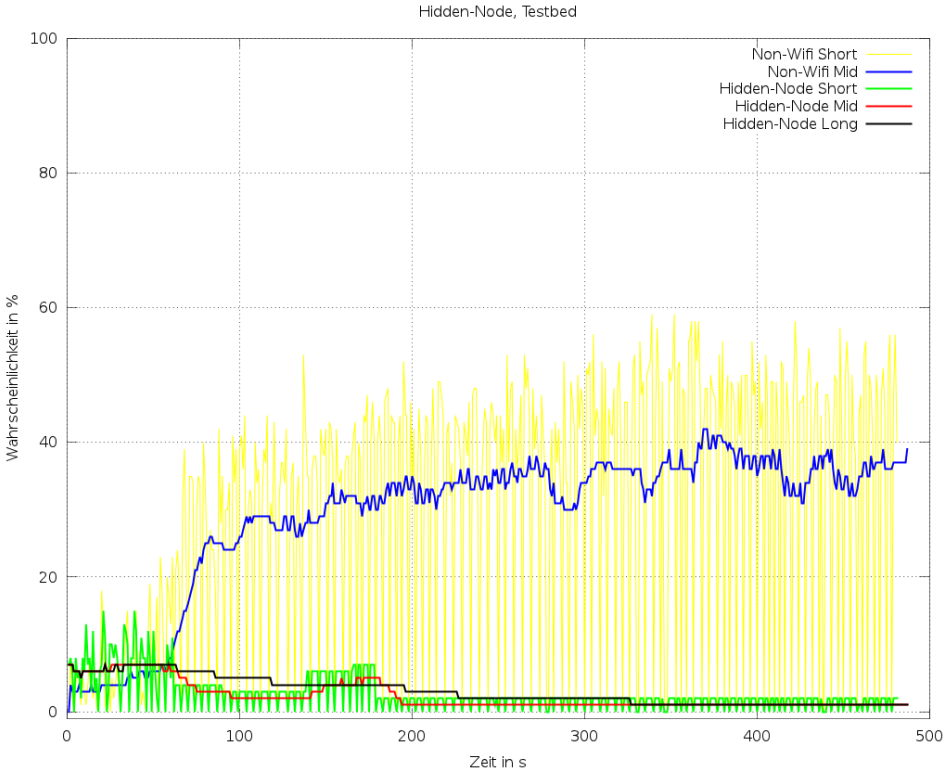

Abbildung 4.47: Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes im Testbed, kooperativ

simuliert werden kann, da Methode, die in der Simulation angewendet wurde, nicht auf die Messungen übertragen werden können.

Wie die Messungen im Testbed zeigen, lassen sich Paketverluste auf Grund zu schwacher Signale gut erkennen. Die Erkennung von Paketverlusten auf Grund von In-Range-Kollisionen scheint zu funktionieren, durch die Einflüsse der vielen anderen Stationen ist die Messung allerdings nicht sehr aussagekräftig.

Die Erkennung von Paketverlusten verursacht durch Hidden-Nodes ist dagegen bei den Messungen im Testbed mit und ohne Kooperation weniger deutlich.

5 Zusammenfassung

Es sollte untersucht werden, inwieweit es möglich ist, Ursachen für Paketverluste in 802.11-Netzwerken zu erkennen und zu klassifizieren. Aus den gewonnenen Daten sollte dann versucht werden, eine Prognose der Ursachen zukünftiger Paketverluste zu erstellen.

Dazu wurden mehrere Elemente im Click-Framework implementiert, um die empfangenen Pakete untersuchen und Wahrscheinlichkeiten für Paketverluste anhand der ermittelten Daten aus den empfangenen Paketen abschätzen zu können.

Im Rahmen des Click-Frameworks wurden dann Szenarien zum Testen der erstellten Elemente entworfen und mit Hilfe des Network-Simulator-2 (NS2) simuliert. Um die Ergebnisse der Simulationen zu verifizieren, wurden zusätzlich Szenarien für Messungen im Testbed des Lehrstuhls entwickelt und getestet.

Die Daten der Simulationen und Messungen im Testbed wurden später mit Octave ausgewertet und Abbildungen zur besseren Veranschaulichung erstellt.

5.1 Ergebnisse

Grundsätzlich ist es möglich, Ursachen für Paketverluste zu erkennen und zu unterscheiden.

Die Ursache Weak-Signal ist anhand des RSSI-Wertes zu ermittelten. Die Erkennung wird allerdings durch die herstellerabhängigen Implementierungen und die damit verbundenen unterschiedlichen Wertebereiche erschwert. Auch ist die Abstufung der RSSI-Werte recht grob. Die Auswertung der Simulationen hat aber ergeben, dass die geschätzte Wahrscheinlichkeit für Paketverluste auf Grund von zu schwachen Signalen mit der Anzahl der tatsächlichen Paketverluste gut korreliert. Die Messungen im Testbed zeigen, dass die Erkennung von Weak-Signal als Ursache für Paketverluste funktioniert.

In-Range-Kollisionen lassen sich recht einfach abschätzen, indem die Anzahl der vorhandenen Nachbarn und der aktuelle Backoff-Wert genutzt werden. Wie sich aber herausgestellt hat, ist die verwendete Berechnung sehr pessimistisch und es kommt zu höheren Paketverlustwahrscheinlichkeiten als die tatsächliche Anzahl der Kollisionen und die Anzahl der Neuübertragungen zeigt.

Es hat sich in den Simulationen herausgestellt, dass eine erhöhte Wahrscheinlichkeit für Paketverluste auf Grund von In-Range-Kollisionen mit einer erhöhten Wahrscheinlichkeit für Paketverluste auf Grund von Non-Wifi-Signalen einhergeht. Diese Beobachtung ist dadurch zu erklären, dass durch die In-Range-Kollisionen Signale der kollidierten Pakete empfangen werden, die aber nicht mehr dekodiert werden können. Diese Beobachtung konnte in den Messungen im Testbed nicht gemacht werden.

Die Erkennung von Paketverlusten verursacht durch Hidden-Nodes hat sich als recht schwierig herausgestellt. Die passive Analyse der empfangenen Daten ist sehr ungenau, da die Zuordnung der erkannten Hidden-Nodes zu den betroffenen Nachbarstationen nicht eindeutig ist. Es lässt sich allein durch passive Analyse nicht genau feststellen, welche Stationen vom Hidden-Node-Problem betroffen sind.

Zusätzlich ist es schwer, den tatsächlichen Datenverkehr und die Datenrate, die für eine Berechnung der Wahrscheinlichkeit von Vorteil wäre, abzuschätzen. Kooperieren die Nachbarstationen dagegen und tauschen Informationen über ihre Nachbarn und die Menge der übertragenen Daten aus, wird die Abschätzung der Wahrscheinlichkeit für Paketverluste auf Grund von Hidden-Nodes genauer.

Allerdings leidet die Abschätzung der Wahrscheinlichkeit, sobald mehrere Hidden-Nodes in einer Region auftreten, da es zwischen den Hidden-Nodes zusätzlich zu In-Range-Kollisionen kommt, was die Berechnung der Auslastung des Kanals negativ beeinflusst.

Auch wurde im Zusammenhang mit Hidden-Nodes eine erhöhte Wahrscheinlichkeit von Paketverlusten auf Grund von Non-Wifi-Signalen festgestellt. Zu erklären ist dieses Phänomen durch den Unterschied zwischen der maximalen Distanz, in der noch Pakete dekodiert werden können und der Distanz in der die Daten selbst nicht mehr dekodiert werden können aber ein Störeinfluss der Sendenden noch gegeben ist. Diese Beobachtung ließ sich durch die Messungen im Testbed bestätigen.

Die Erkennung von Non-Wifi-Signalen hat sich als sehr ungenau herausgestellt. Durch die geringe zeitliche Auflösung lassen sich keine Muster in den Störungen entdecken. So können periodische kurze Störungen nicht von andauernden Störungen unterschieden werden. Störungen durch Bluetooth-Geräte von Störungen durch Mikrowellenherde unterscheiden zu können, erfordert weiteren Aufwand.

Es hat sich weiterhin herausgestellt, dass die spektrale Auflösung ungeeignet ist, um zwischen schmal- und breitbandigen Störungen zu unterscheiden, da immer nur Störungen auf einem Kanal bemerkt werden, deren Bandbreite sich nicht abschätzen lässt. Für genauere Ergebnisse müsste es möglich sein, schnell auf die benachbarten Kanäle umschalten zu können. Dies ist aber nicht praktikabel.

Die Verwendung eines gleitenden Durchschnitts ist bei den Simulationen mit dem Shadowing-Model als Modell der Funkwellenausbreitung und bei den Messungen notwendig, da die einzelnen Wahrscheinlichkeitswerte unter Umständen stark schwanken können. Dadurch lassen sich interpretierbare Werte bei einigen Simulationen und Messungen erst mit Hilfe eines gleitenden Durchschnitts über 20 Sekunden erreichen. Der gleitende Durchschnitt über 200 Sekunden hat sich weniger geeignet, da Änderungen der zu Grunde liegenden Werte sehr langsam zu sehen sind.

5.2 Ausblick

Es hat sich gezeigt, dass es durchaus möglich ist, Paketfehlerursachen zu erkennen. Wenn diese Informationen zur gezielteren Anwendung der verschiedenen Strategien zur Vermeidung von Paketverlusten genutzt werden würden, ließe sich der Durchsatz für alle beteiligten Station durch die Vermeidung von Neuübertragungen erhöhen. Es wäre wünschenswert das Funkspektrum genauer untersuchen zu können, um bessere Vorhersagen zu ermöglichen.

Der Ansatz der Kooperation hat sich bewährt. Durch den Austausch weiterer Daten ließe sich die WLAN-Umgebung besser untersuchen und Paketverlustursachen besser und genauer lokalisieren. Beispielsweise ließe sich durch die Auswertung der RSSI-Werte des Empfängers durch den Sender die Anpassung der Sendeleistung und der Kodierung auf Senderseite eventuell verbessern. Auch könnten Non-Wifi-Störquellen wie Mikrowellenherde oder Babyphone besser lokalisiert werden und so das Routing in Multihop-Netzwerken beeinflusst und störanfällige Links zwischen Stationen umgangen werden.

Mit zusätzlichen Radios könnte man eventuell das Spektrum absuchen oder mit Hilfe der Software-Radios weitere Daten sammeln. Damit ließen sich eventuell auch Non-Wifi-Muster erkennen und so die Erkennung von speziellen Geräten bewerkstelligen.

In der Arbeit wurden auch nicht alle Ursachen für Paketverluste untersucht. Beispielsweise ließen sich möglicherweise mit Software-Radios auch Nachbarkanalstörungen erkennen.

Auch könnten Untersuchungen zu den eingesetzten gleitenden Mittelwerten ermitteln ob eventuell andere gleitende Mittelwerte besser geeignet sind, die geschätzten Wahrscheinlichkeiten zu interpretieren.

Abkürzungsverzeichnis

BPSK **B**inary **P**hase **S**hift **K**eying 13

CDMA **C**ode **D**ivision **M**ultiple **A**ccess 6

CSMA **C**arrier **S**ense **M**ultiple **A**ccess 6

CSMA/CR **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **R**esolution 7

CSMA/CD **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection 7

CSMA/CA **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance 1

CTS **C**lear **t**o **S**end 16

DCF **D**istributed **C**oordination **F**unction 6

DSSS **D**irect **S**equence **S**pread **S**pectrum 5

EDCA **E**nhanced **D**istributed **C**hannel **A**ccess 14

FDMA **F**requency **D**ivision **M**ultiple **A**ccess 6

FHSS **F**requency **H**opping **S**pread **S**pectrum 5

LLC **L**ogical **L**ink **C**ontrol 5

IEEE **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers 1

IR **I**nfra**r**otbereich 5

ISM **I**ndustrial, **S**cientific and **M**edical 5

MAC **M**edium **A**ccess **C**ontrol 5

MPDU MAC **P**rotocol **D**ata **U**nit 10

MTU **M**aximum **T**ransfer **U**nit 11

OFDM **O**rthogonal **F**requency **D**ivision **M**ultiplexing 5

PCF **P**oint **C**oordination **F**unction 6

PHY **phy**sische Schicht 9

PLCP **P**hysical **L**ayer **C**onvergence **P**rocedure 9

PSDU **P**LCP **S**ervice **D**ata **U**nit 9

QAM **Q**uadrature **A**mplitude **M**odulation 13

RSSI **R**eceived **S**ignal **S**trength **I**ndication 12

RTS **R**eady **t**o **S**end 16

SFD **S**tart **F**rame **D**elimiter 9

SNR **S**ignal to **N**oise **R**atio 12

SNIR **S**ignal to **N**oise plus **I**nterference **R**atio 12

TDMA **T**ime **D**ivision **M**ultiple **A**ccess 6

WLAN **W**ireless **L**ocal **A**rea **N**etwork 1

Literaturverzeichnis

[AA07] Akl, Robert ; Arepally, Anurag: Dynamic Channel Assignment in IEEE 802.11 Networks. In: *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on* IEEE, 2007. – ISBN 1–4244–1039–8, S. 1–5

[ABB+04] Aguayo, Daniel ; Bicket, John ; Biswas, Sanjit ; Judd, Glenn ; Morris, Robert: Link-level measurements from an 802.11b mesh network. 34 (2004), aug, 121-132. http://dx.doi.org/http://doi.acm.org/10.1145/1030194.1015482. – DOI http://doi.acm.org/10.1145/1030194.1015482. – ISSN 0146–4833

[Abr70] Abramson, Norman: THE ALOHA SYSTEM: another alternative for computer communications. In: *Proceedings of the November 17-19, 1970, fall joint computer conference* ACM, 1970, S. 281–285

[AMM+99] Akyildiz, I.F. ; McNair, J. ; Martorell, L.C. ; Puigjaner, R. ; Yesha, Y.: Medium access control protocols for multimedia traffic in wireless networks. In: *IEEE Network Magazine* 13 (1999), Nr. 4, S. 39–47

[Bar02] Bardwell, J.: Converting Signal Strength Percentage to dBm Values. (2002)

[Bor12] Borchers, Detlef ; Borchers, Detlef (Hrsg.): *Grünes Licht für freies WLAN in Potsdam.* http://heise.de/-1764564. Version: Dezember 2012, Abruf: 2012.12.12

[D'A12] D'Ambrosia, John ; D'Ambrosia, John (Hrsg.): *IEEE 802 Working groups and Executive Committee Study Groups.* http://www.ieee802.org/dots.shtml. Version: 2012, Abruf: 19.10.2012 10:31

[DGP07] Domenico Giustiniano, Douglas J. L. David Malone M. David Malone ; Papagiannaki, Konstantina: Estimating Link Quality in 802.11 WLANs. (2007)

[G+04] Group, IEEE 802.11 W. u. a.: *IEEE Standard for Information Technology—Telecommunications and information exchange between systems—LANs and MANs—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 7: 4.9 GHz–5 GHz Operation in Japan.* 2004

[G+05] Group u. a.: *IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs).* 2005

[G+07] Group, IEEE 802.11 W. u. a.: *IEEE Standard for Information Technology—Telecommunications and information exchange between systems—LANs and MANs—Specific requirements—Part 11: IEEE 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* 2007

[G+09] Group, IEEE 802.11 W. u. a.: *IEEE Standard for Information Technology—Telecommunications and information exchange between systems—LANs and MANs—Specific requirements—Part 11: WLAN MAC and PHY Specifications—Amendment 5: Enhancements for Higher Throughput.* 2009

[Gas05] Gast, Matthew: *802.11 Wireless Networks: The Definitive Guide.* Second Edition. O'Reilly, 2005. – 656 S. – ISBN 0–596–10052–3

[GPK09] Gollakota, Shyamnath ; Perli, Samuel D. ; Katabi., Dina: Interference alignment and cancellation. In: *ACM SIGCOMM Computer Communication Review* Bd. 39 ACM, Association for Computing Machinery (ACM), 2009, 159-170

[GSCR08] Gokhale, Dattatraya ; Sen, Sayandeep ; Chebrolu, Kameswari ; Raman, Bhaskaran: On the Feasibility of the Link Abstraction in (Rural) Mesh Networks. In: *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE* IEEE, 2008. – ISBN 978–1–4244–2026–1 978–1–4244–2025–4, S. 61–65

[GWGS07] Gummadi, Ramakrishna ; Wetherall, David ; Greenstein, Ben ; Seshan, Srinivasan: Understanding and mitigating the impact of RF interference on 802.11 networks. In: *Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, 2007 (SIGCOMM '07). – ISBN 978–1–59593–713–1, 385–396

[HAAW07] Halperin, Daniel ; Ammer, Josephine ; Anderson, Thomas ; Wetherall, David: Interference cancellation: Better receivers for a new wireless MAC. In: *The 6th Workshop on Hot Topics in Networks (HotNets VI)*, 2007

[HMS10] Huehn, Thomas ; Merz, Ruben ; Sengul, Cigdem: Joint Transmission Rate, Power, and Carrier Sense Settings: An Initial Measurement Study. In: *Wireless Mesh Networks (WIMESH 2010), 2010 Fifth IEEE Workshop on* IEEE, 2010. – ISBN 978–1–4244–7977–1 978–1–4244–7975–7, S. 1–6

[Hor07] Hornsteiner, Matthias: Was ist Rauschen? (2007), 38-43. http://www.ukwtv.de/de/reflexion/aktuelle/r213/R213.pdf. – ISSN 0940–1067

[Ins11] Institute, Information S.: *The Network Simulator ns-2: Documentation.* http://www.isi.edu/nsnam/ns/ns-documentation.html. Version: 2011, Abruf: 04.12.2012 10:21

[Ins12] Institute, Information S.: *The Network Simulator - ns2.* http://www.isi.edu/nsnam/ns/. Version: 2012, Abruf: 04.12.2012 10:21

[JKLS10] Jeong, Jangkeun ; Kim, Hyuntai ; Lee, Sangtae ; Shin, Jitae: An Analysis of Hidden Node Problem in IEEE 802.11 Multihop Networks. In: *2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM)* IEEE, IEEE, 2010, S. 282–285

[KE97] Kamerman, Ad ; Erkoçevic, Nedim: Microwave Oven Interference on Wireless LANs Operating in the 2.4 GHz ISM Band. In: *Personal, Indoor and Mobile Radio Communications, 1997.'Waves of the Year 2000'. PIMRC'97., The 8th IEEE International Symposium* Bd. 3 IEEE, IEEE, 1997, S. 1221–1227

[KKJ98] Khurana, Sumit ; Kahol, Anurag ; Jayasumana, Anura P.: Effect of Hidden Terminals on the Performance of IEEE 802.11 MAC Protocol. In: *23rd Annual Conference on Local Computer Networks, 1998. LCN'98.* IEEE, IEEE, 1998, S. 12–20

[KMC+00] Kohler, Eddie ; Morris, Robert ; Chen, Benjie ; Jannotti, John ; Kaashoek, M. F.: The Click Modular Router Laboratory for Computer Science, MIT, 2000

[Koh00] Kohler, Eddie: *The Click Modular Router*, Diss., 2000

[Koh06] Kohler, Eddie: Click for Measurement UCLA Computer Science Department, 2006

[KR09] Kurth, Mathias ; Redlich, Jens-Peter: Carrier Sensing and Receiver Performance in Indoor IEEE 802.11b Mesh Networks. In: *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, ACM, 2009 (IWCMC '09). – ISBN 978–1–60558–569–7, 726–732

[KV08] Kovar, Petr ; Vít, Novontý: New Analytical Model of Distributed Coordination Function. In: *IJCSNS* 8 (2008), Nr. 12, S. 125–129

[LMT04] Lacage, Mathieu ; Manshaei, Hossein ; Turletti, Turletti: IEEE 802.11 rate adaptation: a practical approach. In: *Proceedings of the 7th ACM international symposium on modeling, analysis and simulation of wireless and mobile systems* ACM, 2004, S. 126–134

[MCA03] M. Cordeiro, Rishi T. Sachin Abhyankar d. Sachin Abhyankar A. Sachin Abhyankar ; Agrawal, Dharma P.: A Novel Architecture and Coexistence Method to Provide Global Access to/from Bluetooth WPANs by IEEE 802.11 WLANs. In: *Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International* IEEE, 2003, S. 23–30

[NZR08] Nachtigall, Jens ; Zubow, Anatolij ; Redlich, Jens-Peter: The impact of adjacent channel interference in multi-radio systems using ieee 802.11. In: *Wireless Communications and Mobile Computing Conference, 2008. IWCMC'08. International* IEEE, 2008. – ISBN 978–1–4244–2202–9 978–1–4244–2201–2, S. 874–881

[ONL12] ONLINE, ZEIT: *Das freie WLAN in Berlin startet als Flickenteppich*. `http://www.zeit.de/digital/internet/2012-10/wlan-berlin-kostenlos-2`. Version: Oktober 2012, Abruf: 04.12.2012 10:17

[RCS03] Ray, Saikat ; Carruthers, Jeffrey B. ; Starobinski, David: RTS/CTS-induced congestion in ad hoc wireless LANs. In: *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE* Bd. 3 IEEE, IEEE, 2003, S. 1516–1521

[RCS05] Ray, Saikat ; Carruthers, Jeffrey B. ; Starobinski, David: Evaluation of the Masked Node Problem in Ad Hoc Wireless LANs. 4 (2005), Nr. 5, S. 430–442

[Rec06] Rech, Jörg: *Wireless LANs, 802.11-WLAN-Technologie und praktische Umsetzung im Detail*. Heise Zeitschriften Verlag GmbH & Co. KG Hannover, 2006. – ISBN 3–936931–29–1

[RMA+08] Rayanchu, Shravan ; Mishra, Arunesh ; Agrawal, Dheeraj ; Saha, Sharad ; Banerjee, Suman: Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal. In: *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE* IEEE, 2008. – ISBN 978–1–4244–2026–1 978–1–4244–2025–4, S. 735–743

[RMR+06] Reis, Charles ; Mahajan, Ratul ; Rodrig, Maya ; Wetherall, David ; Zahorjan, John: Measurement-Based Models of Delivery and Interference in Static Wireless Networks. In: *ACM SIGCOMM Computer Communication Review* Bd. 36 ACM, 2006, S. 51–62

[RPB11] Rayanchu, Shravan ; Patro, Ashish ; Banerjee, Suman: Airshark: Detecting Non-WiFi RF Devices using Commodity WiFi Hardware. In: *Internet Measurement Conference (IMC)*, 2011, S. 2–4

[RSC05] Ray, Saikat ; Starobinski, David ; Carruthers, Jeffrey B.: Performance of wireless networks with hidden nodes: a queuing-theoretic analysis. 28 (2005), Nr. 10, S. 1179–1192. `http://dx.doi.org/doi:10.1016/j.comcom.2004.07.024`. – DOI doi:10.1016/j.comcom.2004.07.024

[Rö04] Rödel, Egmar: *Einführung in die Informations- und Kodierungstheorie : theoretische Grundlagen der Telekommunikation*. Shaker, Aachen, 2004. – 133 S.

[Sch06] Schwencke, Daniel: Click - ein modularer Router. 2006. – Forschungsbericht

[Tou01] Tourrilhes, Jean: Fragment Adaptive Reduction: Coping with various interferers in radio unlicensed bands. In: *Communications, 2001. ICC 2001. IEEE International Conference on* IEEE, 2001. – ISBN 0–7803–7097–1, S. 239–244

[TV05] Tse, David ; Viswanath, Pramod: *Fundamentals of wireless communication*. Cambridge Univ Press, 2005

[Wik12] Wikipedia: *Pfadverlust*. `http://de.wikipedia.org/wiki/Pfadverlust`. Version: 2012

[Wol12a] Wolff, Dipl.-Ing. (FH) C.: *Radar Basics - Nahfeld/Fernfeld von Antennen*. `http://www.radartutorial.eu/18.explanations/ex48.de.html`. Version: 2012. – cc-by-sa

[Wol12b] Wolff, Dipl.-Ing. (FH) C.: *Radar Basics - Rauschen in elektronischen Schaltungen*. `http://www.radartutorial.eu/18.explanations/ex08.de.html`. Version: 2012. – cc-by-sa

[WZZN06] Wu, Haitao ; Zhu, Fan ; Zhang, Qiang ; Niu, Zhisheng: Analysis of IEEE 802.11 DCF with hidden terminals. In: *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE* IEEE, 2006. – ISBN 1–4244–0357–X 1–4244–0356–1, S. 1–5

[XGB02] Xu, Kaixin ; Gerla, Mario ; Bae, Sang: How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks? In: *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE* Bd. 1 IEEE, 2002. – ISBN 0–7803–7632–3, S. 72–76

[ZS11] Zubow, Anatolij ; Sombrutzki, Robert: Adjacent Channel Interference in IEEE 802.11n / Humboldt University. 2011. – Forschungsbericht

[ZS12] Zubow, Anatolij ; Sombrutzki, Robert: A Low-cost MIMO Mesh Testbed based on 802.11 n. In: *2012 IEEE Wireless Communications and Networking Conference (WCNC)* IEEE, 2012, S. 3171–3176

Abbildungsverzeichnis

2.1 Token Ring, Urheber: alexander jesner, Quelle: http://upload.wikimedia.org/wikipedia/de/5/53/Tokenbus.png, Lizenz: Public Domain 6
2.2 wahlfreier Zugriff, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 7
2.3 Funknetzwerk, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 9
2.4 PPDU und MPDU für DSSS, Urheber: Mik81 Quelle: http://en.wikipedia.org/wiki/File:Pdu_and_sdu.svg, Lizenz: Public Domain 10
2.5 Interferenz zweier Sinuswellen, Urheber: Jkrieger, Quelle: http://upload.wikimedia.org/wikipedia/de/archive/5/54/20070305203157!21Interferenz_sinus.png, Lizenz: Public Domain 13
2.6 Hidden Node, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 15
2.7 Exposed Node, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 17
2.8 Nachbarkanalstörungen, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 18

3.1 Kollisionswahrscheinlichkeit für verschiedene Contention-Window-Werte, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 24
3.2 Kollisionen durch Hidden Nodes, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 25
3.3 Schmal- und breitbandige Störsignale, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 27
3.4 Baum zur Speicherung der Wahrscheinlichkeiten, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 28

4.1 Wahrscheinlichkeiten Weak-Signal-Auswertung stationär, Two-Ray-Ground-Reflection-Model, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 30
4.2 RSSI-Werte Weak-Signal-Auswertung stationär, Two-Ray-Ground-Reflection-Model, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 31
4.3 Wahrscheinlichkeiten u. RSSI-Werte Weak-Signal-Auswertung stationär, Shadowing-Model, Distanz 30 m, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 33

4.4 Wahrscheinlichkeiten u. RSSI-Werte Weak-Signal-Auswertung stationär, Shadowing-Model, Distanz 60 m, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 34
4.5 Wahrscheinlichkeiten u. RSSI-Werte Weak-Signal-Auswertung stationär, Shadowing-Model, Distanz 90 m, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 35
4.6 Wahrscheinlichkeiten u. RSSI-Werte Weak-Signal-Auswertung stationär, Shadowing-Model, Distanz 120 m, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 36
4.7 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Two-Ray-Ground-Reflection-Model, dynamisch-in, Geschw. 2 m/s, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 39
4.8 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Two-Ray-Ground-Reflection-Model, dynamisch-in, Geschw. 5 m/s, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 40
4.9 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Shadowing-Model, dynamisch-in, Geschw. 2 m/s, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 41
4.10 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Shadowing-Model, dynamisch-in, Geschw. 5 m/s, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 42
4.11 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Two-Ray-Ground-Reflection-Model, dynamisch-out, Geschw. 2 m/s, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 43
4.12 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Two-Ray-Ground-Reflection-Model, dynamisch-out, Geschw. 5 m/s, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 44
4.13 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Shadowing-Model, dynamisch-out, Geschw. 2 m/s, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 45
4.14 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal, Shadowing-Model, dynamisch-out, Geschw. 5 m/s, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 46
4.15 Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Two-Ray-Ground-Reflection-Model, 2 Nachbarn, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 49
4.16 Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 2 Nachbarn, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 50
4.17 Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 5 Nachbarn, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 51

4.18 Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 10 Nachbarn, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 . . 52
4.19 Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 20 Nachbarn, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 . . 53
4.20 Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Two-Ray-Ground-Reflection-Model, 2 bis 20 Nachbarn, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 54
4.21 Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollision, Shadowing-Model, 2 bis 20 Nachbarn, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 55
4.22 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 1 Hidden-Node, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 57
4.23 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 1 Hidden-Node, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 . . . 58
4.24 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 1 Hidden-Node, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 59
4.25 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 1 Hidden-Node, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 60
4.26 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 2 Hidden-Nodes, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 61
4.27 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 2 Hidden-Nodes, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 . . . 62
4.28 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 4 Hidden-Nodes, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 63
4.29 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 4 Hidden-Nodes, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 . . . 65
4.30 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Two-Ray-Ground-Reflection-Model, 4 Hidden-Nodes, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 66
4.31 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Node, Shadowing-Model, 4 Hidden-Nodes, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 67

4.32 Wahrscheinlichkeit von Paketverlusten auf Grund von Non-Wifi-Signalen, Two-Ray-Ground-Reflection-Model, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 . . 68
4.33 Wahrscheinlichkeit von Paketverlusten auf Grund von Non-Wifi-Signalen, Shadowing-Model, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 69
4.34 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR, Two-Ray-Ground-Reflection-Model, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 72
4.35 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR, Shadowing-Model, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 73
4.36 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR, Shadowing-Model, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 74
4.37 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, IR-HN, Two-Ray-Ground-Reflection-Model, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 76
4.38 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, IR-HN, Shadowing-Model, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 77
4.39 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, IR-HN, Shadowing-Model, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 78
4.40 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR-HN, Two-Ray-Ground-Reflection-Model, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 80
4.41 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR-HN, Shadowing-Model, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 81
4.42 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR-HN, Two-Ray-Ground-Reflection-Model, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 82
4.43 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes und In-Range-Kollisionen, HN-IR-HN, Shadowing-Model, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 83
4.44 Wahrscheinlichkeit von Paketverlusten auf Grund von Weak-Signal im Testbed, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 85

4.45 Wahrscheinlichkeit von Paketverlusten auf Grund von In-Range-Kollisionen im Testbed, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 86
4.46 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes im Testbed, nicht-kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 88
4.47 Wahrscheinlichkeit von Paketverlusten auf Grund von Hidden-Nodes im Testbed, kooperativ, Urheber: Michael Kühn, Quelle: eigenes Werk, Lizenz: CC BY-NC-SA 3.0 89

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 22. Januar 2013 .....

Statement of authorship

I declare that I completed this thesis on my own and that information which has been directly or indirectly taken from other sources has been noted as such. Neither this nor a similar work has been presented to an examination committee.

Berlin, January 22, 2013 .....