HOCHSCHULE
FÜR ANGEWANDTE
WISSENSCHAFTEN
MÜNCHEN

Hochschule München

Fakultät Elektrotechnik und Informationstechnik

Masterarbeit von Sebastian Bartsch

Vergleich spezifischer Übertragungscharakteristiken zwischen WLAN und UMTS

Specific Transmission Characteristics of WLAN in Comparison to UMTS

Bearbeitungsbeginn: 05.06.2014

Abgabetermin: 15.10.2014

lfd. Nr. gemäß Belegschein: 294

HOCHSCHULE
FÜR ANGEWANDTE
WISSENSCHAFTEN
MÜNCHEN

Hochschule München

Fakultät Elektrotechnik und Informationstechnik

Masterarbeit von Sebastian Bartsch

Vergleich spezifischer Übertragungscharakteristiken zwischen WLAN und UMTS

Specific Transmission Characteristics of WLAN in Comparison to UMTS

Bearbeitungsbeginn: 05.06.2014

Abgabetermin: 15.10.2014

Betreuer: Prof. Dr. Manfred Paul

lfd. Nr. gemäß Belegschein: 294

Hochschule München

Fakultät für Elektrotechnik und Informationstechnik

Erklärungen des Bearbeiters:

Name	Vorname

1) Ich erkläre hiermit, dass ich die vorliegende Masterarbeit selbständig verfasst und noch nicht anderweitig zu Prüfungszwecken vorgelegt habe.
Sämtliche benutzte Quellen und Hilfsmittel sind angegeben, wörtliche und sinngemäße Zitate sind als solche gekennzeichnet.

Ort, Datum	Unterschrift

2) Ich erkläre mein Einverständnis, dass die von mir erstellte Masterarbeit in die Bibliothek der Hochschule München eingestellt wird. Ich wurde darauf hingewiesen, dass die Hochschule in keiner Weise für die missbräuchliche Verwendung von Inhalten durch Dritte infolge der Lektüre der Arbeit haftet. Insbesondere ist mir bewusst, dass ich für die Anmeldung von Patenten, Warenzeichen oder Geschmacksmuster selbst verantwortlich bin und daraus resultierende Ansprüche selbst verfolgen muss.

Ort, Datum	Unterschrift

Kurzzusammenfassung

Diese Masterarbeit untersucht, inwiefern bereits bekanntes UMTS-Kanalverhalten auf WLAN übertragen werden kann. Als spezifische Vergleichsgrößen werden hierbei Eigenschaften auf IP-Ebene – speziell die Inter-Packet Time von UDP-Paketen am Empfänger, unter Verwendung einer zeitlich konstanten Quelle – genutzt. Neben einer ausführlichen Einarbeitung in die betreffenden Protokolle und Standards werden eigene Versuche konzipiert und umgesetzt. Diesbezüglich werden geeignete Funkstrecken – speziell zur Untersuchung der Einflüsse von Implementierung, Interferenzen und Fading – im Labor aufgebaut. Dabei kommen eigens entwickelte Programme – konkret eine echtzeitfähige Paketquelle sowie verschiedene Skripte zur statistischen Analyse – zum Einsatz. Zur anschließenden Ergebnisfindung wird der bisherige Forschungsstand bei UMTS aufgearbeitet und den in Theorie und Praxis gewonnenen Resultaten zur 802.11n-Kanalcharakteristik gegenübergestellt. Mit der Gesamtlaufzeit und der Deterministik des Verzögerungsverhaltens werden zwei konkrete Unterscheidungsmerkmale der Übertragungscharakteristiken von UMTS und WLAN identifiziert. Weiterhin werden kanalspezifische Charakterisierungsmöglichkeiten – auch unter der Bewertung aus QoS-Sicht – diskutiert. Abschließend wird ein Ausblick hinsichtlich des weiteren Nutzens der gewonnenen Erkenntnisse gegeben.

Abstract

This master thesis investigates WLAN characteristics (channel behavior) and compares them with known UMTS characteristics. The technical characteristics of the IP-protocol are used as specific comparison basis. For this particular case the inter-package time of UDP packages from a time-constant source is used. In addition to extensive familiarization and analysis of used standards and protocols, several measurement scenarios are designed and implemented. For this purpose an adequate 802.11n radio link is built up in the laboratory including the capability to simulate different fault scenarios. Focus of the investigation is to evaluate the implementation of the Wi-Fi radio-link and to analyze the results of interferences and fading. For generating measurement-results specific software is developed. This software provides an engine for real-time packages generation and various scripts for statical analysis. The current status of UMTS research is evaluated and compared with the analysis results of the performed measurements (theoretical as well as practical results). With dimension and deterministic behavior of the packet delay, two distinguishing features of the transmitting characteristics of UMTS and WLAN are identified. Thus, methods for characterization (channel behaviors) are discussed including the assessment of QoS results. Finally this thesis provides an outlook for further use of achieved results.

Danksagung

An dieser Stelle möchte ich mich bei allen Personen, die durch ihre Unterstützung zum Gelingen dieser Arbeit wesentlich beigetragen haben, herzlich bedanken. Mein persönlicher Dank gilt dabei insbesondere:

- Meinen Betreuern – *Prof. Dr. Michael Dippold*, *Prof. Dr. Thomas Michael* und *Prof. Dr. Manfred Paul* – sowie meiner Kollegin *Rafiaa Boujbel*, die mich bei meiner Forschung exzellent unterstützt und somit diese Arbeit erst ermöglicht haben.
- Dem Leibniz-Rechenzentrum – namentlich Herrn *Jochen Gebert* – für die unkomplizierte Leihgabe eines Access Points und der Zentrale IT der Hochschule München – hier in erster Linie Herrn *Peter Schmieja* – für die technische Hilfestellung.
- Meiner Familie – insbesondere meiner Frau *Tanja Bartsch* und meinem Vater *Udo Bartsch* für die mentale Unterstützung sowie für den sprachlichen beziehungsweise erfahrungstechnischen Beistand – und meinen Freunden *Korbinian Schechner*, *Christian Hofmann* und *Michael Eckstein* fürs qualifizierte Korrekturlesen.

Weiterhin gilt meine Dankbarkeit allen freien Entwicklern, ohne deren Software diese Arbeit so nicht möglich gewesen wäre. Besonders hervorheben möchte ich an dieser Stelle die Projekte *Debian GNU/Linux*, *Wireshark*, *R*, *LaTeX*, *LibreOffice* und *GIMP*. Mein spezielle Verbundenheit gilt diesbezüglich auch jedem Einzelnen, der zu *Wikipedia*, zur *Open Clip Art Library* und zu *Linux Mint* beigetragen hat und deren Leistungen mir viel bei der Ein- beziehungsweise Ausarbeitung geholfen haben.

„If I have seen further it is by standing on ye sholders of Giants.“ – Isaac Newton[1]

In diesem Sinne möchte auch ich meine Arbeit der Allgemeinheit zur Verfügung stellen. Siehe diesbezüglich die Anmerkungen zur Lizenz auf der letzten Seite dieses Dokuments.

[1] Aus einem Brief an Robert Hooke vom 5. Februar 1676,
nach *The correspondence of Isaac Newton* von H.W. Turnbull

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACK Acknowledgement *(Signal oder Paket zur Empfangsbestätigung von Daten)*
AP Access Point *(Basisstation bzw. Zugangspunkt zu einem WLAN-Netzwerk)*
ARQ Automatic Repeat reQuest *(automatische Wiederholungsanfrage)*
AWGN Additive White Gaussian Noise *(Kanalmodell mit gaußverteiltem Rauschen)*
BPSK Binary Phase Shift Keying *(Phasenmodulationsverfahren mit zwei Phasen)*
BSS Basic Service Set *(WLAN-Netz; bestehend aus mindestens einer STA und einem AP)*
CRC Cyclic Redundancy Check *(spezielles Verfahren zur Bestimmung einer Prüfsumme)*
CSMA/CA Carrier Sense Multiple Access/Collision Avoidance *(Kollisionsvermeidungsstrategie)*
CSV Comma-Separated Values *(Format zur Speicherung und zum Austausch von Daten)*
CW Contention Window *(Gültigkeitsbereich der Backoffzeit im WLAN-Konfliktfall)*
DCF Distributed Coordination Function *(verteilte WLAN-Koordinierungsfunktion)*
DIFS Distributed Coordination Function Interframe Spacing *(DCF-Paketabstand)*
EDCA Enhanced Distributed Channel Access *(verteilte Koordinierungsfunktion mit QoS)*
FCS Frame Check Sequence *(Zeichenfolge zur Fehlererkennung, meist CRC)*
FDD Frequency Division Duplex *(Frequenzmultiplexverfahren, z.B. bei UMTS)*
GPRS General Packet Radio Service *(Datenübertragungsdienst in GSM-Netzen)*
GSM Global System for Mobile Communications *(2nd-Generation Mobilfunkstandard)*
HCCA HCF Controlled Channel Access *(zentrale Koordinierungsfunktion mit QoS)*
HCF Hybrid Coordination Function *(QoS-erweiterte Koordinierungsfunktion)*
HMM Hidden Markov Model *(stochastisches Verfahren zur Zustandsmodellierung)*
HSDPA High Speed Downlink Packet Access *(verbesserte UMTS-Datenverfahren)*
IP Internet Protocol *(Netzwerkprotokoll zur Implementierung der Internetschicht)*
IPT Inter-Packet Time *(Zeitabstand zwischen zwei Paketen; hier als Messgröße verwendet)*
ISM-Band Industrial, Scientific and Medical Band *(lizenzfrei nutzbarer Frequenzbereich)*
LLC Logical Link Control *(Teil der Sicherungsschicht im erweiterten OSI-Referenzmodell)*
LTE Long Term Evolution *(4rd-Generation Mobilfunkstandard)*
MAC Media Access Control *(Teil der Sicherungsschicht im erweiterten OSI-Referenzmodell)*
MCS Modulation and Coding Scheme *(Tabelle zur Bestimmung der Datenrate)*
MIMO Multiple Input Multiple Output *(Nutzung mehrerer Sende- bzw. Empfangsantennen)*
NAV Network Allocation Vector *(Hilfsmittel zur virtuellen Trägerprüfung)*
OFDM Orthogonal Frequency-Division Multiplexing *(spezielles Frequenzmultiplexverfahren)*
OSI-Modell Open Systems Interconnection Model *(Schichtenmodell für Netzwerkprotokolle)*
PCF Point Coordination Function *(zentrale WLAN-Koordinierungsfunktion)*
PCIe PCI-Express *(Erweiterungsstandard für serielle Punkt-zu-Punkt-Verbindungen)*
PCI Peripheral Component Interconnect *(ursprünglicher, paralleler Bus-Standard)*
PHY Physical Layer *(Abkürzung der Bitübertragungsschicht im OSI-Referenzmodell)*
PLCP Physical Layer Convergence Procedure *(PHY-Sublayer zur WLAN-Framestruktur)*
PMD Physical Medium Dependent *(PHY-Sublayer zur WLAN-Signalerzeugung)*
QAM Quadrature Amplitude Modulation *(spezielles, kombiniertes Modulatiosverfahren)*
QoS Quality of Service *(Dienstgütebeschreibung für Kommunikationsdienste)*
QPSK Quadrature Phase-Shift Keying *(Phasenmodulationsverfahren mit vier Phasen)*
RIFS Reduced Interframe Spacing *(reduzierter DCF-Paketabstand)*
RLC Radio Link Control *(MAC-Sublayer zur UMTS-Verbindungssteuerung)*

RNC Radio Network Controller *(zentrales UMTS-Netzelement)*
RRC Radio Resource Control *(Signalisierungsprotokoll bei UMTS)*
RTS/CTS Request To Send/Clear To Send *(optionaler Mechanismus zur Kollisionsvermeidung)*
SIFS Short Interframe Spacing *(kurzer DCF-Paketabstand)*
SSID Service Set Identifier *(frei wählbarer Name eines Service Sets)*
STA Station *(Gerät, das sich mit einem WLAN-Netzwerk verbindet)*
TCP Transmission Control Protocol *(verbindungsorientiertes Netzwerkprotokoll)*
TDM Time Division Multiplexing *(Zeitmultiplexverfahren, z.B. bei DECT)*
TTI Transmission Time Interval *(Rahmen zur Datenübertragung bei UMTS)*
UDP User Datagram Protocol *(minimales, verbindungsloses Netzwerkprotokoll)*
UE User Equipment *(Benutzerendgerät im UMTS-Netzaufbau)*
UMTS Universal Mobile Telecommunications System *(3rd-Generation Mobilfunkstandard)*
USB Universal Serial Bus *(weit verbreitetes, serielles Bus-System)*
UTRAN UMTS Terrestrial Radio Access Network *(UMTS-Zugangsnetz)*
VoIP Voice over IP *(Telefonieren über IP-basierte Computernetzwerke)*
WCDMA Wideband Code Division Multiple Access *(Funkzugriffstechnik bei UMTS)*
WEP Wired Equivalent Privacy *(veraltete WLAN-Verschlüsselung)*
WLAN Wireless Local Area Network *(lokales Funknetz, meist aus der IEEE 802.11-Familie)*
WMM Wi-Fi Multimedia *(Mindeststandard für QoS-Unterstützung im WLAN)*
WPA Wi-Fi Protected Access *(neuere WLAN-Verschlüsselung)*

1 Einleitung

1.1 Hintergrund und Motivation

Mit dem Durchbruch des Internets haben sich IP-basierte Netzwerke zur Datenübertragung etabliert. Das Konzept der *Next Generation Networks* beschreibt hierbei den Umstieg von der traditionell leitungsvermittelten Telekommunikation – wie der klassischen Telefonie über Vermittlungsstellen – auf eine einheitlich paketvermittelte Netzinfrastruktur – wie beispielsweise die durch *Voice over IP* (*VoIP*) realisierte Sprachübertragung. Es umfasst dabei neben Kabelfernseh- und Telefonnetzen auch den Bereich des Mobilfunks.

2013 waren, der Bundesnetzagentur zufolge, schätzungsweise ein Fünftel der deutschen Festnetzanschlüsse[2] „Sprachzugänge über entbündelte und für VoIP genutzte DSL-Anschlüsse“, was einem Anstieg von ca. 22% gegenüber dem Vorjahr entspricht [Bun13, Seite 71]. Nach Ankündigungen der *Deutschen Telekom AG* soll die Umstellung auf „vollständig IP-basierte Angebote“ bereits 2016 abgeschlossen sein.[3] Das Internet ist somit als Technologie zum Informationsaustausch weiter auf dem Vormarsch.

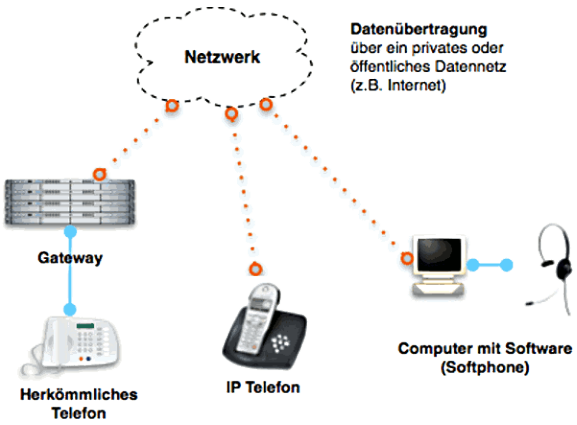


Abbildung 1.1: *Struktur eines VoIP-Netzwerks. Bildquelle: wikimedia.org (CC BY-SA* Bthorben*)*

Um diesen Siegeszug zu ermöglichen, spielt die Sicherung der Dienstgüte (engl. *Quality of Service*, kurz *QoS*) eine wichtige Rolle. Denn nur wenn der Telekommunikationsanbieter eine – im Vergleich zur alten, leitungsvermittelten Technik – konstant gute Übertragungsqualität erreichen und zusichern kann, sind die Kunden von der neuen Vermittlungstechnik zu überzeugen. Zur Gewährleistung dieser Ansprüche müssen die Netzbetreiber häufig – vor allem im Bereich des Mobilfunks – technisch aufwändige und somit teure Kontrollverfahren einsetzen. Beispielsweise dürfen Datenübertragungsvorgänge im Mobilfunk keinesfalls zu Gesprächsunterbrechung führen. Kommt es hier zu Problemen, können diese meist nur unter Einsatz von speziellen Funkmesswagen mit hochwertigem Testequipment aufgespürt und behoben werden.

[2] Ohne Berücksichtigung der providerinterne Vermittlungstechnik.

[3] Quelle: `http://heise.de/-1807580` (vom 21.02.2013, aufgerufen am 08.10.2014)

Durch die Verwendung des Internetprotokolls und der damit verbundenen Eigenschaften – wie der Netzwerktransparenz – lässt sich das Kanalverhalten auf Qualitätsmerkmale der höheren Ebenen abbilden. Dies ermöglicht unter anderem die Entwicklung eines kosteneffizienten und providerunabhängigen Messwerkzeugs zur klassifizierenden Beschreibung von Kanälen [Bar07, Seite 77 ff.]. Hierzu ist Know-How über die Zusammenhänge zwischen den Übertragungsverfahren und deren Auswirkungen auf die IP-basierte Kommunikation nötig.

Im *MobQoS*-Projekt[4] der *Hochschule München* wurde der Zusammenhang zwischen den Kanalcharakteristiken von UMTS-Verbindungen und entsprechenden IP-Parametern bereits genauer untersucht. Die Beschreibung der Wechselwirkung zwischen IP- und Kanalverhalten basiert hierbei auf dem sogenannten *Hidden Markov Model* (*HMM*), einem stochastischen Modell, das komplexere Systeme auf Markow-Ketten[5] abbildet. Als Ergebnis der 2013 abgeschlossenen Forschungen sind unter anderem die Implementierung eines Testwerkzeugs zur Kanalklassifizierung sowie die Emulation des UMTS-Kanalverhaltens auf IP-Ebene zu nennen (vgl. [Bar12, Bar11]). Das Nachfolgeprojekt *NetQoS* schließt hier an und soll eine solche Qualitätsanzeige auch für heterogene Netzwerke ermöglichen.

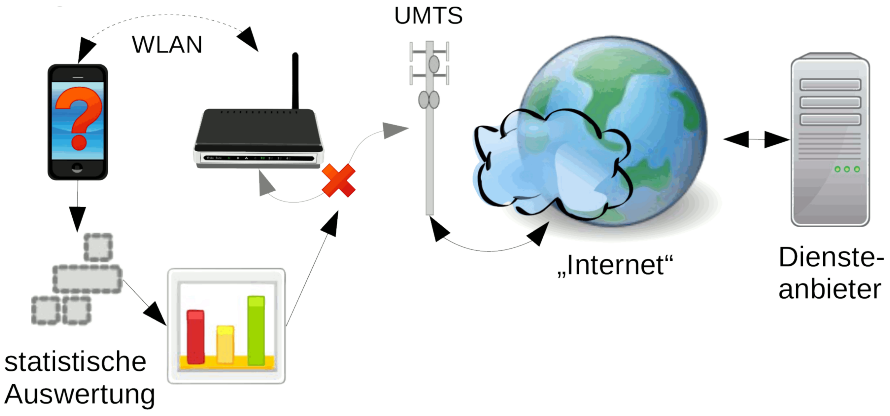


Abbildung 1.2: *Analyse von Netzwerkproblemen mithilfe statistischer Kommunikationsmodelle.*

Wie in Abb. 1.2 skizziert, sollen somit Übertragungsprobleme in komplexeren Infrastrukturen – als Beispiel sei die Betrachtung von Youtube-Videos auf einem Smartphone, das per WLAN über einen UMTS-Router mit dem Internet verbunden ist, genannt – erkannt und klassifiziert werden. Um die Heterogenität abbilden zu können, müssen natürlich weitere Kanäle, wie beispielsweise WLAN, untersucht werden. Hierfür ist es erforderlich, anfallende Paketinformationen statistisch auszuwerten und ein entsprechendes Kanalmodell zu erstellen.

[4] vgl. `http://ee.hm.edu/forschung/projekte/publikationdetail_326.de.html`

[5] Eine Markow-Kette ist ein spezieller stochastischer Prozess zur Beschreibung von Zustandsübergängen.

1.2 Ziel der Arbeit

Ziel der Arbeit ist es, die im Rahmen der bisherigen Forschung erlangten Erkenntnisse über die UMTS-Kanaleigenschaften um WLAN-spezifisches Wissen zu erweitern und die entsprechend erarbeiteten Übertragungscharakteristiken anschließend gegenüberzustellen. Hierbei stehen stochastische Erkenntnisse zu speziell übertragenen Paketen im Vordergrund.

Um einen wissenschaftlich fundierten Vergleich zwischen WLAN und UMTS zu ermöglichen, ist ein tieferes Verständnis beider Technologien erforderlich. Durch die Einarbeitung in die entsprechenden Netztopologien und die unterschiedlichen Übertragungstechniken sollen theoretische Unterschiede herausgearbeitet werden. Des Weiteren soll die Theorie der Praxis gegenübergestellt und somit der direkte Vergleich zwischen UMTS und WLAN durchgeführt werden. Hierzu müssen auch entsprechende Messszenarien entwickelt und umgesetzt werden. Dies soll schließlich spezifische Aussagen zum jeweiligen Kanalverhalten erlauben und somit einen entsprechenden Ausblick für die weitere Forschung ermöglichen.

1.3 Gliederung der Arbeit

Zunächst wird in Kapitel 2 auf die für diese Arbeit wichtigen Grundlagen eingegangen. Dies umfasst neben der Einführung in die verwendeten Netzwerkprotokolle auch ausführliche Informationen zu den Funkstandards UMTS und WLAN sowie für diese Arbeit interessante Eigenschaften der Funkübertragung und Fehlerbehandlung.

In Kapitel 3 erfolgt die Beschreibung des Messaufbaus. Diesbezüglich wird das zugrundeliegende Konzept sowie die konkrete Umsetzung der einzelnen Messungen vorgestellt. Anschließend wird auf die verwendeten Komponenten und Programme eingegangen. Hierbei werden gegebenenfalls auch kurz deren Implementierung sowie spezielle Eigenschaften erläutert. Weiterhin wird im Abschnitt 3.4 eine Messung exemplarisch nachvollzogen.

Kapitel 4 beschäftigt sich schließlich mit der Auswertung der durch die Messungen gewonnenen Ergebnisse. Hierfür werden die Beobachtungen aus den UMTS- und WLAN-Messungen getrennt voneinander vorgestellt, analysiert und anschließend miteinander verglichen. Neben der Bestätigung des theoretisch erarbeiteten Kanalverhaltens werden auch konkrete Unterscheidungsmerkmale zwischen WLAN und UMTS herausgearbeitet.

Zum Abschluss wird die Arbeit in Kapitel 5 hinsichtlich der erbrachten Leistung und der konkreten Ergebnisse zusammengefasst. Zusätzlich wird in Kapitel 6 noch ein projektspezifisches Fazit gezogen und ein Ausblick für weitere Forschungsansätze gegeben.

2 Grundlagen und Begriffserklärung

In diesem Kapitel werden die dieser Arbeit zugrundeliegenden Begrifflichkeiten ausführlich besprochen. Dies umfasst, neben einem kurzen Einstieg in das *Internet Protocol* (*IP*), in erster Linie die *WLAN*- und *UMTS*-Übertragungsstandards. Des Weiteren werden die der Funkübertragung eigenen Fehlerquellen und deren Auswirkungen kurz angesprochen.

2.1 Internetprotokollfamilie

Die Internetprotokollfamilie umfasst Netzwerkprotokolle verschiedener Abstraktionsschichten – wie zum Beispiel das bekannte und im Internet weit verbreitete TCP/IP. Da die Schichtenarchitektur das Verständnis der für diese Arbeit relevanten Standards erleichtert, wird im Folgenden kurz das sogenannte *OSI-Referenzmodell* vorgestellt. Anschließend wird noch genauer auf das im Rahmen dieser Arbeit verwendete *UDP*-Protokoll sowie die entsprechenden *IP-spezifischen Parameter* eingegangen.

2.1.1 ISO/OSI-Modell

Das *Open Systems Interconnection Model* ist ein standardisiertes Referenzmodell für Netzwerkprotokolle und beschreibt diese in einer Schichtenarchitektur (vgl. [Jü09, Einführung]). Es setzt sich aus sieben Schichten (engl. *Layer*) zusammen, deren funktionaler Abstraktionsgrad nach unten hin abnimmt. Sinn des Modells ist es, eine einheitliche und transparente Sicht auf Kommunikationssysteme zu schaffen, um ein besseres Verständnis der Systeme zu ermöglichen. Weiterhin dient es als Bezugssystem bei der Implementierung neuer Verfahren.

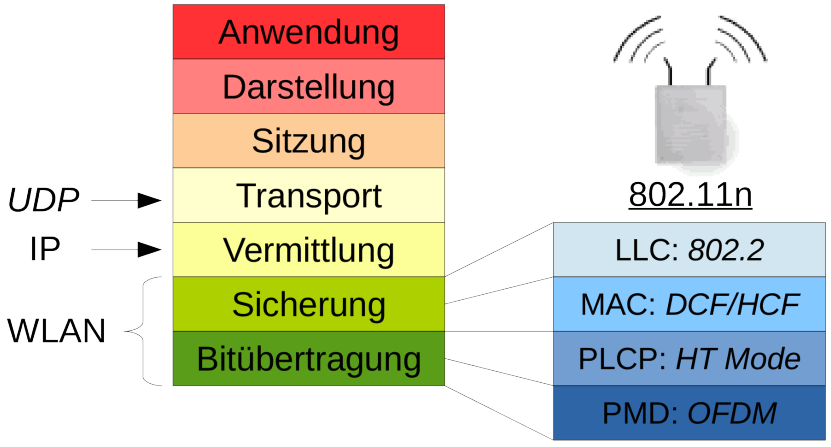


Abbildung 2.1: *Projektspezifische Ansicht des OSI-Referenzmodells mit WLAN-Sublayer.*

In Abb. 2.1 sind die sieben OSI-Layer – um projektspezifische Anmerkungen ergänzt – dargestellt. Im Rahmen der Arbeit interessant ist der Zusammenhang zwischen der physikalischen Bitübertragung des Funkkanals (engl. *Physical Layer*, kurz *PHY*) und der Abbildung auf die höhere IP-Ebene. Als Transportprotokoll kommt hierbei UDP zum Einsatz. Weiterhin sind in der Darstellung auch spezielle, für das Verständnis des WLAN-Kanals wichtige, Schichten aufgeschlüsselt. Nach dem erweiterten OSI-Modell wird die Sicherungsschicht in die Adressierung und Fehlerprüfung (engl. *Logical Link Control*, kurz *LLC*) sowie das Medienzugriffsverfahren (engl. *Media Access Control*, kurz *MAC*) aufgeteilt. Die abgebildete Unterteilung des Physical Layers ist funktionalen Ursprungs und wird im Abschnitt 2.2 genauer erläutert.

2.1.2 UDP-Pakete

Das *User Datagram Protocol* (*UDP*) ist ein minimales, verbindungsloses Übertragungsprotokoll der Transportschicht (vgl. [Jü09, TCP/IP]). Es wurde zum Zweck der Sprachübertragung und als einfachere Alternative zum verbindungsorientierten *Transmission Control Protocol* entwickelt und nutzt analog dazu Ports zur Identifikation der Server- beziehungsweise Client-Programme. UDP ist dabei nicht-zuverlässig, ungesichert und ungeschützt. Dies bedeutet, dass Pakete gar nicht, in unterschiedlicher Reihenfolge oder auch mehrfach beim Empfänger eintreffen können. Es gibt weder eine Garantie für die Übertragung noch für die Korrektheit und Sicherheit der Daten. Zur Vermittlung von UDP-Paketen ist IP vorgesehen.

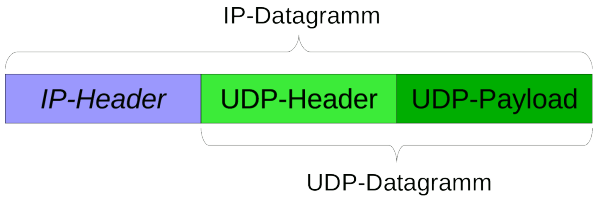


Abbildung 2.2: *Verschachtelung eines UDP-Pakets im IP-Datagramm.*

Wie bei den meisten Netzwerkprotokollen wird ein UDP- in einem IP-Paket verschachtelt übertragen. Diese Verkapselung ist in Abb. 2.2 veranschaulicht. Der IP-Header umfasst hierbei neben der Adressierungsinformation auch eine Identifikationsnummer (siehe diesbezüglich auch [ORB06, Kapitel 1, Seite 23]). Im UDP-Header sind Quell- und Ziel-Port, Länge des Payloads und eine optionale Prüfsumme hinterlegt. Berücksichtigt man neben den Headern auch diese Prüfsumme, ergibt sich eine minimale IP-Paketgröße von 28 Byte (ohne UDP-Payload). Dies entspricht wiederum einem 42 Byte großen Ethernet-Frame beziehungsweise einem mindestens 52 Byte großen WLAN-Paket (vgl. [ORB06, Kapitel 6, Seite 288]).

Da bei UDP auf unnötigen Overhead verzichtet wird, findet es bei einfachen Frage-Antwort-Protokollen – wie z.B. im *Domain Name System* – Anwendung. Des Weiteren bietet sich die ungesicherte Übertragungsform dort an, wo die Laufzeit wichtiger als das Vermeiden von Paketverlusten ist – wie beim Streaming von Video- und Audiodaten oder bei Online-Spielen. So setzt beispielsweise das für VoIP verwendete *Real-Time Transport Protocol* auf UDP auf.

Aufgrund der fehlenden Datenflusssteuerung handelt es sich bei UDP um ein leicht verständliches und somit einfach zu implementierendes Protokoll. Da ohne Flusssteuerung auch keine Fehlerbehandlung möglich ist und Übertragungsfehler folglich direkt zu Paketverlusten führen, eignet es sich auch als Indikator für die Kanalqualität. In Kombination mit der erwähnten IP-Identifikationsnummer können somit Übertragungsfehler erkannt und ausgewertet werden. Und auch aufgrund der Verbreitung im VoIP-Umfeld eignet sich UDP zur QoS-basierten Analyse des Kanalverhaltens.

2.1.3 IP-Parameter

Da die Paketvermittlung den dritten Layer im OSI-Modell darstellt, sind IP-basierte Dienste von den darunterliegenden Schichten abhängig. Wird IP als Übertragungsprotokoll im Telekommunikationsnetz eingesetzt, bedeutet dies, dass sich die Qualität der Übertragung sowohl aus den Eigenschaften der IP-Ebene als auch denen der Sicherungs- und Bitübertragungsschicht zusammensetzt. Das auf den oberen Layern beobachtbare Übertragungsverhalten ergibt sich somit aus dem Zusammenspiel aller möglicher Beeinträchtigungen.

a) Allgemeine Begriffsklärung

Zur Bewertung der Dienstgüte in IP-Netzwerken werden üblicherweise folgende Leistungsparameter verwendet (vgl. [Jü09, Einführung]):

- *Durchsatz*: Die pro Zeiteinheit im Mittel übertragene Datenmenge.
- *Bandbreite*: Die physikalisch obere Grenze des Durchsatzes an Daten.
- *Paketverlustrate*: Die Wahrscheinlichkeit, dass Pakete verloren gehen.
- *Paketumlaufzeit*: Die Übertragungsdauer von der Quelle zum Ziel und wieder zurück; wird auch *Round-Trip-Time* genannt.
- *Latenzzeit*: Die Gesamtverzögerung der Ende-zu-Ende-Übertragung einer Nachricht; auch als *Delay* bezeichnet.
- *Jitter*: Meistens die Abweichung der Latenzzeit von ihrem Mittelwert.

Als *Delay* kann allerdings sowohl die Verzögerung vom Sender zum Empfänger (engl. *end-to-end one-way delay*) als auch die Verzögerung zwischen Paketen (engl. *packet-to-packet delay*) bezeichnet werden. Der Begriff des *Jitters* beschreibt im Allgemeinen lediglich Schwankungen bei der Übertragung von Signalen und ist nicht eindeutig definiert. Die *Internet Engineering Task Force* empfiehlt daher den Begriff möglichst zu vermeiden:

> „The variation in packet delay is sometimes called "jitter". This term, however, causes confusion because it is used in different ways by different groups of people. [...] In this document we will avoid the term "jitter" whenever possible and stick to delay variation which is more precise.“ [Car02, Seite 3]

Um Verwirrungen entgegenzuwirken, werden die im Rahmen der Arbeit verwendeten Parameter im Folgenden detailliert beschrieben und mit alternativen Begriffen besetzt.

b) Projektspezifische Parameter

Wie bereits angedeutet, setzt sich die Zeit, welche zwischen dem Abschicken und der Ankunft einer Nachricht vergeht, aus den unterschiedlichen Verzögerungen – namentlich aus der Verarbeitungs-, Übertragungs- und Ausbreitungsverzögerung – der beteiligten Schichten zusammen. Sie bildet somit auch teilweise die Kanaleigenschaften der entsprechenden Bitübertragungsschicht ab.

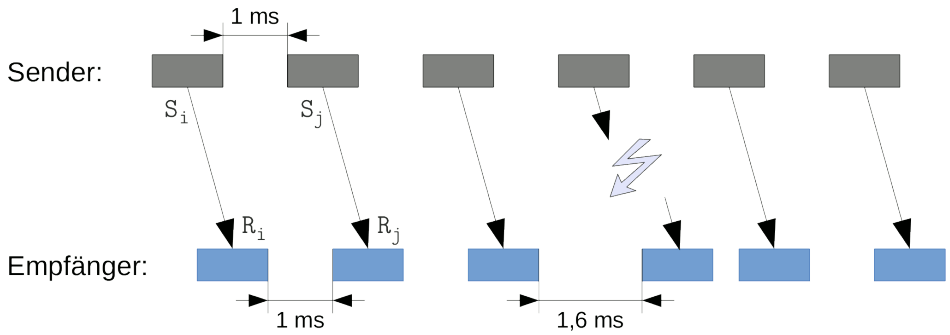


Abbildung 2.3: *Auswirkung von Transportproblemen auf die empfängerseitige Inter-Packet Time.*

Um diese Eigenschaften unkompliziert erfassen zu können, wurde im Rahmen des *MobQoS*-Projekts eine einfache Testmöglichkeit entwickelt: Wie in Abb. 2.3 gezeigt, erzeugt ein Sender einen konstanten Paketstrom (d.h. mit zeitlich gleichbleibendem Abstand: $Sj - Si = const.$). Durch kanalbedingte Schwankungen der Laufzeit entsteht ein nicht mehr konstanter Paketabstand am Empfänger (d.h.: $Rj - Ri \neq const.$).

Die im Projekt verwendete Größe entspricht also dem *Packt-to-Packet Delay* beziehungsweise der *Inter-Packet Time* (*IPT*) auf der Empfängerseite – bei Verwendung einer zeitlich konstanten Paketquelle auf der Sendeseite. Im Rahmen des *NetQoS*-Projekts wird sich hierbei darauf geeinigt, immer von der IPT zu sprechen. Diese Nomenklatur wird im Folgenden auch in dieser Arbeit verwendet.

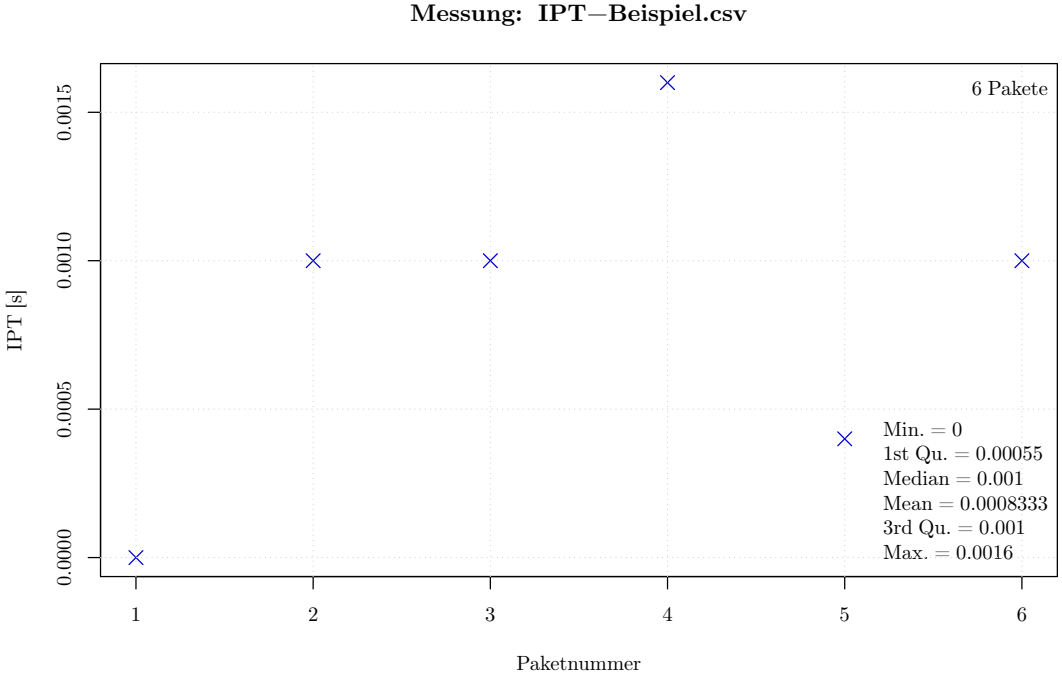


Abbildung 2.4: *Streudiagramm der Abb. 2.3 gezeigten IPTs.*

Abb. 2.4 illustriert die statistische Auswertung des in Abb. 2.3 gegebenen Beispiels mithilfe eines speziell entwickelten *R*-Skripts. Hierbei werden die Inter-Packet Times über die Nummer der jeweils aufgezeichneten Pakete aufgetragen. Dies erleichtert die Identifizierung von Schwankungen in der Übertragungszeit und ermöglicht so die Auswertung kanalcharakteristischer Verzögerungseffekte. Da sich die IPT jeweils aus der zeitlichen Differenz zum vorherigen Paket berechnet, wird zusätzlich das erste Paket als Null-Referenz eingeführt. In Abschnitt 3.3 wird die Funktionsweise des entsprechenden Skripts genauer erläutert.

2.2 Wireless Local Area Network

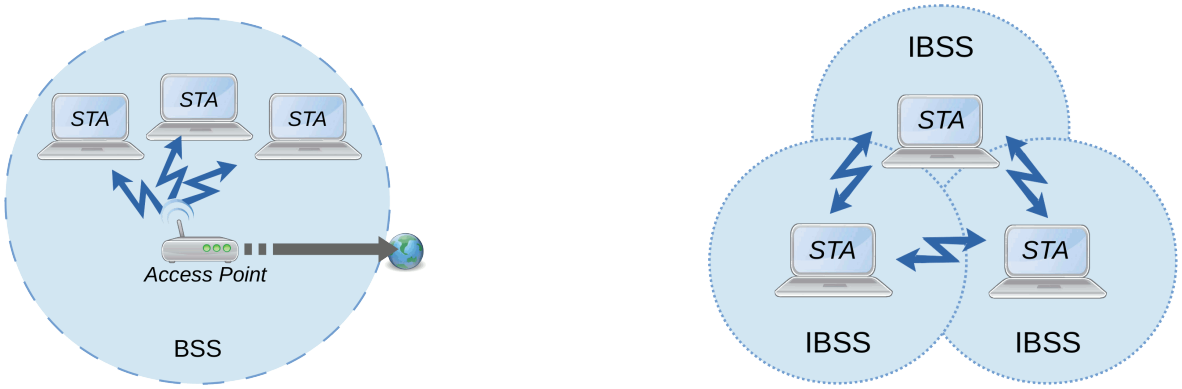
Unter dem Begriff *WLAN* werden meist lokale Funknetzwerke der *IEEE-802.11*-Familie zusammengefasst. Konkret spezifizieren die dahinterliegenden Standards Anpassungen an die Schichten 1 und 2 im OSI-Modell (vgl. [Mar13, Seite 297 ff.]).

Die ursprüngliche Version des Standards von 1997 beschreibt diesbezüglich neben dem MAC-Layer drei physikalische Übertragungstechniken, nämlich zwei Spreizspektrumverfahren zur Kommunikation via Funk und eine Infrarot-basierte Technik (siehe auch [Mus02, Seite 5 und 72 f.]). Ursprünglich befindet sich der Frequenzbereich von WLAN mit 2,4 GHz im lizenzfreien *ISM-Band*. Um höhere Datenraten zu erreichen, wird 1999 der PHY-Layer durch *802.11a* und *802.11b* erweitert. *802.11a* nutzt dabei auch erstmalig Frequenzen im 5 GHz-Bereich. Mit *802.11g* aus dem Jahr 2003 werden die bisherigen Anpassungen für das 5 GHz-Band dann ins ISM-Band übernommen. Erst der 2009 ratifizierte *802.11n*-Standard stellt wieder eine Erweiterung der MAC-Schicht dar. Neben den genannten Normen enthält die *802.11*-Familie auch spezielle Erweiterungen – wie *802.11i* und *802.11e*, die zum Beispiel mögliche Verschlüsselungsverfahren beziehungsweise den QoS-konformen Kanalzugriff spezifizieren.

Im Folgenden soll ein – konkret auf den in der Arbeit betrachteten 802.11n-Standard bezogener – Einblick in Anwendungsszenarien, Medienzugriffsverfahren und Übertragungsarten gegeben werden. Dies soll die Grundlagen zum Verständnis der IPT-Charakteristik legen.

2.2.1 Betriebsarten von WLAN

WLAN-Netze setzen sich im Allgemeinen aus mindestens einem *Access Point* (*AP*) und einer damit verbundenen *Station* (*STA*) zusammen. Diese grundlegende Einheit wird als *Basic Service Set* (*BSS*) bezeichnet (vgl. [Mus02, Seite 6 f.]). Zur Identifikation eines solchen Netzwerks wird daher die *BSS-ID* verwendet. Diese kann um eine frei wählbare Kennung – die sogenannte *SSID* – erweitert werden, welche mithilfe von *Beacon*-Frames über Funk bekannt gegeben wird. Zur Erhöhung der Gesamtreichweite kann ein solches Netz zu einem *Extended Service Set* ausgebaut werden. Dies setzt eine Vernetzung mehrerer Access Points voraus – wie sie beispielsweise in *Wireless Distribution Systems* umgesetzt wird – und soll hier nicht näher besprochen werden. Auch das sogenannte *Repeating* ist nicht Teil dieser Arbeit.



(a) Infrastruktur-Modus.

(b) Ad-Hoc-Modus.

Abbildung 2.5: *Topologien der Betriebsmodi bei WLAN.*

802.11 kennt die zwei Betriebsmodi *Infrastruktur* und *Ad Hoc* (siehe [Fab10, Seite 9]). Wie in Abb. 2.5 veranschaulicht ist, unterscheiden sich diese darin, dass im ersten Fall eine zentrale Stelle die Koordination der Funkzelle übernimmt, im zweiten Fall konfiguriert sich das WLAN selbst. Die Beacon-Frames eines AP im Infrastruktur-Modus enthalten daher neben dem Netzwerknamen auch weitere Informationen, wie beispielsweise zu den unterstützten Übertragungsraten. Im Ad Hoc-Modus hingegen müssen sich alle STAs automatisch auf dieselben Einstellungen einigen, man spricht daher von *Independent Basic Service Sets*.

In den meisten Fällen handelt es sich bei WLAN-Netzen um einzelne, zentral koordinierte BSSs, in denen ein AP mit mehreren STAs verbunden ist. Der Durchmesser solcher Infrastruktur-Netzwerke liegt höchstens bei wenigen hundert Metern (vgl. [Mar13, Seite 352]).

2.2.2 Bitübertragung bei WLAN

Die physikalische Datenübertragung erfolgt bei WLAN im nach Standard definierten Frequenzbereich mit unterschiedlichen Modulationsverfahren. Im Weiteren wird auf die entsprechenden Einzelheiten eingegangen, wobei Erkenntnisse zu 802.11n im Vordergrund stehen.

a) Frequenzbereich

Wie einleitend bereits erwähnt, verwendet WLAN hauptsächlich zwei Frequenzbereiche zur Funkübertragung. 802.11bg nutzt dabei die Frequenzen von 2412 bis 2484 MHz und a arbeitet im Bereich von 4915 bis 5825 MHz. Der neuere n-Standard spezifiziert schließlich den Gebrauch beider Spektren (also im 2,4 und im 5 GHz-Bereich).

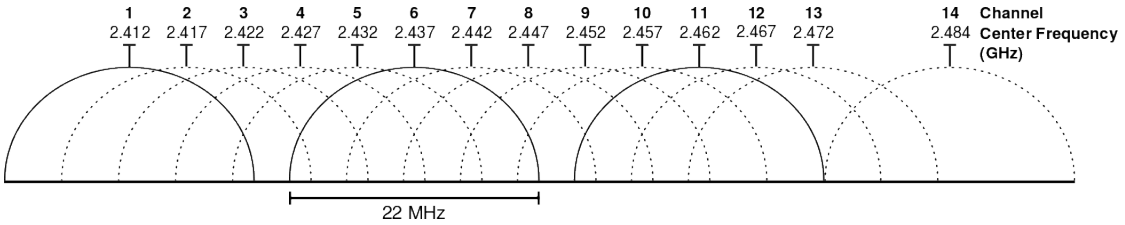


Abbildung 2.6: *Kanalbelegung im 2,4 GHz-Band. [wikimedia.org (CC BY-SA* Michael Gauthier*)]*

Der 2,4 GHz-Bereich unterteilt sich – je nach Frequenzzuteilung der nationalen Regulierungsbehörden[6] – in bis zu 14 Kanäle. Das 5 GHz-Band verfügt in Europa derzeit über 19 zugelassene Kanäle. Die genaue Kanalbreite ist von der jeweiligen Modulation abhängig. So beträgt die Bandbreite eines Kanals bei 802.11b *22 MHz* und bei g *20 MHz*. 802.11n sieht schließlich eine zusätzliche Kanalbündelung auf dann *40 MHz*-Kanalbreite vor. Wie in Abb. 2.6 zu sehen ist, führt diese Frequenzeinteilung im 2,4 GHz-Bereich zu Kanalüberlappungen. Bei einfacher Kanalbreite (20 MHz) ist das 5 GHz-Band überlappungsfrei.

b) Multiplex- und Modulationsverfahren

Während der ursprüngliche 802.11-Standard neben der Infrarotübertragung die zwei Datenübertragungsverfahren *Frequency Hopping* und *Direct Sequence Spread Spectrum* im Funkbereich spezifiziert, ist bei 802.11b die *Complementary Code Keying*-Modulation vorgesehen (siehe auch [Xia12, Seite 2 f.]). Erst mit 802.11a wird das *Orthogonal Frequency-Division Multiplexing* (*OFDM*) – eine spezielle Implementierung der Mehrträgermodulation – eingeführt. Auch 802.11g verwendet dieses Multiplexverfahren, welches im n-Standard schließlich noch um *Multiple Input Multiple Output* (*MIMO*) erweitert wird.

Konkret handelt es sich beim *OFDM* um ein auf mehreren zueinander orthogonalen Trägern beruhendes Frequenzmultiplexverfahren. Zur Erhöhung der Störfestigkeit wird der sogenannte *Guard Interval* verwendet (vgl. [Xia12, Seite 10]). Für die Einzelträger sind dabei die Modulationsverfahren *Phasenmodulation*, *Quadraturphasenumtastung* oder *Quadraturamplitudenmodulation* (kurz *BPSK/QPSK/QAM*) vorgesehen. Als Schema zur Bestimmung der jeweils zur Datenrate passenden Modulation wird seit 802.11n einen spezielles Schema verwendet. Dieses wird im Folgenden kurz vorgestellt.

[6] vgl. `https://en.wikipedia.org/wiki/List_of_WLAN_channels`

c) MCS-Indizierung

Bei Nutzung der MIMO-Technik, unterschiedlicher Bandbreiten und Guard Intervals müssen sich APs und STAs über das zu verwendende Modulations- und Kodierungsverfahren einigen. Hierfür kommt bei 802.11n ein spezielles *Modulation and Coding Scheme* (*MCS*) – wie es in Tab. 1 ausschnittsweise dargestellt ist – zum Einsatz (siehe [Air08, Seite 7 ff.]). Das Schema listet dabei die zu den MCS-Indizes gehörigen Modulationsverfahren, die Informationsraten der Kodierung und die entsprechenden Datenraten auf. Zusätzlich ist die Tabelle in Kanalbreite (20/40 MHz) und Schutzintervallgröße (800/400 ns) untergliedert.

MCS Index	**Spatial Streams**	**Modulation**	**Coderate**	**Datenrate (Mbit/s)**			
				20 MHz		**40MHz**	
				800ns	**400ns**	**800ns**	**400ns**
0	1	BPSK	1/2	6,50	7,20	13,50	15,00
1	1	QPSK	1/2	13,00	14,40	27,00	30,00
2	1	QPSK	3/4	19,50	21,70	40,50	45,00
3	1	16-QAM	1/2	26,00	28,90	54,00	60,00
4	1	16-QAM	3/4	39,00	43,30	81,00	90,00
5	1	64-QAM	2/3	52,00	57,80	108,00	120,00
6	1	64-QAM	3/4	58,50	65,00	121,50	135,00
7	1	64-QAM	5/6	65,00	72,20	135,00	150,00
8	2	BPSK	1/2	13,00	14,40	27,00	30,00
9	2	QPSK	1/2	26,00	28,90	54,00	60,00
10	2	QPSK	3/4	39,00	43,30	81,00	90,00
11	2	16-QAM	1/2	52,00	57,80	108,00	120,00
12	2	16-QAM	3/4	78,00	86,70	162,00	180,00
13	2	64-QAM	2/3	104,00	115,60	216,00	240,00
14	2	64-QAM	3/4	117,00	130,00	243,00	270,00
15	2	64-QAM	5/6	130,00	144,40	270,00	300,00
16	3	BPSK	1/2	19,50	21,70	40,50	45,00
...	...	...	...	...	...	...	...
31	4	64-QAM	5/6	260,00	288,80	540,00	600,00

Tabelle 1: *Exemplarischer Ausschnitt aus der MCS-Tabelle von 802.11n.*[7]

Der *MCS-Index 3* bedeutet beispielsweise, dass die Datenübertragung per 16-fach quantisierter Quadraturamplitudenmodulation und bei einer Coderate von 1/2 stattfindet. Weiterhin wird nur ein Übertragungskanal verwendet (kein MIMO). Bei einer einfachen Kanalbreite und einem Guard Interval von 800 ns ergibt sich eine maximale Datenrate von 26 Mb/s brutto[8].

d) Synchronisation und Signalisierung

Um die Datenübertragung physikalisch umzusetzen, verwendet WLAN – wie bereits in Abb. 2.1 dargestellt – die sogenannte *Physical Layer Convergence Procedure* (*PLCP*) sowie den *Physical Medium Dependent*-Sublayer (*PMD*). Erstere erweitert das WLAN-Frame um Informationen zur Synchronisation und zur Datenrate, Letzterer beschreibt die tatsächliche Umsetzung auf das Übertragungsmedium (vgl. [Fab10, Seite 15 f.]).

Wichtig hierbei ist, dass sich der konkrete Aufbau der PLCP-Pakete zwischen den einzelnen Standards unterscheidet. Bei der in 802.11agn verwendeten OFDM bestehen die physikalischen Pakete aus einer *PLCP-Präambel*, dem *PLCP-Header* und dem eigentlichen Payload. Dabei dient die Präambel zur Erfassung des ankommenden Signals und der Header transportiert die zur Dekodierung der Nutzdaten nötigen Signalinformationen. Um den Empfang dieser Informationen zu gewährleisten, wird im Header eine allgemein festgelegte Modulation eingesetzt (siehe auch [Mus02, Seite 60 ff.]). Erst der angehängte MAC-Frame, also die eigentlichen Nutzdaten, sind dann entsprechend anders kodiert. Aufgrund der verbesserten Modulationsverfahren bei 802.11n ergeben sich hier allerdings Probleme mit der Abwärtskompatibilität zu 802.11abg (vgl. hierzu [Air08, Seite 10 f.]). Konkret sieht der n-Standard daher drei verschiedene Präambeln vor, die von den älteren Geräten vollständig, teilweise oder gar nicht dekodiert (*Legacy/Mixed/Greenfield Mode*) werden können. Ob und inwieweit die Übertragungen Anderer erfasst werden können, ist ein in Bezug auf die Medienzugriffssteuerung wichtiger Aspekt.

2.2.3 Paketsicherung bei WLAN

Die Sicherungsschicht der 802.11-Familie setzt sich – wie ebenfalls bereits in Abb. 2.1 veranschaulicht – aus dem LLC- und dem MAC-Layer zusammen. Auch wurde bereits erwähnt, dass der WLAN-Standard nur die Medienzugriffssteuerung spezifiziert. Konkret ist die LLC-Schicht durch *802.2* standardisiert (vgl. [Fab10, Seite 10]).

[7] siehe diesbezüglich auch `http://mcsindex.com`

[8] Der Durchsatz an reinen Nutzdaten ist entsprechend geringer.

Aufgrund der Tatsache, dass bei WLAN mehrere Teilnehmer (ohne Duplexverfahren) auf demselben Übertragungskanal miteinander kommunizieren, kann es zu Paketkollisionen kommen. Um dies zu vermeiden, werden verschiedene Mechanismen eingesetzt. Da diese einerseits ziemlich komplex, andererseits aber auch besonders charakteristisch für die WLAN-Übertragung sind, sollen sie im Folgenden etwas ausführlicher vorgestellt werden.

a) Grundlegende Medienzugangsverfahren

Grundsätzlich gibt es zwei Ansätze, um den Zugriff auf ein gemeinsames, kollisionsbehaftetes Medium zu regeln. Der eine Ansatz besteht darin, die Wahrscheinlichkeit von Zusammenstößen durch Beobachtung des Kanals und mithilfe stochastischer Verfahren zu verringern. Die andere Möglichkeit ist die Verwendung einer zentralen und deterministischen Koordinationsstelle, die den Übertragungskanal explizit frei gibt. Der 802.11-Standard definiert hierzu die *Distributed Coordination Function* (*DCF*) beziehungsweise die optionale *Point Coordination Function* (*PCF*). Diese sogenannten Koordinierungsfunktionen setzen dabei die beiden, eben erläuterten, grundlegenden Verfahren zur Kollisionsvermeidung um.

Da diese Mechanismen aber keine Qualitätssicherung unterstützen, werden mit *802.11e* weitere Strategien eingeführt. Konkret setzt sich die *Hybrid Coordination Function* (*HCF*) aus dem *Enhanced Distributed Channel Access* (*EDCA*) und dem wiederum optionalen *HCF Controlled Channel Access* (*HCCA*) zusammen (siehe [Mar09, Seite 5 f.]). Beide Verfahren definieren entsprechende Datenverkehrsklassen zur Priorisierung von Paketen.

Oft ist im Zusammenhang mit QoS bei WLAN auch von *WMM* (für *Wi-Fi Multimedia*) die Rede. Diese Industrieinitiative gilt als Mindeststandard für QoS im WLAN-Bereich und schreibt hierzu lediglich die Unterstützung von EDCA vor.[9]

Trotz der Vielzahl an standardisierten Methoden ist für diese Arbeit letztendlich nur die tatsächliche Verbreitung derselben ausschlaggebend. Zu diesem Thema lässt sich eine Feststellung der *Certified Wireless Network Professional* aus dem Jahre 2009[10] zitieren:

> „At the time of this writing, no vendor has implemented PCF or HCCA.“ [Mar09]

Aufgrund der offensichtlich geringen praktischen Bedeutung der zentralisierten Koordinierungsfunktionen wird an dieser Stelle nicht weiter auf diese eingegangen.

[9] Quelle: `http://wifi-insider.com/wlan/wmm.htm` (abgerufen am 08.10.2014)

[10] Soweit dem Autoren bekannt, gilt diese Aussage auch noch zum Zeitpunkt dieser Arbeit. Weder die hier verwendete Hardware verfügt über eine solche Unterstützung noch konnten entsprechende Implementierungen bezogen werden.

b) Konkreter Mehrfachzugriff mittels CSMA/CA

Die für WLANs obligatorische DCF basiert auf dem *CSMA/CA*-Verfahren (für *Carrier Sense Multiple Access/Collision Avoidance*). Im Gegensatz zum beim Ethernet verwendeten *Collision Detection*-Verfahren kann bei der Funkübertragung das Medium während der Übertragung nicht ausreichend überwacht werden[11], CSMA/CA setzt daher auf die *listen before talk*-Strategie zur bestmöglichen Kollisionsvermeidung (siehe [Xia12, Seite 3]). Wird eine Kollision erkannt, arbeitet WLAN mit einem *Backoff*-Stauauflösungsmechanismus.

Grundsätzlich funktioniert CSMA/CA dabei so, dass der Übertragungskanal sowohl physikalisch als auch virtuell überwacht wird (vgl. hierzu auch [Mar09, Seite 7 ff.]). Beim *Physical Carrier Sensing* wird die Signalleistung überwacht und auf erkannte Pakete reagiert. Um zusätzlich gleichzeitige Sendeversuche zu verhindern, arbeitet *Virtual Carrier Sensing* mit einem Netzbelegungsvektor (engl. kurz *NAV*) zur Trägerprüfung. Dieser verarbeitet bekannte Informationen – wie zum Beispiel die im PLCP-Header enthaltene Paketlänge und das Wissen über den grundsätzlichen Protokollablauf – und berechnet daraus die zur Kollisionsvermeidung benötigten Wartezeiten. Erst wenn das Medium in beiden Fällen frei ist, darf eine Übertragung begonnen werden. Um Paketkollision durch gleichzeitige Sendevorgänge zu vermeiden, warten die beteiligten Teilnehmer zusätzlich noch eine zufällige Zeitspanne – die sogenannte *Backoff*-Zeit – ab. Kommt es dennoch zu Zusammenstößen, wird diese Wartezeit exponentiell erhöht und der Überwachungprozess beginnt von vorne. Durch dieses Vorgehen können Kollisionen effizient verhindert und nötigenfalls auch aufgelöst werden.

Zum Abschluss einer Übertragung und zur Kanalfreigabe verwendet WLAN ein `ACK`. Für eine solche, positive Quittierung muss das Paket korrekt empfangen worden sein, d.h. der CRC-Wert muss mit der FCS des WLAN-Frames (siehe unten) übereinstimmen. Weil WLAN über kein *Negative Acknowledgement* zur Ablehnung verfügt, wird der Fehlerfall mithilfe eines Timeouts erkannt. Da weiterhin eine automatische Retransmission im Fehlerfall vorgesehen ist, handelt es sich bei WLAN um ein *ARQ*-Protokoll (für *Automatic Repeat reQuest*). Und weil bei Übertragungsfehlern grundsätzlich von einem Paketzusammenstoß auszugehen ist, wird bei jeder Retransmission die Backoff-Zeit entsprechend erhöht.

[11] Sende- und Empfangspegel unterscheiden sich stark, weswegen eine synchrone Beobachtung technisch aufwändig ist.

Zur weiteren Verringerung der Kollisionswahrscheinlichkeit kann der *RTS/CTS*-Mechanismus (für *Request To Send/Clear To Send*) genutzt werden. Durch Einsatz dieses Handshake-Protokolls werden alle im Übertragungsbereich eines APs befindlichen STAs über Kanalbelegung und die Dauer derselbigen informiert. Wegen des dabei entstehenden Overheads wird aber oft nur das vereinfachte *CTS-to-self*-Verfahren eingesetzt, bei dem die Paketübertragung lediglich vom jeweiligen Sender vorangekündigt wird. Beide genannte Verfahren sind optional.

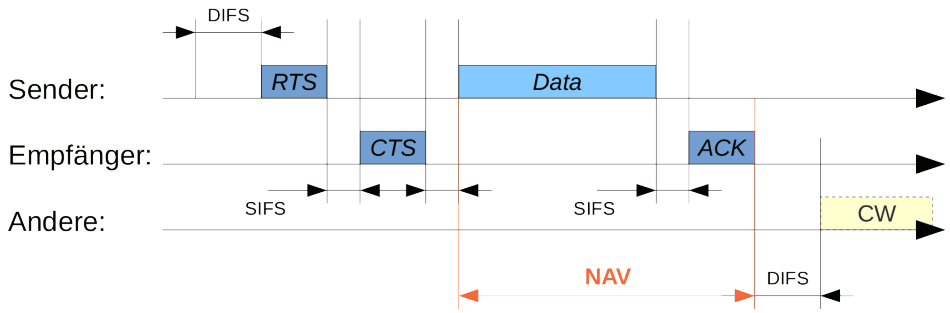


Abbildung 2.7: *DCF Inter-Frame Spacing bei aktiviertem RTS/CTS.*

c) Interframe Spacing

Zur weiteren Verbesserung des Übertragungsverhaltens werden verschieden lange Paketabstände eingeführt (siehe [Mar09, Seite 11 ff.]). Abb. 2.7 zeigt, wie ein Sender eine Sendeanfrage (`RTS`) stellt und nach Erhalten der Kanalfreigabe (`CTS`) die Daten überträgt. Anschließend bestätigt der Empfänger die Korrektheit der Übertragung (`ACK`). Zwischen den einzelnen Paketen kommen dabei unterschiedliche Wartezeiten zum Einsatz.

Diese sogenannten *Interframe Spaces* dienen in erster Linie als optimaler zeitlicher Abstand. Zusätzlich ermöglichen unterschiedliche Längen eine Priorisierung von Paketen (z.B. für Control-Frames wie `CTS` oder `ACK`). Die Berechnung der Wartezeiten erfolgt dabei auf Grundlage der *Slot Time*, dem minimal kollisionsfreien Signalabstand im Funknetzwerk. Als *Contention Window* (*CW*) wird in diesem Zusammenhang der Gültigkeitsbereich des zur Kollisionsvermeidung und Stauauflösung verwendeten Backoffs bezeichnet. Bei EDCA werden die Interframe Spaces je nach Verkehrsklasse des zu übertragenden Pakets angepasst, um so die entsprechenden Dienstgüten umzusetzen. Vereinfacht gesagt „drängeln“ sich wichtigere Pakete vor.

d) WLAN-Frame

Wie schon auf der physikalischen Ebene wird auch auf der MAC-Schicht der entsprechende Payload eines Paketes gekapselt übertragen. Dieser Zusammenhang wird in Abb. 2.8 veranschaulicht. Der MAC-Header besteht aus Adressierungsinformationen, protokollspezifischen Daten und zusätzlichen Informationen für den NAV (vgl. [Mus02, Seite 20 ff.]). Anschließend folgen die Nutzdaten der Vermittlungsschicht, welche durch eine *Frame Check Sequence* (*FCS*) zur Fehlererkennung abgeschlossen werden. Zu den protokollspezifischen Daten gehören insbesondere die für den Medienzugang genutzte Paketlaufzeit (engl. *Duration*) sowie das *Retry*-Flag zur Kennzeichnung von Retransmissionen. Die in 802.11 spezifizierten Pakettypen sind dabei *Management Frames* – wie Beacons –, *Controll Frames* – wie `ACK` – und *Data Frames*.

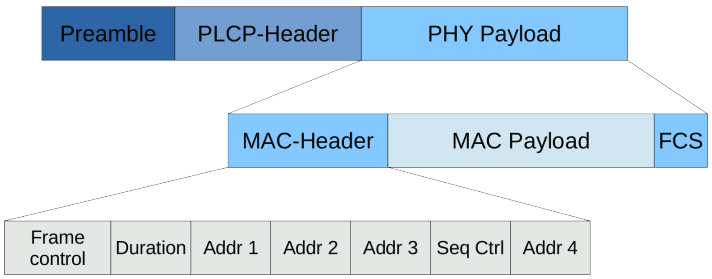


Abbildung 2.8: *Schichtenspezifisch verschachtelter Aufbau eines WLAN-Pakets.*

Auch die WLAN-Verschlüsselung findet auf der MAC-Ebene statt. Sowohl das ursprüngliche *WEP* als auch das verbesserte, nach 802.11i spezifizierte *WPA*-Verschlüsselungsverfahren nehmen dazu Anpassungen am Datenpaket vor.[12] Neben den verschlüsselten Nutzdaten müssen natürlich auch die für die Entschlüsselung nötigen Informationen transportiert werden. Am grundlegenden Aufbau des WLAN-Frames ändert dies allerdings nichts.

Als besondere, standardspezifische Verbesserung sei an dieser Stelle noch die Optimierung des WLAN-Frames bei 802.11e genannt. Da die Kollisionsvermeidung erheblichen Overhead erzeugt, werden zwei Verfahren zur Paketaggregation spezifiziert (siehe [Cis07, Seite 9 ff.]). Die eine Methode entspricht einem *Bursting*, d.h. mehrere Payloads werden zu einem größeren Paket zusammengesetzt. Beim zweiten Verfahren handelt es sich um ein *Block-Acknowledgement*.

[12] Quelle: `http://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx` (vom 28.03.2003, abgerufen am 08.10.2014)

2.2.4 Zusammenfassung für diese Arbeit

Im Rahmen dieses Grundlagenkapitels werden die wichtigsten Eigenschaften von WLAN erarbeitet. Als Betriebsart wird im Folgenden der Infrastrukturmodus mit mindestens einem AP und einer STA untersucht. Auf der physikalischen Schicht ist es wichtig zu wissen, dass das 2,4 GHz-WLAN im ISM-Band liegt und es zu Kanalüberlappungen kommen kann. Aufgrund der Abwärtskompatibilität spielen hierbei auch die unterschiedlichen Modulationsverfahren eine Rolle. Speziell bei 802.11n kommen MCS-Indizes zum Einsatz und es gibt je zwei verschiedene Frequenzbereiche, Kanalbreiten und Schutzintervalllängen. Der Medienzugang ist in WLAN-Netzen meistens durch die DCF geregelt, die mittels WMM um eine QoS-Unterstützung erweitert wird. Zur Verbesserung des Kollisionsverhaltens kann zusätzlich das RTS/CTS-Verfahren genutzt werden. Bei der Regelung des Mehrfachzugriffs werden verschiedene Interframe Spaces verwendet. Als Quittierung und für die Kanalfreigabe wird ein `ACK` gesendet. Werden Übertragungsfehler erkannt, ist eine Retransmission vorgesehen. Dabei werden diese durch Retry-Flags in den WLAN-Frames markiert.

Aufgrund der Tatsache, dass in dieser Arbeit der 802.11n-Standard im Vordergrund steht, folgt noch ein kurzer Überblick über die entsprechenden Besonderheiten (vgl. [Air08, Cis07]):

(i) PHY-Schicht:

- *Frequenzband*: 2,5 und 5 GHz. (Kanäle in Europa: 1 – 13 sowie 36 – 140)
- *Kanalbündelung*: Zwei 20 können zu einem 40 MHz-Kanal kombiniert werden.
- *Verbesserte Modulation*: Neues MCS-Schema mit bis zu 4×MIMO. (*High Throughput*)
- *Kürzerer Guard Interval*: Optionale 0,4 statt bisherige 0,8 μs Schutzintervalllänge.
- *Abwärtskompatibilität*: Verschiedene PLCP-Präambeln. (*Legacy/Mixed/Greenfield Mode*)

(ii) MAC-Schicht:

- *Reduced Interframe Space*: RIFS statt bisher SIFS.
- *Packet Aggregation*: A-MSDU (*Bursting*), A-MPDU (*Block-ACK* mit *Selective Repeat*).

(iii) Zusatz-Normen:

- *802.11i-Verschlüsselung*: WPA/WPA2.
- *802.11e-QoS bzw. WMM*: EDCA/HCCA (statt DCF/PCF).

2.3 Universal Mobile Telecommunications System

Als Mobilfunkstandard der dritten Generation ordnet sich *UMTS* zwischen *GSM* und *LTE* ein (siehe [Mar13, Seite 127 ff.]). Zur Veranschaulichung sind die – durch die stetige Weiterentwicklung im Bereich der mobilen Telefonie entstandenen – Techniken der verschiedenen Generationen in Abb. 2.9 anhand der maximal erreichbaren Bitraten aufgeschlüsselt.

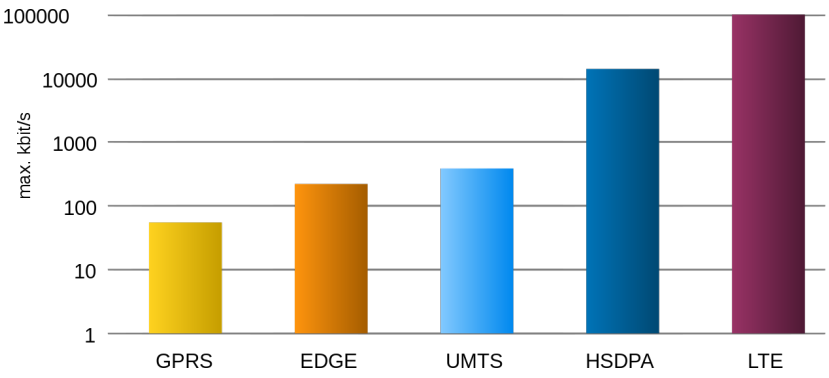


Abbildung 2.9: *Übertragungsraten im Mobilfunk. [wikimedia.org (CC BY-SA* McZusatz*)]*

Ursprünglich vom *Europäischen Institut für Telekommunikationsnormen* entwickelt, wurde UMTS von der *International Telecommunication Union* für den – auch unter dem Akronym *3G* bekannten – *IMT-2000*-Standard ausgewählt. Heute wird der Standard unter der Aufsicht des *3rd Generation Partnership Project*s gepflegt und stetig weiterentwickelt. So führt beispielsweise das – ebenfalls in Abb. 2.9 aufgelistete – *HSDPA*-Verfahren zu einer weiteren, deutlichen Beschleunigung der Datenübertragung.

Im nächsten Abschnitt wird die UMTS-Netzwerkarchitektur vorgestellt und anschließend wird auf die dahinterstehende Übertragungstechnik eingegangen. Aufgrund der andauernden technischen Weiterentwicklung bezieht sich diese Arbeit dabei auf die ursprüngliche Veröffentlichung, das *Release 99*[13] aus dem Jahre 1999.

2.3.1 Netzwerkaufbau bei UMTS

Wie in Abb. 2.10 ersichtlich, besteht ein UMTS-Netzwerk prinzipiell aus einem Zugangs- und einem Kernnetzwerk (vgl. [Har10, Seite 75 ff.]). Das auch als *UTRAN* bezeichnete Zugangsnetz setzt sich aus mindestens einer Basistation (*NodeB*) und dem zugehörigen *Radio Network Controller* (*RNC*) zusammen. Zum besseren Verständnis sind die wichtigsten Einzelkomponenten in Tab. 2 zusammengetragen (siehe hierzu auch [Bar07, Seite 15]).

[13] siehe diesbezüglich auch `http://www.3gpp.org/specifications/releases/77-release-1999`

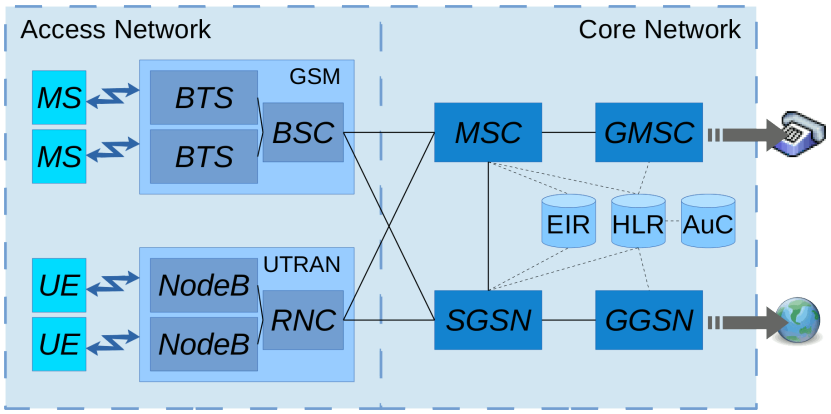


Abbildung 2.10: *Aufbau der kombinierten GSM-UMTS-Netzarchitektur.*

Während der NodeB nur für die eigentliche Funkverbindung zuständig ist, verwaltet der Netzwerkcontroller die Frequenzen und ermöglicht somit beispielsweise *Handovers*. Ein RNC steuert daher auch meistens mehr als einen Knoten. Der Durchmesser einer normalen UMTS-Funkzelle liegt dabei in der Größenordnung eines Kilometers (vgl. [Mar13, Seite 136]).

Das UMTS-Kernnetz ist von *GSM/GPRS* abgeleitet und besteht aus einem leitungs- und einem paketvermittelten Teil; jeweils entsprechende Gateways dienen als Verbindung zur Außenwelt. Weiterhin verfügt das Kernnetzwerk über drei Datenbanken mit Nutzerinformationen. Diese enthalten beispielsweise die – insbesondere für den Verbindungsaufbau wichtige – letzte Position eines Endgerätes oder zur Geräteauthentifizierung wichtige Daten.

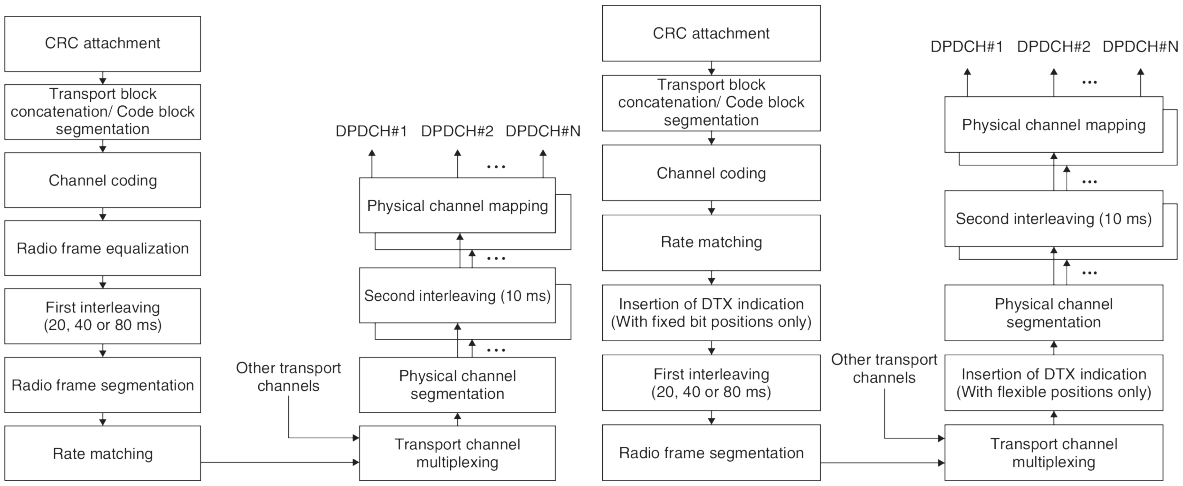
UMTS-Netzelemente	**GSM-Entsprechung**	**Funktion**
User Equipment (UE)	Mobile Station (MS)	mobiles Endgerät
NodeB	Base Station (BTS)	eigentl. Funkübertragung
Radio Network Controller (RNC)	BTS Controller (BSC)	Verwaltung der Knoten
Mobile Switching Controller (MSC)	...	Leitungsvermittlung
Gateway MSC (GMSC)	...	entspr. Zugangspunkt
Serving GPRS Suport Node (SGSN)	...	Paketvermittlung
Gateway GSN (GGSN)	...	entspr. Zugangspunkt
Equipment Identity Register (EIR)	...	Geräteverwaltung
Home Location Register (HLR)	...	Teilnehmerverwaltung
Authentication Center (AuC)	...	Authentifizierungsstelle

Tabelle 2: *Namen, Funktionen und Gegenüberstellung der einzelnen Netzelemente.*

2.3.2 Bitübertragungsschicht von UMTS

Die Funkübertragung erfolgt bei UMTS im je nach Regulierungsbehörde freigegebenen Frequenzband[14] mit dem *Wideband Code Division Multiple Access*-Verfahren (*WCDMA*). Allgemein umfasst der nutzbare Frequenzbereich dabei 1900 bis 2170 MHz. Im Vergleich zur wechselseitigen Datenübermittlung bei WLAN spezifiziert UMTS für WCDMA ein Zeit- beziehungsweise Frequenzduplexverfahren. Während *FDD* für Up- und Downlink unterschiedliche Frequenzen verwendet, findet bei *TDM* diese Trennung mithilfe von Zeitschlitzen statt (siehe [Bar07, Seite 20 ff.]). UMTS verwendet bisher hauptsächlich *FDD*.

Bei WCDMA handelt es sich um ein sogenanntes Codemultiplexverfahren (vgl. [Har10, Seite 104 ff.]). Dies bedeutet, dass die Unterscheidung der Träger nicht – wie bei OFDM – anhand der Frequenz, sondern mithilfe der Codierung geschieht.[15] Hierfür werden spezielle Spreizcodes eingesetzt, deren physikalisches Signal schließlich per *Quadraturphasenumtastung* moduliert übertragen wird. Die Bandbreite dieses Spreizsignals liegt bei 5 MHz.



(a) Kodierungsschema des dedizierten Uplinks.

(b) Kodierungsschema des dedizierten Downlinks.

Abbildung 2.11: *Multiplexing und Kanalkodierung bei UMTS. [Har10, Seite 113 und 118]*

Sowohl der Uplink als auch der Downlink werden in verschiedene WCDMA-Kanäle – welche von den jeweiligen Abstraktionsschichten abgeleitet sind – eingeteilt. Neben logischen Kanälen für den eigentlichen Informationsfluss gibt es sogenannte Transportkanäle zur Abbildung der Datenpakete und physikalische Kanäle, die die tatsächliche Übertragung beschreiben (siehe

[14] vgl. auch `https://en.wikipedia.org/wiki/UMTS_frequency_bands`

[15] Als Analogie zur Veranschaulichung dieses Verfahrens eignet sich die Beobachtung, dass man seine Muttersprache in einem internationalen Sprachwirrwarr heraushören kann.

auch [Bar07, Seite 24]). Im Rahmen dieser Arbeit interessant sind insbesondere die jeweiligen *Dedicated Channel*s, da hauptsächlich dort der Transport von Nutzdaten stattfindet.

Das Multiplexing dieser Datenkanäle findet in verschiedenen Schritten – die in Abb. 2.11 abgebildet sind – statt (vgl. [Har10, Seite 111 ff.]). Hierbei steht das *Interleaving* im direkten Zusammenhang mit dem sogenannten *Transmission Time Interval* (*TTI*). Der TTI ist ein Parameter zur Datenkapselung und dient vereinfacht gesagt dazu, die dynamische Anpassung der Datenrate an kanalspezifische Eigenschaften zu ermöglichen. Man kann ihn sich dabei als adaptiv anpassbare Paketrahmengröße vorstellen. Im *Release 99* liegt der kürzeste TTI bei 10 ms und kann die davon k-fachen Werte 20, 40 oder 80 ms annehmen. Die eigentliche physikalische Datenübertragung findet letztendlich in 15 Zeitschlitzen von jeweils etwa 666 μs statt. Aufgrund der festen Größen dieser *Radio Frame*s ist eine entsprechende Segmentierung im Rahmen der Paketsicherung nötig. Diese wird nun näher beleuchtet.

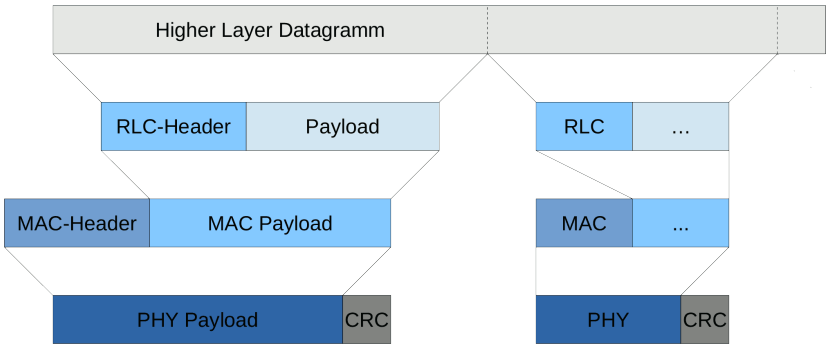


Abbildung 2.12: *Schichtenspezifischer Aufbau eines fragmentierten UMTS-Pakets.*

2.3.3 Paketsicherungsschicht von UMTS

Die UMTS-Sicherungsschicht besteht aus dem *Radio Link Control* (*RLC*) und dem *Radio Resource Control* (*RRC*) sowie dem darunterliegenden MAC-Layer (siehe [Bar07, Seite 26 ff.]).

Da aufgrund der erwähnten Duplexverfahren der Medienzugriff bereits klar geregelt ist, entfällt bei UMTS die Kollisionsvermeidung. Die Aufgaben der MAC-Schicht beschränken sich somit im Wesentlichen auf die Zuweisung der WCDMA-Kanäle, die Auswahl des passenden Übertragungsformats und die Prioritätssteuerung. Hauptaufgabe von RLC ist die Segmentierung sowie die Fehlerbehandlung von einzelnen Paketen. RRC schließlich kümmert sich in erster Linie um die Signalisierung zwischen der Basistation und dem Endgerät – wie sie beispielsweise für den Verbindungsaufbau oder Handovers benötigt wird.

Abb. 2.12 dient zur Veranschaulichung der Paketsegmentierung und Datenkapselung (siehe [Mar13, Seite 164 ff.]). Diese *Radio Frame Segmentation* ist nötig, um größere Pakete höherer Schichten in die wesentlich kleineren Rahmen der Übertragungsschicht abzubilden. Umgekehrt können auf diese Art aber auch kleinere Pakete zur Übertragung aggregiert werden. Die Segmentgröße steht dabei wiederum im Zusammenhang zum bereits erwähnten TTI.

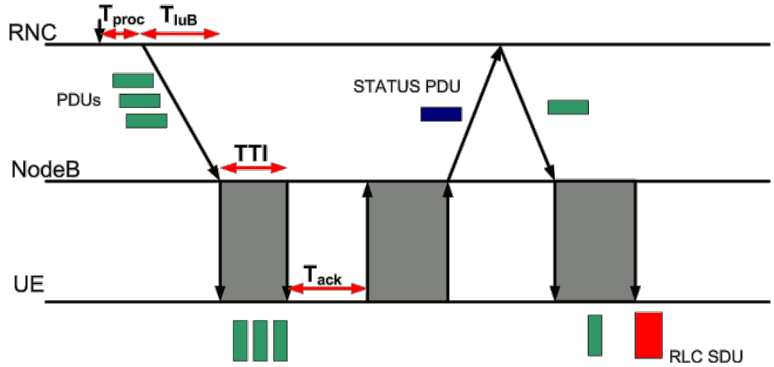


Abbildung 2.13: *Paketübertragung im RLC Acknowledge-Modus. [Bar07, Seite 35]*

Weiterhin ist RLC für die Quittierung beziehungsweise die Neuanforderung von fehlerhaft übertragenen Paketen zuständig. Hierfür sind drei Übertragungsmodi spezifiziert. Der *Acknowledged Mode* bildet die von TCP bekannte Datenflusssteuerung ab, wohingegen der *Unacknowledged Mode* dem verbindungslosen Verhalten von UDP entspricht. Im *Transparent Mode* schließlich werden die Pakete nicht weiter verändert. Dieser Modus wird zum Beispiel zur Sprachübertragung verwendet. Im Rahmen dieser Arbeit ist allerdings nur der *Acknowledged Mode* interessant, da sich lediglich hier der im Folgenden besprochene, diskrete IPT-Verlauf ergibt (vgl. diesbezüglich auch [Bar07, Seite 60]).

In Abb. 2.13 ist dargestellt, wie Daten vom Netzwerkcontroller (RNC) zum Endgerät (UE) übertragen werden. Neben der Paketverkapselung sind auch die TTI-Übertragungsfenster zu sehen. Weiterhin wird die Datenflusssteuerung inklusive Neuanforderung eines fehlerhaften Pakets veranschaulicht. Die hier abgebildeten Verarbeitungs- und Laufzeiten werden in Abschnitt 4.1 zur Abschätzung der UMTS-Paketlaufzeiten benötigt.

Wichtig aus diesem Unterkapitel ist das Wissen über die Existenz einer komplexen Systemebene sowie zur Paketbehandlung der Sicherungsschicht. Betrachtet wird im Folgenden nur die Datenübertragung im Acknowledge-Modus. Diese wird wiederum vom vorgestellten TTI beeinflusst, der im Retransmissionsverhalten von UMTS eine wichtige Rolle spielt.

2.4 Eigenschaften der Funkübertragung

Da beide in dieser Arbeit zu vergleichenden Technologien auf der Funkübertragung basieren und diesbezüglich bereits einige Begriffe gefallen sind, soll im Folgenden noch ein kurzer Überblick hierzu – insbesondere hinsichtlich Fehlerquellen, deren Auswirkungen und den entsprechenden Gegenmaßnahmen – gegeben werden.

2.4.1 Rauschen, Dämpfung und Fading

Die Ausbreitung einer elektromagnetischen Welle ist grundsätzlich wellenlängen- und frequenzabhängig (siehe [Bar07, Seite 18 ff.]). Die maximale Reichweite einer Funkübertragung wird neben der eigentlichen Wellenausbreitung auch von der Sendeleistung und der Empfängerempfindlichkeit sowie von der Umwelt beeinflusst.

a) Rauschen

Das Rauschen stellt meistens die größte Störquelle dar (vgl. [Kla10, Seite 220 f.]). Als Hauptindikator für die Signalqualität wird daher das *Signal-Rausch-Verhältnis* verwendet. Rauschen tritt im gesamten Übertragungssystem auf, wobei man zwischen inneren und äußeren Rauschquellen unterscheidet. Einen großen Einfluss hat das *thermische Rauschen*, welches sowohl als Hintergrundrauschen der Atmosphäre als auch als Widerstandsrauschen in elektrischen Leitern auftritt. Dieses Wärmerauschen setzt sich überwiegend aus dem sogenannten *weißen Rauschen* zusammen. Das entsprechende Kanalmodell wird daher auch als *additives weißes gaußsches Rauschen* (engl. kurz *AWGN*) bezeichnet. Es spielt eine wichtige Rolle in der Simulation von Übertragungskanälen, bildet dabei aber viele Effekte der Funkübertragung – wie das im Folgenden beschriebene Fading – nicht ab.

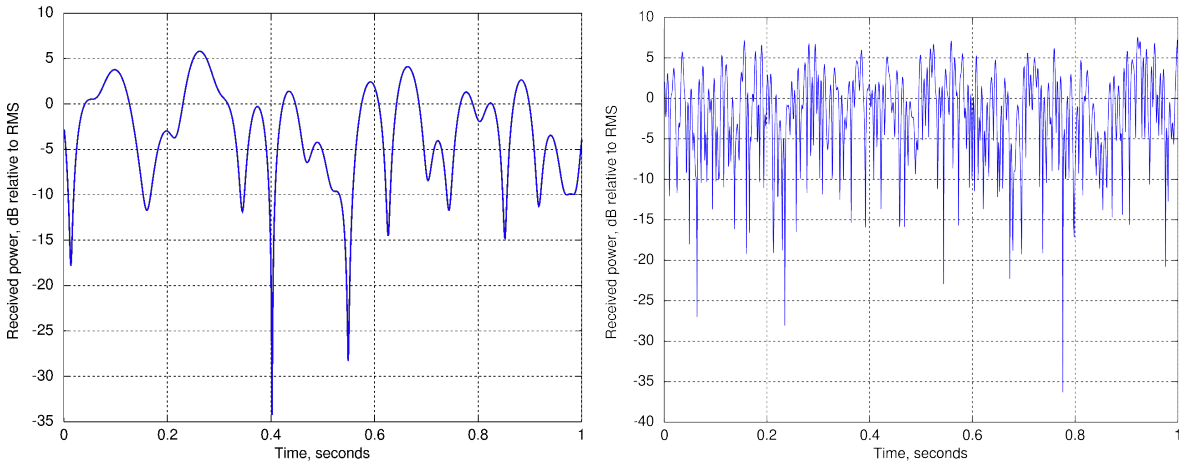
b) Freiraumdämpfung

Einen wichtigen Einfluss auf ein ansonsten ungestörtes Signal hat weiterhin die sogenannte *Freiraumdämpfung*. Diese hat ihre Ursache in der kugelförmigen Ausbreitung elektromagnetischer Wellen. Gemäß des Abstandsgesetzes kommt es so auch ohne weitere Störeinflüsse zu einer Reduzierung der Leistungsdichte und somit zu einer Dämpfung des Nutzsignals.

c) Fading

Da eine Funkübertragung meist nicht im luftleeren Raum stattfindet, müssen weitere Einflüsse berücksichtigt werden. Als Schwund (engl. *Fading*) bezeichnet man in diesem

Zusammenhang Effekte, die sich durch *Abschattung*, *Interferenz*, *Mehrwegeausbreitung* und den *Doppler-Effekt* ergeben (siehe auch [Raj07, Seite 4 ff.]). Den offensichtlichsten Effekt stellt dabei die direkte Abschattung, also die komplette *Absorption* der Strahlung durch Hindernisse, dar. Wie Lichtwellen unterliegen auch Funkwellen physikalischen Einflüssen, wenn sie auf Materie treffen. Sie werden reflektiert, gebrochen, gestreut und gebeugt. Kommt ein so beeinflusstes Signal anschließend mehrfach beim Empfänger an, so spricht man von *Mehrwegeempfang*. Auch aufgrund dieser Ausbreitungseffekte kann es zu Wellenüberlagerungen, also *Interferenzen*, kommen. Durch einen relativen Geschwindigkeitsunterschied zwischen Sender und Empfänger kommt es weiterhin zu Frequenzverschiebungen, dem sogenannten *Doppler-Effekt*. Je nach verwendetem Übertragungsverfahren wirken sich diese Effekte dabei unterschiedlich stark aus. Betreffen die Störungen dabei verschiedene Bereiche des Übertragungsbands unterschiedlich stark, spricht man auch von selektivem Trägerschwund.



(a) Doppler-Verschiebung von 10 Hz. [wikimedia.org] (b) Doppler-Verschiebung von 100 Hz. [wikimedia.org]

Abbildung 2.14: *Simuliertes Rayleigh-Fading. (CC BY-SA* Splash*)*

Im Rahmen der Arbeit besonders hervorzuheben ist das sogenannte *Rayleigh*-Fading, ein statistisches Modell, welches speziell zur Simulation der Mehrwegeausbreitung in stark bebauten Bereichen dient (vgl. auch [Kla10, Seite 211 f.]). Wie in Abb. 2.14 anhand der Häufigkeit und Stärke der Pegeleinbrüche zu erkennen ist, spielt hierbei auch die Geschwindigkeit eine wichtige Rolle. Für Szenarien mit direkter Sichtverbindung kann auch das *Rice*-Fadingmodell verwendet werden. Der in Abschnitt 3.2 vorgestellte und im Rahmen der Messungen verwendete Kanalemulator unterstützt beide Fading-Modelle (siehe [Spi10]).

2.4.2 Modulation, Kodierung und Fehlerarten

Um die Auswirkungen der beschriebenen Effekte zu reduzieren, existieren verschiedene technische Verfahren. Leider genügt es meist nicht, nur die Empfindlichkeit des Empfängers zu erhöhen. Neben der Modulation spielt auch die Kodierung eine wichtige Rolle.

a) Modulationsverfahren

Im Laufe der historischen Entwicklung wurden analoge von digitalen Verfahren abgelöst und im Bereich der Funkübertragung setzt sich zunehmend die Modulation mit mehreren Trägern – wie die bei 802.11n verwendete OFDM – durch (siehe auch [Kla10, Seite 136]). Diese hat den Vorteil, dass die Auswahl der genutzten Frequenzen an die Übertragungseigenschaften des jeweiligen Kanals angepasst werden kann. In Kombination mit möglichst schmalbandigen Trägern führt dies zu einer verbesserten Störsicherheit. Einen ähnlichen Ansatz verfolgt die sogenannte *Frequenzspreizung*, bei der ein wesentlich größerer Frequenzbereich genutzt wird als er eigentlich zur Übertragung benötigt würde. Auch dies führt zu einer größeren Robustheit gegenüber schmalbandigen Störungen. Als konkretes Beispiel für eine solche Implementierung sei das bei UMTS eingesetzte WCDMA-Spreizbandverfahren genannt.

b) Kodierungsverfahren

Als weitere Möglichkeit zum Schutz gegen Übertragungsfehler bietet sich das Hinzufügen von Redundanz mittels entsprechender Kanalkodierung an. Durch den Einsatz von Kodierungsverfahren können Fehler erkannt und gegebenenfalls auch korrigiert werden. Sowohl WLAN als auch UMTS setzen hierbei in erster Linie auf sogenannte *Faltungscodes* (vgl. [Kla10, Seite 140 ff.]). Wobei im 802.11n-Standard zusätzliche *Low-Density-Parity-Check-Codes* spezifiziert sind und bei UMTS auch sogenannte *Turbo-Codes* zum Einsatz kommen können.

c) Fehlerarten

Aufgrund der genannten Verfahren ergeben sich aus Störungen – durch Rauschen, Kurzzeitstörungen oder Signalverformungen und abhängig von den jeweiligen Kanaleigenschaften – sogenannte *Einzelbit-* beziehungsweise *Blockfehler* (vgl. auch [Bar07, Seite 33 ff.]). Die Häufigkeit beziehungsweise Wahrscheinlichkeit dieser Fehler ist ein wichtiges Maß für die Qualität der Übertragung. Aufgrund des gehäuften Auftretens der Blockfehler werden sie auch als *Bündel-* oder *Burstfehler* bezeichnet. Kommt es zusätzlich zum Verlust des physikalischen Übertragungsrahmens, spricht man auch von *Synchronisationsfehlern*.

Zur automatischen Sendewiederholung im Fehlerfall kommen hierbei oft *ARQ*-Protokolle zum Einsatz. Dadurch, dass der Empfänger das Resultat der Fehlererkennung an den Sender zurückgibt, kann dieser nötigenfalls einen Paketwiederholungsvorgang anstoßen. Sowohl WLAN als auch UMTS verwenden diesbezüglich jeweils spezielle `ACK`-Pakete zur Empfangsbestätigung. Kommt keine oder eine negative Bestätigung für das Paket zurück, wird von einem Übertragungsfehler ausgegangen und eine Retransmission eingeleitet.

Durch physikalische Effekte kommt es also zu Störungen der Funkübertragung, die – falls sie nicht mit entsprechenden Modulations- und Kodierungsverfahren kompensiert werden können – zu Übertragungsfehlern führen. Sowohl WLAN als auch UMTS nutzen daher solche Modulierungsverfahren, die insbesondere schmalbandige Störimpulse gut kompensieren können. Bei beiden Techniken findet zusätzlich eine entsprechende Bitfehlerkorrektur statt. Zur Erkennung von irreparabelen Blockfehlern kommen CRC-Prüfsummen zum Einsatz. Je nach Standard und Implementierung werden fehlerhafte Pakete anschließend entweder verworfen oder erneut angefordert, was zu einer entsprechenden Paketverzögerung führt. Da diese Arbeit die IPTs auf der IP-Ebene zur Klassifikation des Übertragungskanals verwendet, werden im Folgenden ausschließlich Sendewiederholungsverfahren verglichen.

Wie am Anfang dieses Kapitels erarbeitet, lassen sich die hier vorgestellten Eigenschaften des Übertragungskanals statistisch auf Paketeigenschaften höherer Netzwerkebenen abbilden. Um das entsprechende Kanalverhalten von WLAN und UMTS abschätzen und geeignete Versuche entwickeln zu können, müssen hierbei die Einflüsse der unteren Schichten bekannt sein. Weiterhin ist ein grundlegendes Verständnis der jeweiligen Netzinfrastruktur und der geeigneten Störszenarien erforderlich. Mithilfe entsprechender Modelle – wie AWGN-Rauschen oder Rayleigh-Fading – lassen sich physikalische Störungen im Labor nachbilden. Somit können die Auswirkungen dieser auf die zu untersuchenden Übertragungsverfahren erforscht werden. Im nun folgenden Kapitel wird auf diesen Grundlagen aufbauend ein Konzept entwickelt und ein entsprechender Messaufbau implementiert.

3 Konzept und Umsetzung der Messungen

Dieses Kapitel beschäftigt sich mit den im Rahmen dieser Arbeit durchgeführten Messungen. Dazu wird das grundlegende Konzept des Messaufbaus erarbeitet sowie die dort verwendete Hard- und Software vorgestellt. Zur Veranschaulichung des Ganzen wird anschließend eine entsprechende Messung exemplarisch nachvollzogen.

3.1 Planung des grundlegenden Messaufbaus

Wie bereits in Kapitel 2 erwähnt, soll die Inter-Packet Time zur Kanalcharakterisierung verwendet werden. Voraussetzung hierfür ist eine zeitlich möglichst konstante Paketquelle auf der Sendeseite und eine vergleichbar hochauflösende Paketaufzeichnung auf der Empfangsseite. Des Weiteren muss eine angemessen konfigurierbare Teststrecke aufgebaut werden. Hierfür gilt es geeignete Störszenarien zu entwickeln und umzusetzen. Die bezüglich dieses Teilaspekts durchgeführte Erarbeitung eines Konzepts wird nun genauer erläutert.

3.1.1 MobQoS-Messaufbau

Aufgrund der Tatsache, dass die neuen Messungen mit den bereits bestehenden Ergebnissen vergleichbar bleiben sollen, orientiert sich der grundlegende Versuchsaufbau am – in Abb. 3.1 illustrierten – Konzept aus dem *MobQoS*-Projekt.

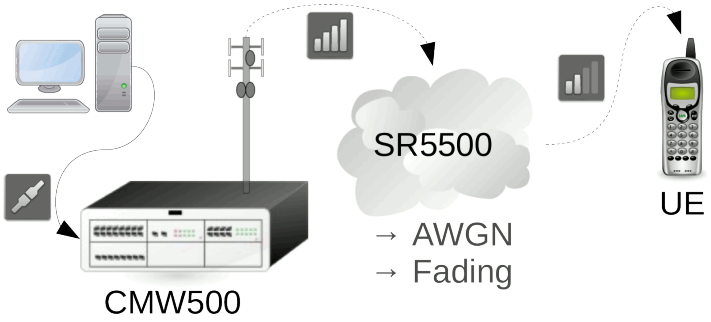


Abbildung 3.1: *Veranschaulichung des grundlegenden UMTS-Messaufbaus.*

Die Anordnung muss hierbei die vorgestellte UMTS-Netztopologie abbilden und gleichzeitig die erwähnten Störszenarien umsetzen können. Zur Simulation des UMTS-Netzes dient das *CMW500*-Testgerät. Der *SR5500* emuliert den Übertragungskanal. Die Einspeisung von Testpaketen erfolgt über eine Ethernetverbindung. Für die Verkabelung zwischen den Instrumenten werden koaxiale Hochfrequenzkabel und Leistungsteiler verwendet.

Zur Beurteilung des Übertragungsverhaltens werden – wie in Abschnitt 2.1 besprochen – IP-Pakete aus einer zeitlich konstanten Quelle verwendet. Die von einem eigens entwickelten Paketgenerator erzeugten UDP-Pakete werden über den *CMW500* in das simulierte Funknetzwerk eingespeist und sind an das dort angemeldete Endgerät adressiert. Der vom *SR5500* gestörte Übertragungskanal wirkt sich schließlich so auf die Paketübertragung aus, dass sich die Störung anschließend anhand der IP-Parameter am Empfänger charakterisieren lässt. Das wichtigste Maß hierfür stellt die Verteilung der Inter-Packet Times am Empfänger dar. Um zusätzliche Informationen aus dem *CMW500* – wie die Paketverlustrate oder Details zum Protokollablauf – ergänzt, erlaubt sie eine Klassifizierung des Übertragungskanals.

Je nach simuliertem Szenario müssen die Einstellungen am *CMW500* beziehungsweise am *SR5500* angepasst werden. Aufgrund der speziellen Eigenschaften des UMTS-Kanals stehen hier in erster Linie RLC-Optionen sowie die Störung durch Rauschen und Fading im Vordergrund. Weiterhin spielen auch die einstellbaren IP-Parameter – vor allem die Paketgröße und die IPT am Sender – eine wichtige Rolle bei der Modellbildung.

3.1.2 NetQoS-Messaufbau

WLAN-Netzwerke unterliegen jedoch teilweise andersartigen Störeinflüssen als sie bei der UMTS-Übertragung im Vordergrund stehen. Da sich dadurch grundlegende Auswirkungen auf den Messaufbau ergeben können, sollen diese nun kurz vorgestellt und bewertet werden.

a) WLAN-Szenarien

Wie in Abschnitt 2.2 herausgearbeitet, ist WLAN inhärent anfällig für Paketkollisionen und verwendet im 2,4 GHz-Bereich Frequenzen aus dem ISM-Band. Anders als im Mobilfunk ist dieser Frequenzbereich nicht reguliert und zur Nutzung benötigt man daher lediglich eine allgemeine Zulassung der Frequenzverwaltungsstelle (siehe [Mar13, Seite 298 f.]). Somit ergibt sich eine erhöhte Anfälligkeit für Störungen durch WLAN-eigene und WLAN-fremde Funkübertragungen. Dies führt dazu, dass Interferenzen bei WLAN eine größere Rolle spielen als bei UMTS. Als Störquellen kommen hierbei in erster Linie andere WLAN-Netze und sonstige Hochfrequenz-Anwendungen in Frage. Durch die nicht überlappungsfreien Kanäle ergeben sich weiterhin unterschiedlich starke Störszenarien für die WLAN-Interferenzen. Störungen von anderen Geräten können beispielsweise durch Bluetooth oder durch den Betrieb von Mikrowellenherden entstehen.[16]

[16] vgl. auch `https://en.wikipedia.org/wiki/Electromagnetic_interference_at_2.4_GHz`

Aber auch WLAN unterliegt natürlich solchen Störungen, wie sie durch Fading hervorgerufen werden. Bei der Auswahl von geeigneten Fading-Modellen muss allerdings berücksichtigt werden, dass WLAN meistens nur innerhalb von Gebäuden, in statischen Netzen und bei einer niedrigeren relativen Geschwindigkeit zwischen Sender und Empfänger genutzt wird. Auch ist die durchschnittliche Größe eines WLAN-Netzes nicht mit einer UMTS-Zelle vergleichbar.

Aufgrund der Tatsache, dass ein Standard nur die Rahmenbedingungen für eine Technik liefert und die jeweilige Implementierung Aufgabe der Hersteller ist, müssen selbstverständlich auch diesbezügliche Einflüsse untersucht werden. Insbesondere wegen den – im Vergleich zu UMTS – kurzen Umlaufzeiten ist im WLAN-Netzwerk mit implementierungsspezifischen Auswirkungen auf die Messungen zu rechnen. Daher sind unbedingt verschiedene Hardware-Implementierungen miteinander zu vergleichen. Darüber hinaus sollen auch treiber- beziehungsweise konfigurationsspezifische Einflüsse berücksichtigt werden.

	Quelle	**Einflüsse auf der Messstrecke**	**Senke**
UMTS	*CMW500*	Rauschen und Fading (*SR5500*)	UMTS-Stick
WLAN	APs	Implementierung/Interferenzen/Fading	STAs

Tabelle 3: *Direkter Vergleich zwischen dem UMTS- und WLAN-Messkonzept.*

Insgesamt ergeben sich also neue Störszenarien, die es in der Testumgebung zu berücksichtigen gilt. Daher reicht es nicht aus, lediglich die Quelle und Senke im Messaufbau auszutauschen. Wie in Tab. 3 zusammengefasst, werden zu den bisher berücksichtigten Störungen durch Fadingeffekte Interferenzen hinzugefügt. Weiterhin soll speziell auch der Einfluss verschiedener Hardwareimplementierungen und weiterer Optionen untersucht werden.

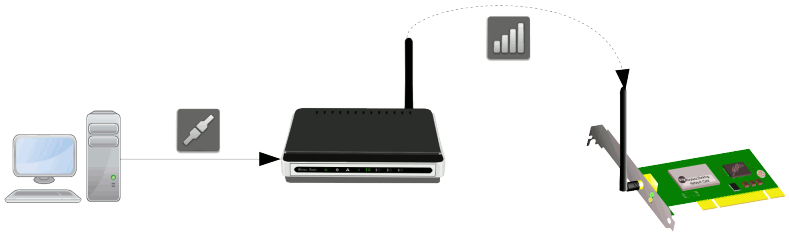


Abbildung 3.2: *Direkte und ungestörte Messanordnung.*

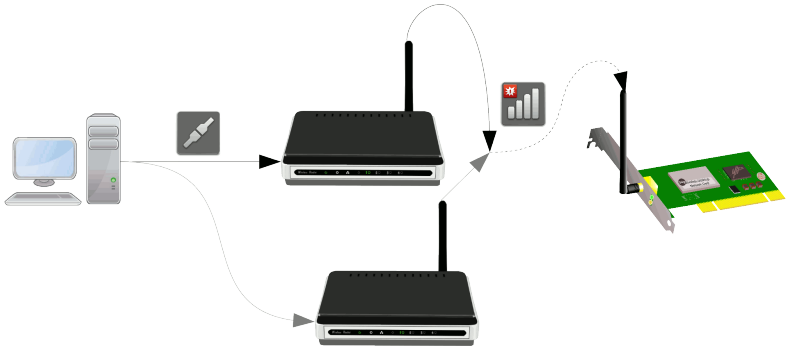


Abbildung 3.3: *Einfacher Aufbau zur WLAN-Interferenzmessung.*

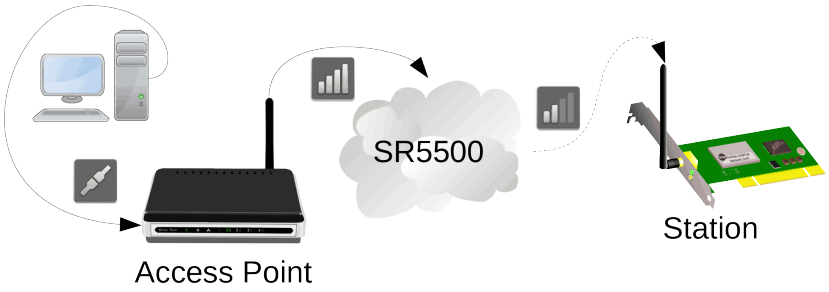


Abbildung 3.4: *Messanordnung mit Kanalemulator zur Fadingmessung.*

b) Entsprechender Versuchsaufbau

Für erste Vergleichsmessungen und zur Auswertung der einzelnen Implementierungs- und Standardeinflüsse wird eine ungestörte Anordnung verwendet. Diese ist in Abb. 3.2 dargestellt und umfasst einen per Ethernet angeschlossenen Access Point sowie eine direkt damit verkabelte Station. Der Aufbau ermöglicht es, sowohl ein Grundverständnis für die störungsfreien WLAN-Übertragung zu entwickeln als auch unterschiedliche Hardware – wie zum Beispiel verschiedene PCIe-Karten und USB-Sticks – miteinander zu vergleichen. Des Weiteren lassen sich die Auswirkungen standardspezifischer Optionen genauer untersuchen.

Zur Untersuchung der WLAN-Interferenzen wird anschließend ein weiterer Access Point mit in den Versuchsaufbau eingebracht. Dieser Aufbau ist in Abb. 3.3 visualisiert. Je nach Konfiguration des verwendeten APs können dabei sowohl vollständige als auch teilweise Frequenzüberlappungen mit unterschiedlicher Kanalauslastung getestet werden. Zur Entkoppelung der Empfangshardware bietet sich die Verwendung einer zusätzlichen STA an.

Um abschließend auch das Fading-Verhalten zu untersuchen, wird die – in Abb. 3.4 dargestellte – Anordnung verwendet. Prinzipiell entspricht diese dem bereits vorgestellten *MobQoS*-Messaufbau. Hauptunterschied zu den UMTS-Messungen ist, dass der *CMW500* durch einen Access Point ausgetauscht ist. Und da der Antennenanschluss am AP (im Gegensatz zum *CMW500*) keine Kanaltrennung erlaubt, wird im WLAN-Aufbau sowohl der Up- als auch der Downlink gestört. Hierfür müssen beide Kanäle des *SR5500* verwendet werden und die Kabelverbindung ist mittels Leistungsteiler beidseitig aufzuteilen.

Obwohl sich das grundlegende Konzept des Versuchsaufbaus nicht erheblich von den Messungen aus den *MobQoS*-Projekt unterscheidet, müssen dennoch Besonderheiten der jeweilig zu testenden Übertragungstechnologie berücksichtigt werden. Als nächstes werden die zum Aufbau der eben konzeptionierten Messstrecken nötigen Teile vorgestellt.

3.2 Verwendete Hardwarekomponenten

Zur Umsetzung des besprochenen Versuchaufbaus werden verschiedene Komponenten verwendet. Im Weiteren sollen neben der PC- und HF-Technik insbesondere die verwendeten WLAN-Komponenten sowie die bereits angesprochene Messtechnik vorgestellt werden.

3.2.1 PC-Technik

Sowohl zur Datenerzeugung als auch zur Datenverarbeitung werden handelsübliche *Fujitsu Esprimo*-Arbeitsplatzrechner verwendet. Diese verfügen über einen Quad-Core-Prozessor mit 2,8 GHz Taktrate und 4 GB Arbeitsspeicher. Die Verbindung zwischen Computer und Testgerät erfolgt via Gigabit-Ethernet auf der einen und mittels entsprechender HF-Hardware auf der anderen Seite.

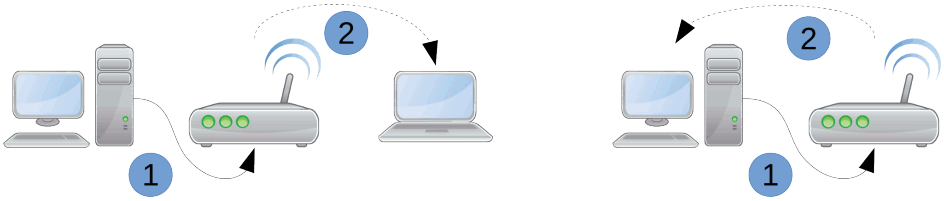


Abbildung 3.5: *Vergleich zwischen alter und neuer, vereinfachter Testanordnung.*

Der ursprüngliche *MobQoS*-Messaufbau verwendet zwei Rechner. Aufgrund komplexerer Anpassungen am Betriebssystem der PCs und zur Harmonisierung des Datenaustausches wird dieser Aufbau vereinfacht. Wie in Abb. 3.5 zu sehen ist, wird das ursprüngliche Verfahren – bei dem je ein Rechner als Quelle (①) und einer als Senke (②) dient – durch die Verwendung eines einzigen Computers vereinfacht. Die Verifikation der neuen Anordnung ergibt, dass weder der einfache Aufbau noch die zum Vergleich verwendete Ethernetverbindung einen messbaren Einfluss auf die IPT-Charakteristik haben (siehe hierzu auch Abschnitt 4.2).

Als Betriebssystem auf den Testrechnern kommt die Linux-Distribution *Debian 7.6* (Codename *Wheezy*) zum Einsatz. Die besonderen Anpassungen am System und die eingesetzte Software werden in Abschnitt 3.3 noch genauer beschrieben. Des Weiteren ist eine ausführliche Dokumentation zum gesamten Versuchsaufbau in Anhang A hinterlegt.

3.2.2 HF-Technik

Zur Realisierung der beschriebenen Messstrecke müssen entsprechende Verbindungselemente eingesetzt werden. Die hierfür verwendete Technik umfasst folgende Bestandteile:

- **Verkabelung:** Koaxialkabel mit *RP-SMA* und *N*-Steckverbindern[17]
- **Verzweigung:** Leistungsteiler *Inmet 6007-02* und *HP 11667A*
- **Überprüfung:** Spektrumanalysator *FSH3* von *Rohde&Schwarz*

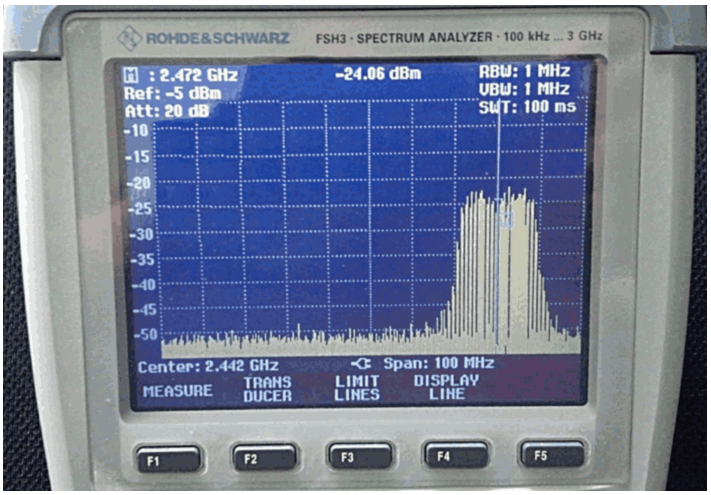


Abbildung 3.6: *OFDM-moduliertes WLAN-Signal im Spectrum Analyzer.*

Durch den zweckmäßigen Einsatz von Kabeln und Adaptern können die beschriebenen Versuchsszenarien umgesetzt werden. Hierbei gilt es aber immer zu beachten, dass der entsprechende Aufbau hochfrequenztechnisch korrekt implementiert ist. Beispielsweise können zur Verzweigung eingesetzte T-Stücke unerwünschte Reflexionen hervorrufen. Aus diesem Grund finden hierfür ausschließlich speziell abgeschlossene Leistungsteiler Verwendung. Um den Versuch auf unerwünschte Effekte zu überprüfen, kommt der *Spectrum Analyzer* zum Einsatz. Eine entsprechende Messung wird in Abb. 3.6 gezeigt. Dort sind Einzelträger des OFDM-Signals zu erkennen, mögliche Störungen sind im dargestellten Frequenzbereich nicht zu beobachten. Da der Messbereich des Analysators aber auf unter 3 GHz beschränkt ist, können die 5 GHz-Versuche nicht überprüft werden (vgl. diesbezüglich [Roh07]).

[17] vgl. `https://de.wikipedia.org/wiki/Koaxiale_Steckverbinder_f%C3%BCr_Hochfrequenzanwendungen`

3.2.3 WLAN-Hardware

Um die Herstellerabhängigkeit der Übertragungscharakteristik zu untersuchen, werden im Messaufbau mehrere, unterschiedliche Komponenten eingesetzt. Diese sind in Tab. 4 – inklusive der jeweils verbauten Chipsätze und der wichtigsten Funktionen – aufgelistet.

	Bezeichnung	**Chipsatz**	**Funktionsumfang**
AP	*HP-MSM466* (J9622A)	AR9390	Dualband, 2x3 Anschlüsse
	TL-WDR3600	AR9344/AR9582	Dualband, zwei Anschlüsse
	TL-WA701ND	AR9285	nur 2,4 GHz und ein Anschluss
	TL-WA730RE	AR9331	nur 2,4 GHz und ein Anschluss
PCIe	*TL-WDN3800*	AR9382	Dualband, zwei Anschlüsse
	Asus PCE-N10	RTL8188CE	nur 2,4 GHz und ein Anschluss
USB	*TL-WN722N*	Atheros AR9271	nur 2,4 GHz und ein Anschluss
	AVM Fritz!WLAN Stick N	AR9170/AR9104	Dualband, kein Anschluss
	Trendnet TEW-664UB	RT2870/RT2850	Dualband, kein Anschluss

Tabelle 4: *Im Rahmen der Arbeit verwendete WLAN-Komponenten.*[18]
HP *steht für den Hardwarehersteller* Hewlett-Packard *und* TL *für* TP-LINK.
Bei den Chips steht AR *für* Atheros, *RTL für* Realtek *und* RL *für* Ralink.

Bei der Beschaffung der WLAN-Hardware wird darauf geachtet, dass diese besonders für den Messaufbau geeignet ist. Hierzu gehört – neben einer ausreichenden Treiber-Unterstützung für Linux – in erster Linie das Vorhandensein externer Antennenanschlüsse. Weiterhin sollten möglichst beide von 802.11n spezifizierten Frequenzbereiche unterstützt werden. Da aber die Auswahl solcher Komponenten beschränkt ist, wird letztendlich auch Hardware verwendet, die diesen Kriterien nicht vollständig entspricht. Lediglich die 802.11n-Unterstützung wird immer als zwingend notwendig vorausgesetzt.

Für den Hardwarevergleich ist außerdem zu beachten, dass auch die Chipsätze der Access Points per PCI-Express angebunden sind. Mit USB ergeben sich somit zwei verwendete Bussysteme, die nun kurz bezüglich möglicher Messeinflüsse bewertet werden. Bei *PCI-Express* handelt es sich – im Gegensatz zum parallelen PCI – um separate, serielle Punkt-zu-Punkt-Verbindungen. Dabei ist PCIe vollduplexfähig und arbeitet mit mindestens 250 MByte/s

[18] siehe bezüglich der Chipsatzinformationen auch `https://wikidevi.com`

pro Lane.[19] Trotz der theoretisch hohen Brutto-Datenrate von 802.11n im MIMO-Betrieb ergibt sich praktisch nur eine Durchsatzrate von höchstens 260 Mbit/s (siehe [LAN09]). Dies entspricht 32,5 MByte/s und kann somit vom PCIe-Bus leicht bedient werden. Weiterhin wird kein Ansatz gefunden, das Datenübertragungsverfahren des Busses auf das in den Messungen beobachtete Verhalten zurückzuführen (vgl. auch [PCI02, Seite 383]). Interessanter ist hier der *Universal Serial Bus* (*USB*). Beim von der Testhardware genutzten *USB 2.0* liegt zwar die Datenrate bei insgesamt 60 MByte/s, doch die Einteilung in *Micro-Frames*[20] zu je 125 μs wird in den Messungen sichtbar (siehe auch [Mic07]). Da Bussysteme nicht Thema der Arbeit sind, sind detailliertere Informationen weiterführender Literatur zu entnehmen.

3.2.4 Weitere Messtechnik

Um den Funkkanal beziehungsweise das UMTS-Netzwerk nachzubilden, werden auch zwei industrielle Testinstrumente verwendet, die nun noch kurz vorgestellt werden.

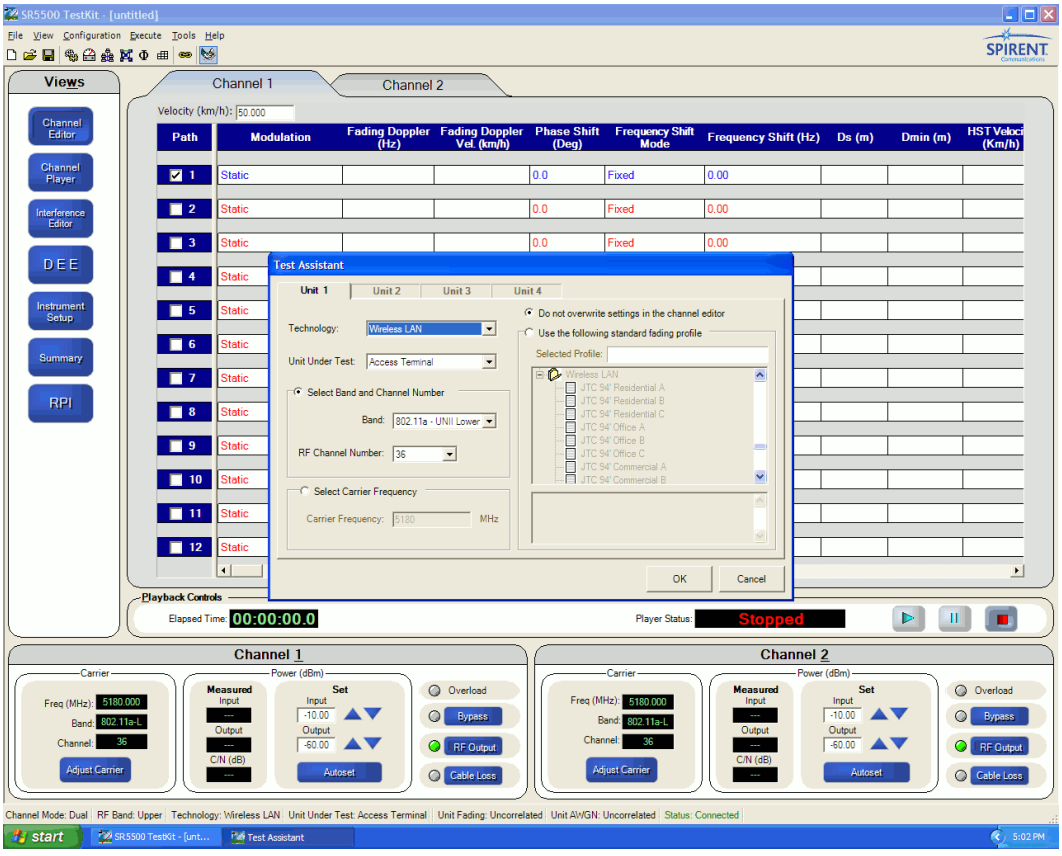


Abbildung 3.7: *Test Assistent zur Konfiguration des Fadings im SR5500.*

[19] Quelle: `https://www.pcisig.com/news_room/faqs/pcie3.0_faq/#EQ3` (aufgerufen am 06.10.2014)
[20] Quelle: `http://wiki.osdev.org/Universal_Serial_Bus` (vom 15.08.2013, aufgerufen am 08.10.2014)

a) SR5500

Der *Wireless Channel Emulator* von *Spirent Communications* wird im Messaufbau dazu verwendet, die Funkkanalstörungen im Versuchsaufbau abzubilden. Neben additivem Rauschen kann dieses Gerät auch den Echtzeitschwund für verschiedene Übertragungsstandards umsetzen (vgl. [Spi10]). Für WLAN kann hierbei das *JTC '94 Indoor Channel Model* verwendet werden. Dieses Fadingmodel setzt drei grundlegende Szenarien um, die die Signalausbreitung im Innenbereich von Gebäuden simulieren (siehe auch [Int01, Seite 3]). Für jedes Szenario gibt es je drei Profile, die jeweils verschiedene Laufwege mit unterschiedlichen Verzögerungen und Dämpfungen realisieren. Speziell für den Einsatz im 5 GHz-Bereich benötigt der Kanalemulator die zusätzliche *6-GHz-EX option*. In Abb. 3.7 ist die Konfiguration des *SR5500* zu sehen. Hier sind auch die eben angesprochenen WLAN-Fadingmodelle zu erkennen. Der Screenshot zeigt dabei den Einsatz bei 5 GHz. Als Übertragungsband ist daher *802.11a* ausgewählt. Für Messungen im 2,4 GHz-Bereich ist dementsprechend das *g*-Band zu verwenden.

b) CMW500

Der *Wideband Radio Communication Tester* von *Rohde&Schwarz* dient im beschriebenen Messaufbau zur Emulation des UMTS-Netzes. Je nach installierter Lizenz können weitere Technologien – wie beispielsweise auch WLAN – getestet werden. Aufgrund der Tatsache, dass die Beschaffung der entsprechenden Lizenzen – im Gegensatz zur Verwendung eigener Access Points – zu teuer ist, wird der *CMW500* aber nur für UMTS eingesetzt. Hier ermöglicht er die Nachbildung des Kern- und Zugangsnetzwerks im Labor und erlaubt des Weiteren die Paketeinspeisung, wie sie im Rahmen der Arbeit benötigt wird. Speziell die Auswertungsmöglichkeiten des Protokollablaufs und die Darstellung der Blockfehlerwahrscheinlichkeit spielen bei der bisherigen *MobQoS*-Modellbildung eine wichtige Rolle (vgl. [Bar07, Seite 37 f.]). Als Ersatz hierfür wird bei den WLAN-Messungen *Wireshark* im *Monitor Mode* eingesetzt (siehe nächster Abschnitt).

Neben den vorgestellten Geräten zur Umsetzung und Überprüfung der Messstrecke werden also auch spezielle Testinstrumente eingesetzt. Alternativ zu den beiden Kanalemulatoren kann auch ein *CMU200* mit einem *SMIQ* Signalgenerator gekoppelt werden. Diese Konfiguration wurde für die ursprünglichen Beobachtungen zu UMTS verwendet und erst später durch den hier beschriebenen *MobQoS*-Messaufbau ersetzt (siehe hierzu [Bar07, Seite 57 ff.]).

3.3 Genutzte Software

Zur Paketerzeugung, Teststreckenkonfiguration, Datengewinnung und Datenverarbeitung werden unterschiedliche Programme eingesetzt. Diese werden nun in der genannten Reihenfolge vorgestellt und besprochen. Eine ausführlichere Dokumentation sowie die entsprechenden Quelltexte sind dabei in Anhang A hinterlegt.

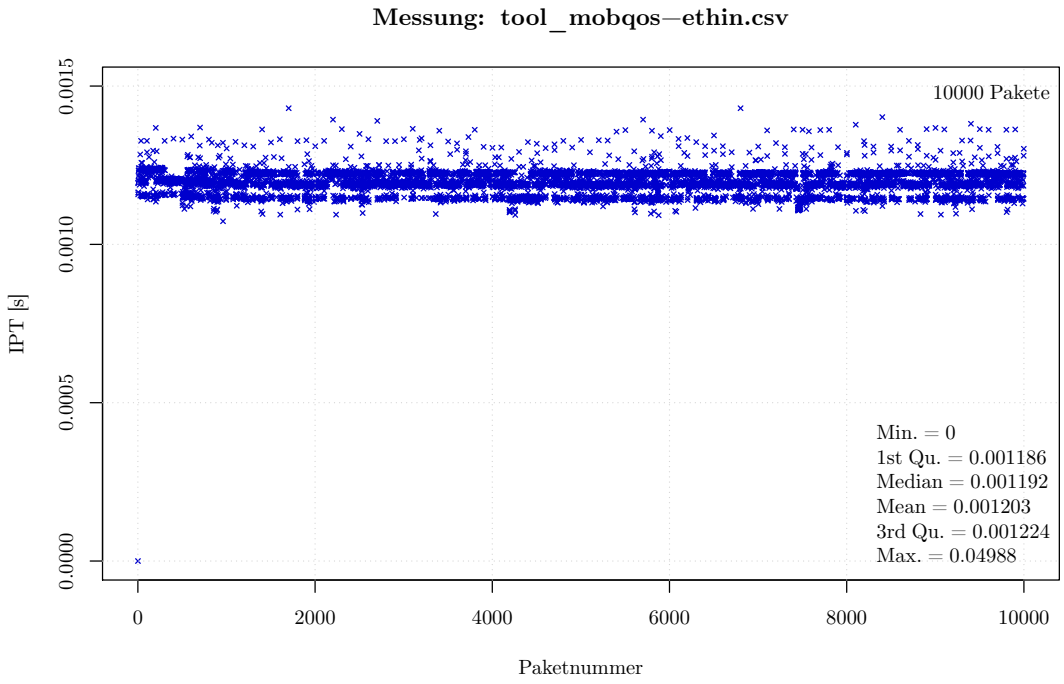
3.3.1 Paketerzeugung

Bei den *MobQoS*-Forschungen kamen insgesamt mehrere, eigens entwickelte Paketquellen zum Einsatz. Allen gemein ist, dass UDP-Pakete mit einem zeitlich konstanten Abstand erzeugt und versendet werden. Zur ursprünglichen Charakterisierung der UMTS-Übertragung wurde hierzu ein Perl-Skripts verwendet (vgl. [Bar07, Seite 97]). Im Rahmen des *NetQoS*-Projekts wird anfänglich der sogenannte *MobQoS-Client* – eine Java-Anwendung aus dem Vorgängerprojekt – eingesetzt. Neben der Paketerzeugung kann dieses spezielle Programm auch als Senke und zur HMM-Modellbildung verwendet werden. Leider hat das Programm Genauigkeitsprobleme im – in dieser Arbeit für die WLAN-Messungen verwendeten – unteren Millisekundenbereich. Aus diesem Grund wird ein neuer Paketgenerator entwickelt, welcher im Folgenden vorgestellt wird.

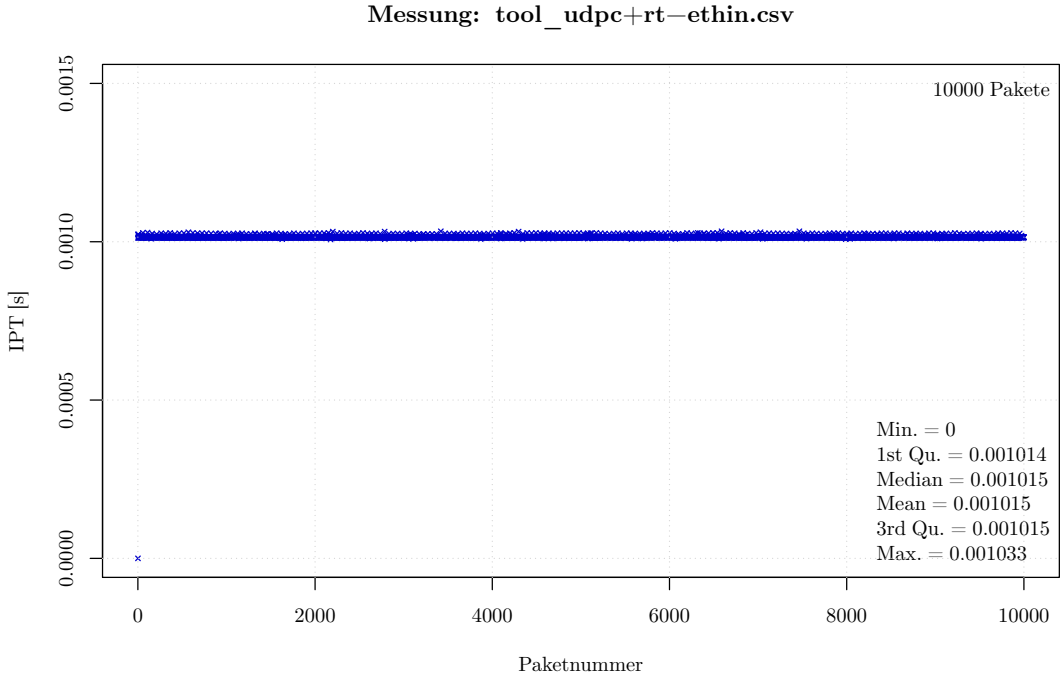
a) udp.c-Paketquelle

Um eine möglichst hohe zeitliche Auflösung gewährleisten zu können, setzt diese in *C* geschriebene Paketquelle verschiedene Prämissen der Echtzeitprogrammierung um.[21] Als Kommandozeilenanwendung prüft das Programm erst die Nutzereingabe und die Betriebsumgebung bevor es entsprechende UDP-Pakete versendet. Der Systemcheck beinhaltet dabei die Prüfung auf einen echtzeitfähigen Linux-Kernel und auf den vom Betriebssystem verwendeten Zeitgeber (engl. *clock source*, siehe unten). Weiterhin wird abgefragt, ob die dynamische Prozessortaktung deaktivert ist und ob gegebenenfalls kritische Module geladen sind. Erst anschließend wird der Prozess auf eine CPU beschränkt, das eigentliche *Real-Time Scheduling* aktiviert und der allokierte Speicher gesperrt. Durch all diese Maßnahmen werden mögliche Störungen im Prozessablauf unterbunden. Das Versenden der Testpakete erfolgt schließlich in einer `while`-Schleife und ist mithilfe der `clock_nanosleep()`-Funktion getimed.

[21] vgl. auch `http://alpha-supernova.dev.filibeto.org/lib/rel/4.0D/APS33DTE/TOC.HTM`



(a) IPT-Verteilung des *MobQoS-Client* aus dem Vorgängerprojekt.



(b) IPT-Verteilung des neu entwickelten *udp.c*-Tools.

Abbildung 3.8: *Ethernet-Vergleichsmessung der Paketquellen mit IPTs am Sender.*

Wie in Abb. 3.8 zu sehen ist, kann durch die beschriebenen Maßnahmen sowohl die relative als auch die absolute Genauigkeit der Paketquelle deutlich erhöht werden. Die höhere Auflösung ist insbesondere aufgrund der kürzeren Paketlaufzeiten in WLAN-Netzwerken nötig und ermöglicht zudem auch Verbesserungen bei der UMTS-Kanalcharakterisierung.

Als Übergabeparameter erwartet das kompilierte *udp.c*-Tool neben der Ziel-IP und dem Port auch die Anzahl der zu sendenden Pakete, den Paketabstand sowie die Größe des UDP-Payloads. Die Gesamtgröße des tatsächlich übertragenen Pakets hängt dann – wie bereits in Abschnitt 2.1 erläutert – vom jeweiligen Übertragungsprotokoll-Overhead ab.

b) Echtzeitsystem

Die wichtigste Rolle bei zeitkritischen Anwendungen spielt neben dem verwendeten Betriebssystem die grundlegende Konfiguration des Rechners. Mit der Installation des *PREEMPT_RT*[22]-Kernels `3.2.0-4-rt-amd64` wird das eingesetzte Linux realtime-fähig gemacht. Zusätzliche Anpassungen an den BIOS-Einstellungen und den Bootparametern verbessern das Echtzeitverhalten des Systems weiter. Neben der Deaktivierung der dynamischen Prozessortaktung ist in diesem Zusammenhang vor allem die vom System verwendete Taktquelle[23] zu erwähnen. Allein durch die Wahl des richtigen Zeitgebers verbessert sich bereits das Verhalten des nicht echtzeitfähigen *MobQoS-Client* merklich. Je nach verwendeter Hard- und Software müssen die möglichen Parameter durchprobiert und die entsprechenden Auswirkungen überprüft werden.[24] Durch die Verwendung des einfachen Messaufbaus, bei dem derselbe Rechner als Paketquelle und Senke dient, wird dies vereinfacht.

c) Routing

Gerade der einfache Messaufbau führt jedoch zu einem Problem. Dadurch, dass die Ziel-IP-Adresse und die entsprechende Paketquelle im selben Rechner vereint sind, werden die Testpakete vom Linux-Kernel standardmäßig an der Hardware vorbeigeleitet. Um dieses lokale Routing zu unterbinden, muss die Routingtabelle des Betriebssystems angepasst werden. Hierzu wird ein einfaches Shell-Skript (`_routing-quick.sh`) verwendet. Dieses löscht erst das automatische Routing (mittels `ip route`-Befehl) und biegt anschließend die Adressauflösung mithilfe des *Address Resolution Protocol*s (durch das `arp`-Tool) so um, dass die Pakete vom

[22] vgl. `https://rt.wiki.kernel.org/index.php/Main_Page`

[23] vgl. `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_MRG/2/html/Realtime_Reference_Guide/chap-Realtime_Reference_Guide-Timestamping.html`

[24] Auch diese Anpassungen sind im Rahmen der Projektdokumentation in Anhang A hinterlegt.

System extern weitergegeben werden. Aufgrund der festkodierten Hardwareadressen muss das Skript bei Einsatz alternativer Netzwerkkarten gegebenenfalls manuell angepasst werden. Um die Bedienung dennoch möglichst einfach zu gestalten, enthält das Programm eine simple, kommandozeilenbasierte Benutzerschnittstelle.

3.3.2 Teststreckenkonfiguration

Zur Parametrisierung der Teststrecke müssen die dort genutzten Hardwarekomponenten entsprechend konfiguriert werden. Diesbezüglich wird nun ein kurzer Überblick gegeben.

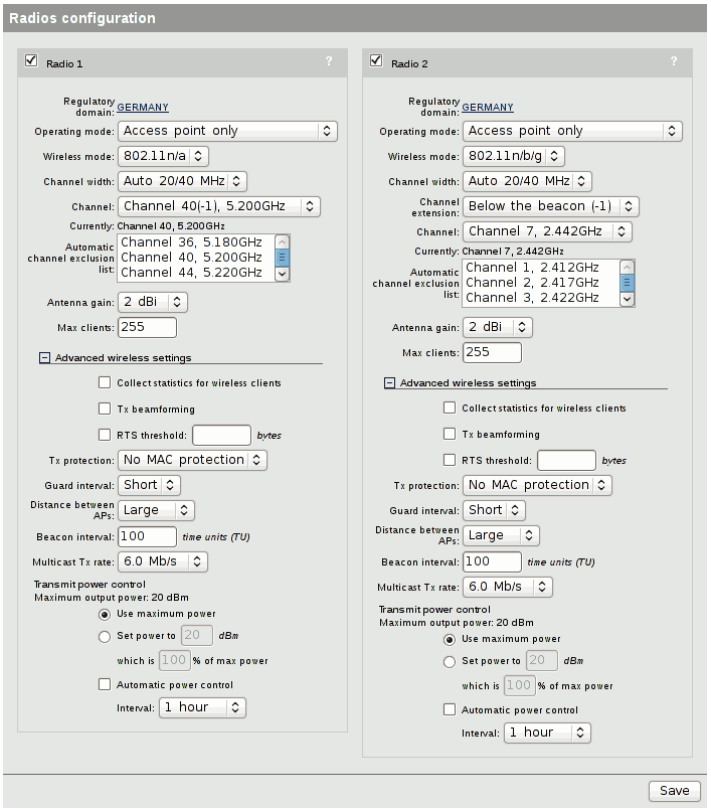


Abbildung 3.9: *Ausschnitt aus der Webkonfiguration des MSM466.*

a) Hewlett-Packard-AP

Da es sich beim *MSM466* um einen Access Point für den professionellen Einsatz handelt, bietet die Webkonfiguration viele Einstellungsmöglichkeiten (siehe auch [Hew11]). Nach der erstmaligen Einrichtung kann hier das Netzwerk und das WLAN grundlegend konfiguriert werden. Neben dem zu verwendenen Standard und Kanal sind auch 802.11n-spezifische

Optionen – wie der Frequenzbereich, die Kanalbreite und die Länge des Guard Intervals – einstellbar. Auch lässt sich das Medienzugriffsverfahren (RTS/CTS), die minimale Datenrate und die maximale Sendeleistung der WLAN-Chips konfigurieren. Weiterhin lassen sich sogar die insgesamt unterstützten MCS-Schemen sowie der verwendete QoS-Mechanismus festgelegen. In Abb. 3.9 sind die entsprechenden WLAN-spezifischen Einstellungsmöglichkeiten der zwei installierten Chipsätze beispielhaft für die Webkonfigurationsoberfläche illustriert.

b) TP-LINK-APs

Weit weniger Auswahl bieten die Konfigurationsoberflächen der *TP-LINK*-Router. Neben grundlegenden Netzwerkeinstellungen kann hier nur der WLAN-Standard, der zu verwendende Kanal und gegebenenfalls noch dessen Breite eingestellt werden. Als Alternative zur derart beschränkten Original-Firmeware bietet sich daher die Verwendung von *OpenWRT* an.

c) OpenWRT-Firmeware

Bei *OpenWRT* handelt es sich um eine spezielle Linux-Distribution für embedded Geräte, insbesondere für Router und Access Points. Bereits die Weboberfläche dieser freien Firmware bietet einen erweiterten Konfigurationsumfang. Ähnlich wie beim *MSM466* lassen sich somit auch beim *WDR3600* die WLAN-Chips einzeln konfigurieren. Auch können die unterstützten MCS-Indizes einschränkt werden, wozu jedoch der direkte Zugriff auf das Betriebssystem nötig ist. Mittels einer SSH-Verbindung können alle unter Linux möglichen und vom Treiber unterstützten Einstellungen[25] umgesetzt werden. Durch den Einsatz von *OpenWRT* und den direkten Zugriff darauf übertrifft der *WDR3600* sogar den professionellen AP bezüglich des konfigurierbaren Funktionsumfangs.

d) SR5500/CMW500

Als industrielle Messtechnik verfügen sowohl der Kanalemulator als auch der Kommunikationstester über eine speziell entwickelte Konfigurationssoftware. Wie bereits in Abb. 3.7 illustriert, ermöglicht diese beispielsweise detaillierte Einstellungen der Störszenarien. Da die hierbei verwendeten Programme relativ komplex sind, wird auf eine ausführliche Darstellung – wie bei den zuvor beschriebenen Geräten – an dieser Stelle verzichtet. Bezüglich der genauen Konfigurationen wird daher auf die Projektdokumentation und weiterführende Literatur verwiesen (vgl. Anhang A und insbesondere auch [Paw14]).

[25] siehe hierzu auch `http://wireless.kernel.org/en/users/Documentation/iw`

3.3.3 Datengewinnung

Auch zur empfangsseitigen Aufzeichnung der Testpakete sowie zum Ermitteln weiterer Informationen werden quellfreie Programme eingesetzt. Im Folgenden wird kurz auf diesbezüglich erwähnenswerte Besonderheiten eingegangen.

a) Linux-Befehle

Für die Gewinnung von Systeminformationen – beispielsweise über den verbauten WLAN-Chipsatz – werden Kommandozeilenwerkzeuge wie `lspci` oder `lsusb` verwendet. Zum Auslesen WLAN-spezifischer Daten kommen Tools des Treiberprojekts *Linux Wireless* zum Einsatz. Beispielhaft genannt sei hier das, auch in *OpenWRT* genutzte, `iw`.

Komplexere Befehlsketten – wie die Anpassung des Routings – werden dabei als Shell-Skripte realisiert und für die spätere Weiterentwicklung ausführlich kommentiert. Informationen zu den Konsolenbefehle können den verwendeten Linux-Manpages[26] entnommen werden.

b) Wireshark

Hauptwerkzeug zur Datenaufzeichnung ist der Paketsniffer *Wireshark*[27]. Dieses Netzwerkanalysetool ist in der Lage, die Netzwerkübertragung auf beliebigen Schnittstellen – wie beispielsweise an der WLAN-Karte – unkompliziert mitzuschneiden und ermöglicht die bequeme Analyse dieser Aufzeichnungen. Hierbei können sowohl bei der Aufnahme als auch bei der Auswertung Filter verwendet werden, um so beispielsweise UDP-Pakete eines speziellen Ports – wie sie im Messaufbau verwendet werden – herauszufiltern. Mittels zusätzlicher Spalten in der tabellarischen Paketansicht lassen sich die IPT, IP-ID und weitere Informationen einfach darstellen und auswerten (vgl. Abb. 3.11 und Abb. 4.11). Weiterhin können die so gewonnenen Paketinformationen gesichert und exportiert werden (siehe auch Abb. 3.10). Die Exportfunktion ermöglicht es dabei, die dargestellte Spaltenansicht in CSV-Dateien zu übertragen. Diese können anschließend weiter ausgewertet und archiviert werden. Für einen tieferen Einstieg in den Funktionsumfang des Programms – insbesondere zum WLAN-Sniffing – sei an dieser Stelle auch auf weiterführende Literatur verwiesen (vgl. [ORB06, Kapitel 6, Seite 267 ff.]).

[26] vgl. `http://manpages.debian.org`

[27] Hauptsächlich genutzte Version: 1.10, vgl. auch `https://www.wireshark.org/`

c) Empfangsmodi

Prinzipiell kennen Paketsniffer zwei Modi zur Datenaufzeichnung. Im sogenannten *Non-Promiscuous Mode* wird nur der tatsächlich an die Netzwerkkarte adressierte Datenverkehr mitgeschnitten, wohingegen der *Promiscuous Mode* alle ankommenden und abgehenden Pakete – also auch solche, die eigentlich für andere Rechner bestimmt sind – aufzeichnet. Speziell bei WLAN gibt es noch den *Monitor Mode*, in dem zusätzlich alle empfangenen WLAN-Frames – auch die anderer Netzwerke und Kanäle – an den Sniffer weiterleitet werden. Da in diesem Modus zusätzliche, WLAN-spezifische Informationen – wie zum Beispiel MCS- und Retry-Daten aus dem Header – verfügbar sind, eignet sich dieser Modus besonders zur Erforschung des Kanalverhaltens und ersetzt somit teilweise die Auswertungsmöglichkeiten des *CMW500*.

3.3.4 Datenverarbeitung

Auch um die gewonnenen Daten anschließend auswerten zu können, werden verschiedene Kommandozeilenprogramme verwendet. Insbesondere wird jedoch ein Skript in der speziell für die Untersuchung statistischer Probleme entwickelten Programmiersprache *R* entwickelt.

a) R-Skript

Die ursprünglich im *MobQoS*-Projekt durchgeführte Verarbeitung der gewonnenen Paketdaten basiert auf der manuellen Auswertung mithilfe von Texteditoren und *Microsoft Excel* sowie verschiedener, kleiner Skripte. Da aber die statistische Aufbereitung größerer Datensätze nicht Aufgabe der Tabellenkalkulation ist, leiden unter diesem Vorgehen sowohl die Benutzerfreundlichkeit als auch die Datenauswertung. Aus diesem Grund wird im *NetQoS*-Projekt auf die im wissenschaftlichen Bereich weit verbreitete, freie Programmiersprache *R*[28] gesetzt.

Speziell zur Auswertung der IPT-Informationen aus den CSV-Datensätzen von *Wireshark* wird ein eigenes R-Skript (hinterlegt in `R-Skript.zip` im Anhang A) erstellt. Hauptaufgabe dieses Programms ist die grafische Aufbereitung der Paketinformationen. Hierzu liest das Skript alle CSV-Dateien innerhalb eines Ordners ein und wertet diese anschließend in der gewünschten Darstellungsform (zum Zeitpunkt der Arbeit implementiert sind: *Indexplot*, *Densityplot*, *Histogram*, *Variation* oder *Phasenplot*) statistisch aus.

Neben einer einfachen Nutzerschnittstelle besteht das Skript in erster Linie aus einer Schleife über alle gefundenen CSV-Dateien. Innerhalb dieser werden die Dateien einzeln eingelesen, deren Format überprüft, gegebenenfalls angepasst und abschließend wird die jeweils gewählte

[28] Im Rahmen der Arbeit genutzte Version: 3.1, siehe auch `http://www.r-project.org/`

Auswertungsform als Grafik gesichert. Neben der *Wireshark*-Aufzeichnungsnummer wird hierbei mindestens noch der Zeitstempel der Pakete vorausgesetzt. Falls nicht mit übergeben, wird daraus die Inter-Packet Time berechnet. Sind zusätzlich die IP-Identifikationsnummern hinterlegt, sucht das Skript automatisch nach Sequenzfehlern und Paketwiederholungen. Somit lassen sich Übertragungsfehler sowie Retransmissionen erkennen und entsprechend darstellen. Alle vorgenommenen Anpassungen werden gesichert und schließlich wird mit der eigentlichen Datenauswertung begonnen. Diese umfasst neben grundlegenden statistischen Informationen – wie der Anzahl an Paketen und gegebenenfalls auch der Fehler beziehungsweise der Paketwiederholungen – hauptsächlich die Umwandlung der IPTs in eine grafisch anschauliche Darstellung. Zusätzlich kann dem Skript auch eine feste Achsenskalierung übergeben werden. Um die Darstellung bei automatischer Skalierung zu verbessern, ist ein Quantil-basierter Schwellwert zur Filterung von Ausreißern einprogrammiert. Dieser kann bei Bedarf im Quelltext auskommentiert werden.

Zur Darstellung der IPTs wird im Rahmen der Arbeit hauptsächlich die Form des Indexplots gewählt. Hierbei wird die jeweilige IPT über die entsprechende Paketnummer aufgetragen. Diese Darstellungsform wurde auch bereits in Abb. 2.4 kurz veranschaulicht.

b) Shell-Skripte

Zum vereinfachten Aufrufen des R-Skripts und zur vorherigen Sicherung der ursprünglichen Messdaten werden wiederum einfache Skripte verwendet (auch in `R-Skript.zip`). Auch zur Auswertung weiterer Messdaten – wie bei der Verbreitungsanalyse in Abschnitt 4.2 (`_auswertung.sh`) – werden Skripte eingesetzt. Diese kleinen Programme verfügen über mehr oder weniger aufwändige Benutzerschnittstellen und sind immer ausreichend kommentiert.

Zur Verbesserung der Paketerzeugung wird also eine neue, realtime-fähige Quelle entwickelt, was auch entsprechende Anpassungen am System nötig macht. Bei der Konfiguration der Messumgebung wird neben den Herstellerlösungen vor allem auf *OpenWRT* gesetzt. Für die Datengewinnung kommen abgesehen von *Wireshark* auch geeignete Linux-Tools zum Einsatz. Die anschließende Verarbeitung der Messdaten wird hauptsächlich in *R* durchgeführt.

3.4 Konkrete Messdurchführung

Im Folgenden wird eine Messung generisch nachvollzogen. Dies dient zur Veranschaulichung des Ablaufs und soll den konkreten Einsatz der vorgestellten Komponenten illustrieren.

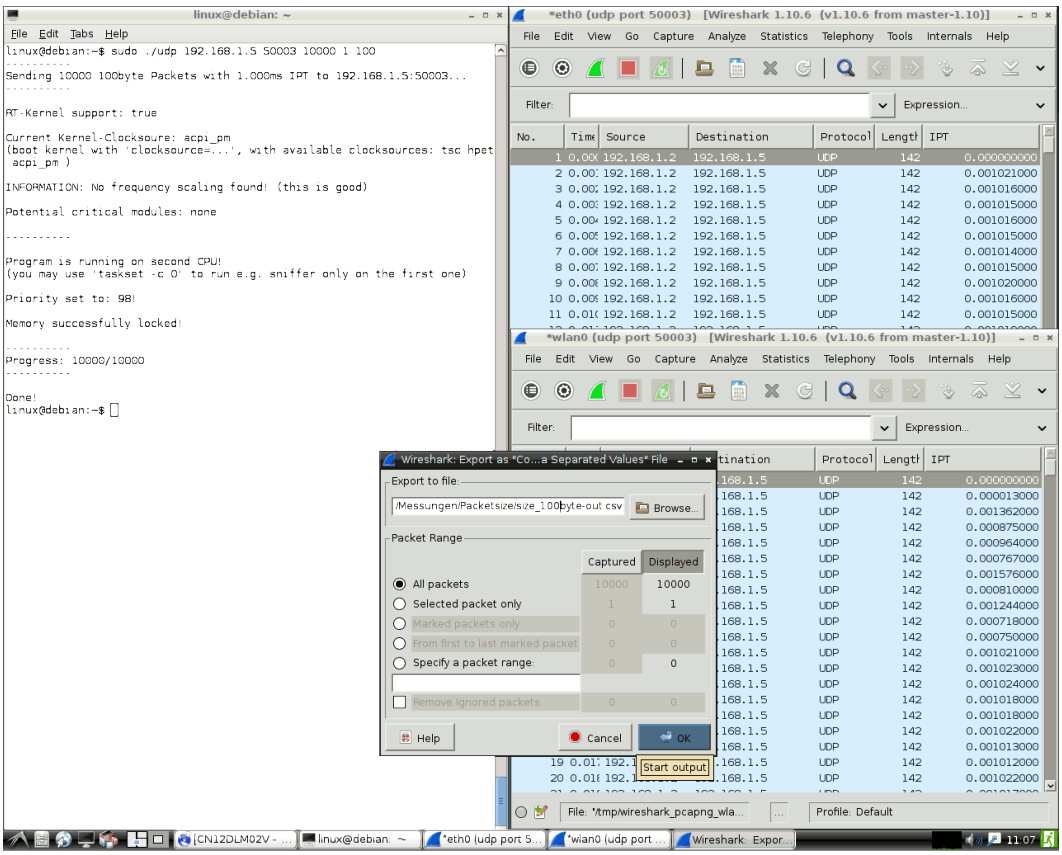


Abbildung 3.10: *Beispielhafter Screenshot aus einer Messdurchführung.*

a) Vorbereitungen

Zu Beginn gilt es, ein im Rahmen des *NetQoS*-Projekts erarbeitetes Messprotokoll auszufüllen. Dies hat – neben der standardisierten Dokumentation – hauptsächlich den Sinn, häufige Fehlerquellen systematisch auszuschließen. Des Weiteren wird dadurch eine intellektuelle Vorbereitung auf die Messung gefördert. Hierbei sind unter anderem der Grund für sowie die Erwartungen an die Messung kurz auszuarbeiten. Im Gegensatz zu den allgemeinen Szenarien steht dabei der konkrete Messaufbau im Vordergrund. Erst nach der Erarbeitung eines entsprechenden Messkonzepts wird mit dem Aufbau begonnen.

b) Grundlegender Aufbau

In einem ersten Schritt wird die Umsetzung des Konzepts in den technischen Versuchsaufbau durchgeführt. Neben der Installation der einzelnen Test- und Messgeräte steht die Verkabelung des Messaufbaus im Vordergrund. Hierbei werden entsprechende Kabel und Adapter so miteinander verbunden, dass das theoretisch erarbeitete Szenario praktisch umsetzbar wird. Dies umfasst auch die Verwendung der erwähnten Leistungsteiler sowie die schaltungstechnisch korrekte Anbindung des Testequipments. Als Beispiel sei die Störung von Up- und Downlink mithilfe der Leistungsteiler und des *SR5500* genannt.

c) Initialisierung der Geräte

Ist der grundlegende Messaufbau hardwaremäßig umgesetzt, müssen die benötigten Instrumente und Rechner eingeschaltet beziehungsweise hochgefahren werden. Diese Initialisierung kann auch weitere, nicht direkt mit der Teststrecke in Zusammenhang stehende, Konfigurationsmaßnahmen umfassen. Zum Beispiel muss der Access Point mit dem Testrechner oder der *SR5500* mit dem entsprechenden Konfigurationsrechner verbunden werden.

d) Parametrisierung der Teststrecke

Sind alle beteiligten Geräte korrekt installiert, können die softwaretechnischen Anpassungen vorgenommen werden. Hier sind insbesondere die grundlegende Konfiguration des Netzwerks sowie WLAN-spezifische Einstellungen am AP zu erwähnen. Gegebenenfalls ist weiterhin das gewünschte Störverhalten am *SR5500* einzustellen. Bei der Parametrierung der Teststrecke ist insbesondere darauf zu achten, dass die vorgenommenen Einstellungen auch tatsächlich übernommen wurden. Hierzu kann beispielsweise die Signalstärke überwacht werden.

e) Durchführung der eigentlichen Messung

Der eigentliche Messvorgang lässt sich in mehrere Schritte unterteilen. Zu Beginn jeder Messreihe ist, unter Verwendung des entsprechenden Skripts, einmalig die Routing-Tabelle anzupassen und der diesbezügliche Erfolg zu prüfen. Anschließend folgt die eigentliche Messdurchführung. Hierfür wird das *udp.c*-Programm aufgerufen, während die Netzwerkschnittstellen mit Wireshark überwacht werden. Der Paketquelle sind Parameter – wie Ziel-Adresse und Port und die Payloadgröße – zu übergeben. Die Inter-Packet Time liegt meist bei 1 ms und die Paketzahl beträgt im Allgemeinen 10.000 . Wireshark sollte dabei so konfiguriert sein, dass ausschließlich Testpakete aufgezeichnet und die IPT sowie die IP-ID in der Spaltenansicht

dargestellt werden. Um Messfehler zu vermeiden, wird grundsätzlich auch die Paketquelle – meistens am Ausgang, also an der Ethernetkarte – überwacht. Ist die Aufzeichnung erfolgreich abgeschlossen, folgt die Sicherung der Messdaten. Zum Export der Paketinformationen kommt hier das bereits erwähnte CSV-Format zum Einsatz. Die Dateinamen sollen dabei systematisch möglichst viele Informationen über die Messung enthalten.[29] Der softwaretechnische Ablauf einer solchen Messung ist in Abb. 3.10 illustriert. Neben der Paketquelle im Terminal und den Wireshark-Senken ist dort auch der Datenexport abgebildet.

f) Auswertung der gewonnenen Messdaten

Nach dem Export der erzeugten Daten werden diese grundsätzlich mit dem erwähnten R-Skript ausgewertet und anschließend systematisch archiviert. Für eine fehlerfreie Messung dürfen die IPTs der Kontrollmessung keine ungewöhnlichen Schwankungen aufzeigen. Durch mehrmaliges Wiederholen gleicher Messungen können weiterhin zufällige Abweichungen erkannt und berücksichtigt werden. Auch eventuell zusätzlich gewonnene Informationen – wie aus dem in Abb. 3.11 dargestellten WLAN-Sniffing – fließen in die Auswertung mit ein. Abschließend werden die gewonnenen Erkenntnisse schriftlich festgehalten.

Der Ablauf der vorgestellten Messung entspricht der grundsätzlichen Vorgehensweise aller im Rahmen dieser Arbeit durchgeführten Versuche. Daher werden mögliche Unterschiede und Besonderheiten im Weiteren extra hervorgehoben.

[29] Beispielsweise steht `size_100byte-out.csv` für ein Messresultat mit 100 Byte großem Payload. Die Standard-IPT von 1 ms wird hierbei vorausgesetzt, ebenso die Anzahl von 10.000 Testpaketen.

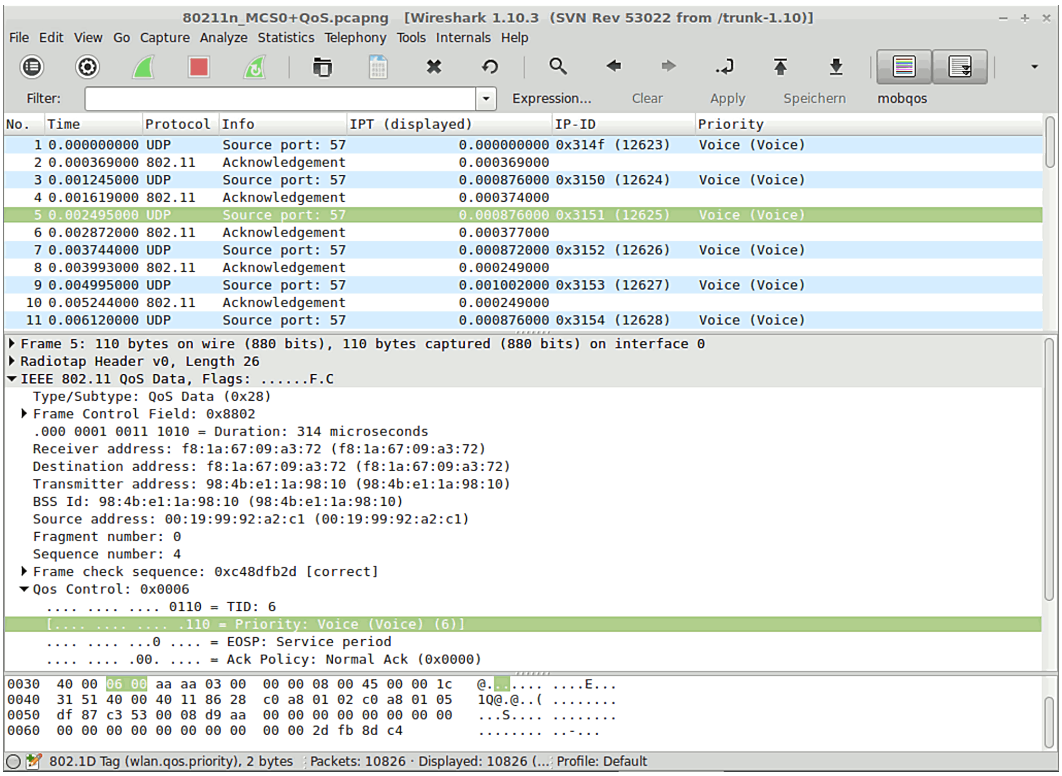


Abbildung 3.11: *Auswertung der QoS-Flags aufgezeichneter WLAN-Pakete.*

Zusammenfassend dient dieses Kapitel dazu, sowohl die Konzeptionierung als auch die Implementierung des in der Arbeit verwendeten Messaufbaus zu erläutern. Speziell im Bezug auf die konkrete Versuchsumsetzung wird die verwendete Hard- und Software vorgestellt. Weiterhin wird der Ablauf einer Versuchsdurchführung kurz illustriert. Neben dem allgemeinen Einblick in den Messaufbau spielt auch das – im Rahmen der WLAN-Hardware diskutierte – Busverhalten in der Ergebnisanalyse eine wichtige Rolle.

4 Ergebnisanalyse

Im Folgenden werden die theoretischen Grundlagen aus Kapitel 2 auf das IPT-Verhalten übertragen und entsprechenden Messergebnissen gegenübergestellt. Hierbei wird erst der UMTS-Kanal untersucht und anschließend wird eine adäquate WLAN-Übertragungscharakteristik herausgearbeitet. Abschließend findet ein Vergleich beider Kanalverhalten statt.

4.1 UMTS-Kanalverhalten

In diesem Abschnitt wird das Kanalverhalten von UMTS theoretisch erarbeitet und anschließend mithilfe von Messergebnissen verifiziert. Diesbezüglich finden neben einer Auswertung bisheriger Arbeiten auch eigene Versuche statt.

4.1.1 Ergebnisse bisheriger Arbeiten

Wie in den Grundlagen (Abschnitt 2.3) herausgearbeitet, handelt es sich bei UMTS um einen Standard, der einerseits eine komplexe Systemebene beschreibt und andererseits die Fehlerbehandlung auf der Paketebene ausführlich spezifiziert. Somit sind theoretische Aussagen über die Größenordnung der Paketlaufzeit sowie über das Retransmissionsverhalten möglich. Als Grundlage dient hierbei die Masterarbeit von Baris Güzelarslan (siehe [Bar07]).

a) Einflussfaktoren auf die Paketlaufzeiten

Die Laufzeit eines Datenpakets im UMTS-Netzwerk setzt sich aus den Verarbeitungs- und Übertragungszeiten aller beteiligten Komponenten zusammen und liegt insgesamt bei 150 bis 200 ms (vgl. hierzu [Bar07, Seite 50 ff.]). Der Verbindungsaufbau für einen *Dedicated Channel* benötigt einmalig zwischen 6 und 8 s. Auch Funkzellenübergaben machen sich in der Paketlaufzeit bemerkbar. Man unterscheidet hier zwischen *Soft Handovers* – mit einmaligen Verzögerungen von etwa 200 ms – und *Hard Handovers*, die einen kompletten Verbindungsabbruch zur Folge haben. Zusätzlich können Mobilfunk-spezifische Effekte wie die sogenannte *Zellatmung*, das *Re-Routing* von Paketen innerhalb des Netzwerks sowie vorübergehende *Blockierungen* der Datenübertragung zu Laufzeitschwankungen und Paketverlusten führen. Insbesondere das sogenannte *Scheduling* zur Optimierung der Ressourcennutzung wird in Form von *Bandwith Oscillation* – also temporären Schwankungen der Datenraten – sichtbar. All diese Effekte beeinflussen die Datenübertragung auf eine charakteristische Weise.

b) Verzögerungen durch Retransmissionen

Vernachlässigt man die Einflussfaktoren der Systemebene und betrachtet ausschließlich den Verzug durch die Fehlerbehandlung, ergibt sich ein vereinfachtes Kanalverhalten. Im *Acknowledge Modus* der RLC-Schicht führt ein Paketverlust beziehungsweise ein irreparabler Übertragungsfehler zur Neuanforderung der betroffenen Daten. Die maximal vier bis sieben Wiederholungen genießen dabei absolute Priorität. Wird ein Übertragungsversuch mit k bezeichnet, gilt (siehe hierzu [Bar07, Seite 33 ff.]):

$$k \in \mathbb{N}\ ,\ 1 \leq k \leq 8 \tag{4.1}$$

Die Laufzeit eines Paketes setzt sich wie erläutert prinzipiell aus der Verarbeitungs- und Übertragungsdauer zusammen. Aufgrund der speziellen Datenkapselung bei UMTS ist hierbei der TTI mit der relativen Paketauslastung zu gewichten (vgl. auch Abb. 2.13):

$$D_1 = T_{proc} + T_{transmit} + l \cdot TTI \tag{4.2}$$

$$l = \left\lceil \frac{PDUs\ pro\ SDU}{PDUs\ pro\ Radio\ Frame} \right\rceil \tag{4.3}$$

Die Verzögerung im Wiederholungsfall setzt sich wiederum aus der Fehlererkennungszeit und der priorisierten Neuanforderung der fehlerhaften Daten zusammen:

$$T_1 = T_{ack} + 2 \cdot (TTI + T_{transmit}) \tag{4.4}$$

Somit berechnet sich schließlich die Gesamtlaufzeit wiederholt angeforderter Pakete durch:

$$D_k = D_1 + (k-1) \cdot T_1 \tag{4.5}$$

Theoretisch ergeben sich also nach Anzahl der Retransmissionen diskretisierte Übertragungszeiten. Diese sind insbesondere durch die hohe UMTS-Umlaufzeit geprägt und liegen daher bei Vielfachen von 150 bis 200 ms. Mit einer Wiederholungsanzahl $k_{max} = 8$ ergeben sich maximale Laufzeitverzögerungen im Bereich von einer Sekunde.

c) Bisherige Messergebnisse

Dieses theoretische Verhalten wird durch Messungen von Baris Güzelarslan bestätigt. Hierbei wird ein Perl-Skript – ähnlich dem in dieser Arbeit verwendeten *udp.c*-Programm – und eine *CMU200-SMIQ*-Messtrecke – vergleichbar mit der beschriebenen *CMW500-SR5500*-Messstrecke – eingesetzt. Wie in Abb. 4.1 veranschaulicht ist, verhalten sich die IPTs einer gestörten UMTS-Übertragung tatsächlich diskret zur Anzahl der Paketwiederholungen.

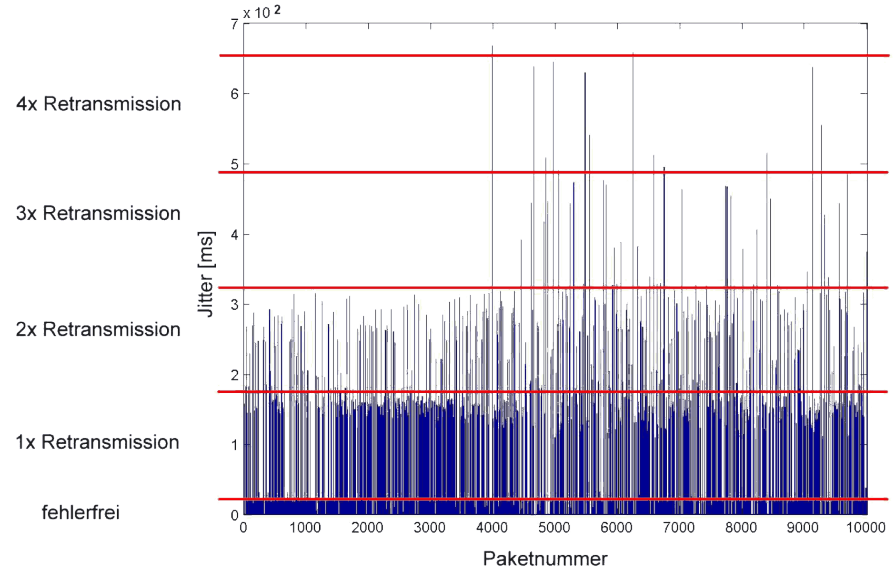
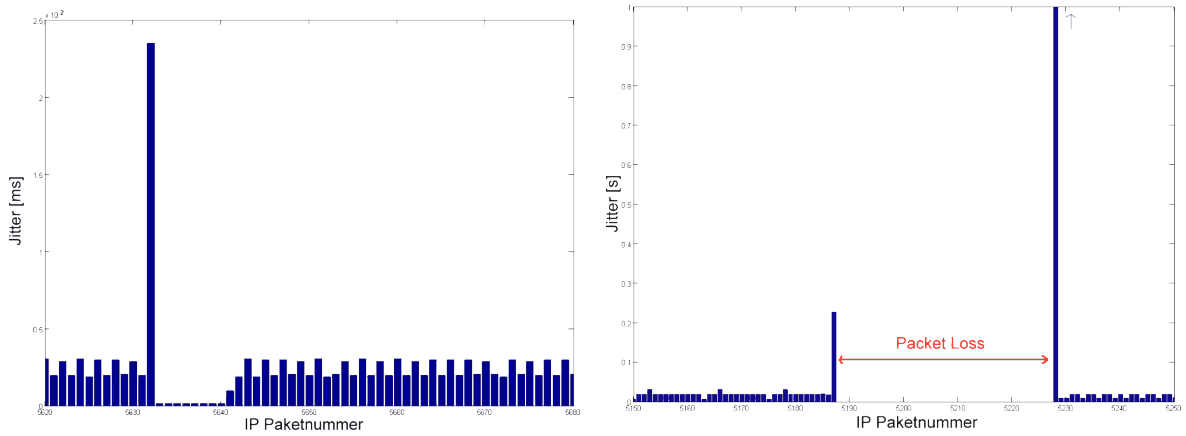


Abbildung 4.1: *Durch Paketwiederholungen diskretisierte IPTs bei UMTS. [Bar07, Seite 36]*

Bei genauerer Betrachtung der Messdaten wird das beschriebene zeitliche Verhalten auch für den einzelnen Fehlerfall bestätigt. Abb. 4.2a stellt den detaillierten IPT-Verlauf bei einer Retransmission dar. Aufgrund der Laufzeitverzögerung von 200 ms kann auf eine einfache Neuanforderung geschlossen werden. Weiter ist ersichtlich, dass die anschließend folgenden Pakete bereits verarbeitet sind und gepuffert im Endgerät vorliegen („0er“-IPTs).



(a) Auswirkung einer einfachen Paketwiederholung.

(b) Auswirkung eines kompletten RLC-Resets.

Abbildung 4.2: *Ausschnitt aus dem UMTS-spezifischen IPT-Verhalten. [Bar07, Seite 61/62]*

Dieses Verhalten unterscheidet sich statistisch von den Einflussfaktoren der Systemebene. Wie in Abb. 4.2b dargestellt, kommt es beispielsweise bei Verbindungsabbrüchen zu tatsächlichen Paketverlusten und deutlich längeren Verzögerungen.

Insgesamt lässt sich somit anhand der IPT- und Paketverlustdaten die Qualität des UMTS-Übertragungskanals klassifizieren (siehe hierzu insbesondere [Bar07, Seite 63 ff.]). Beispielsweise lassen sich Störungen durch AWGN-Rauschen von Rayleigh-Fading unterscheiden. Während beim Fading Paketwiederholungen (Abb. 4.2a) dominieren, kommt es beim Rauschen schnell zu Verbindungsabbrüchen (Abb. 4.2b).

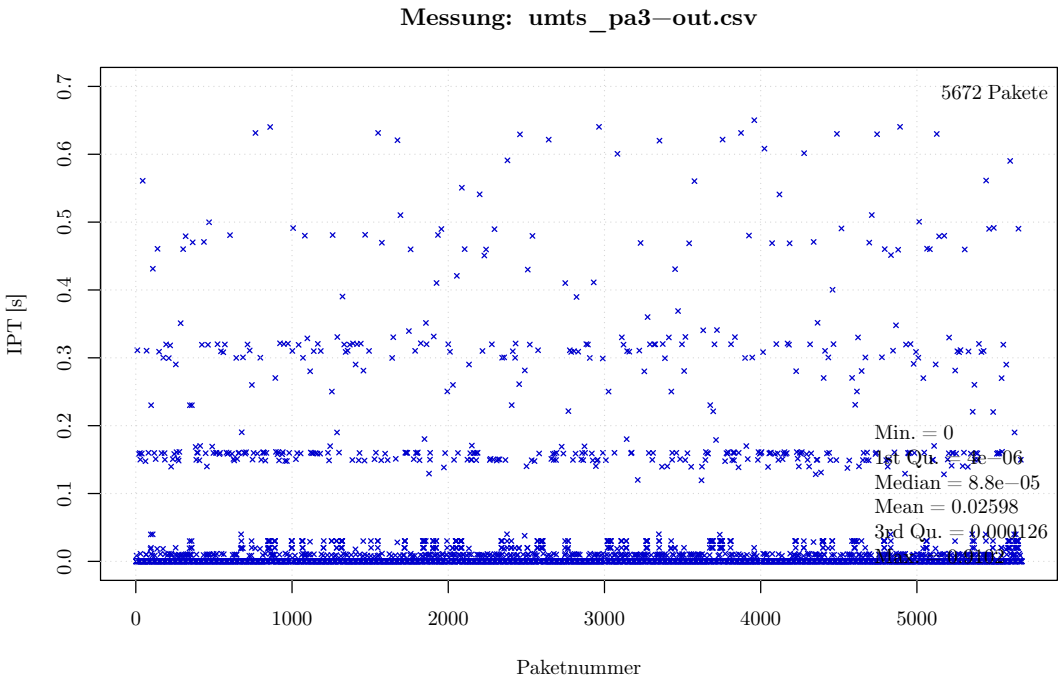
4.1.2 Bestätigung der Beobachtungen

Die beschriebene Kanalcharakteristik wird im Rahmen dieser Masterarbeit im neuen Versuchsaufbau überprüft. Hierfür wird der in Abschnitt 3.1 beschriebene *MobQoS*-Messaufbau – also die *CMW500-SR5500*-Messstrecke – verwendet. Als Paketquelle kommt das neue *udp.c*-Programm zum Einsatz und die Datenauswertung findet mithilfe des R-Skripts statt.

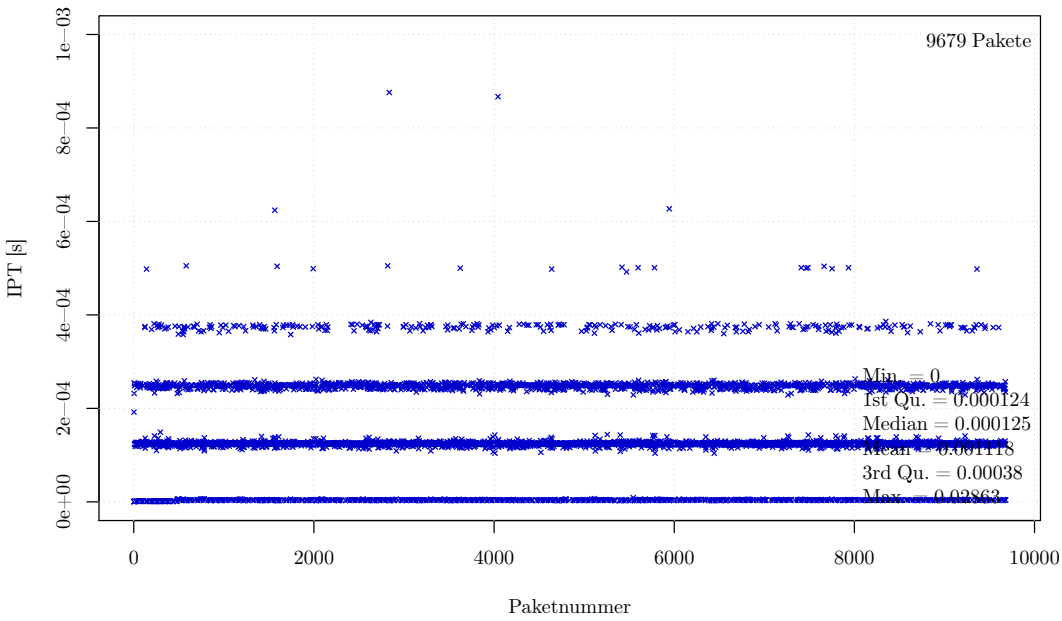
Zur Kanalstörung werden von der *International Telecommunication Union* standardisierte Fading-Modelle verwendet (vgl. auch [Raj07, Seite 18 f.]). Analog zu den WLAN-Modellen umfassen diese unterschiedlich intensive Mehrwegeverzögerungen für *Indoor*-, *Pedestrian*- und *Vehicular*-Szenarien bei verschiedenen Geschwindigkeiten. Um die Kanalcharakteristik zu bestätigen, werden die im *SR5500* vorkonfigurierten Störmodelle bei unterschiedlichen Gesamtdämpfungen verwendet. Wie bei allen bisher am Lehrstuhl durchgeführten Mobilfunkmessungen wird dabei nur der Downlink gestört, der ungestörte Uplink wird mittels Leistungsteiler eingekoppelt. Wichtig beim UMTS-Versuchsaufbau sind die genauen Kanaleinstellungen und die passende Paketgröße. Diese werden der Arbeit von Baris Güzelarslan entnommen und auf den neuen Messaufbau übertragen (siehe [Bar07, Seite 85 ff.]).

Somit ergibt sich beispielsweise für das *PA3*-Modell – also in einer *Pedestrian*-Umgebung bei 3 km/h – das in Abb. 4.3a illustrierte IPT-Verhalten mit einer maximalen Paketverzögerung von 0,9 s. Neben dem diskreten UMTS-Übertragungsverhalten kann das verbesserte Messverfahren auch das bereits in Abschnitt 3.2 im Rahmen der WLAN-Hardware angesprochene USB-Busverhalten des verwendeten *ZTE MF821D*-Sticks erfassen. Abb. 4.3b hebt die diesbezüglichen IPT-Diskretisierungen hervor. Der Abstand der sich ergebenden Linien entspricht dabei mit 125 μs der Größe der *USB 2.0-Micro-Frames*. Dieses Verhalten ist bei allen im Rahmen der Arbeit vermessenen USB-Geräten beobachtbar.

Weitere Messungen mit dem HSDPA-Datenübertragungsverfahren ergeben ähnliche Diskretisierungen, allerdings mit Unterschieden bezüglich der Gesamtlaufzeit. Aufgrund der Themenstellung werden diese aber nicht weiter untersucht und daher auch nicht vorgestellt.



(a) IPT-Diskretisierung aufgrund des UMTS-Kanalverhaltens.



(b) IPT-Diskretisierung aufgrund des USB-Busverhaltens.

Abbildung 4.3: *Ergebnis der im Rahmen dieser Arbeit durchgeführten UMTS-Messungen.*

Um das Retransmissionsverhalten weiter zu veranschaulichen, kann auch ein Histogramm oder eine Kerndichteschätzung verwendet werden. Die geschätzte Dichtefunktion der IPTs – wie sie in Abb. 4.4 dargestellt ist – offenbart dabei nicht nur die bis zu sechs Retransmissionsvorgänge in der Messung, sondern darüber hinaus auch die physikalische Datenübertragung. Wie in den UMTS-Grundlagen in Abschnitt 2.3 erwähnt, erfolgt diese in TTI-Fenstern von mindestens 10 ms. Der Transmission Time Interval wird in den kleinen Diskretisierungen in der Kerndichteschätzung sichtbar.

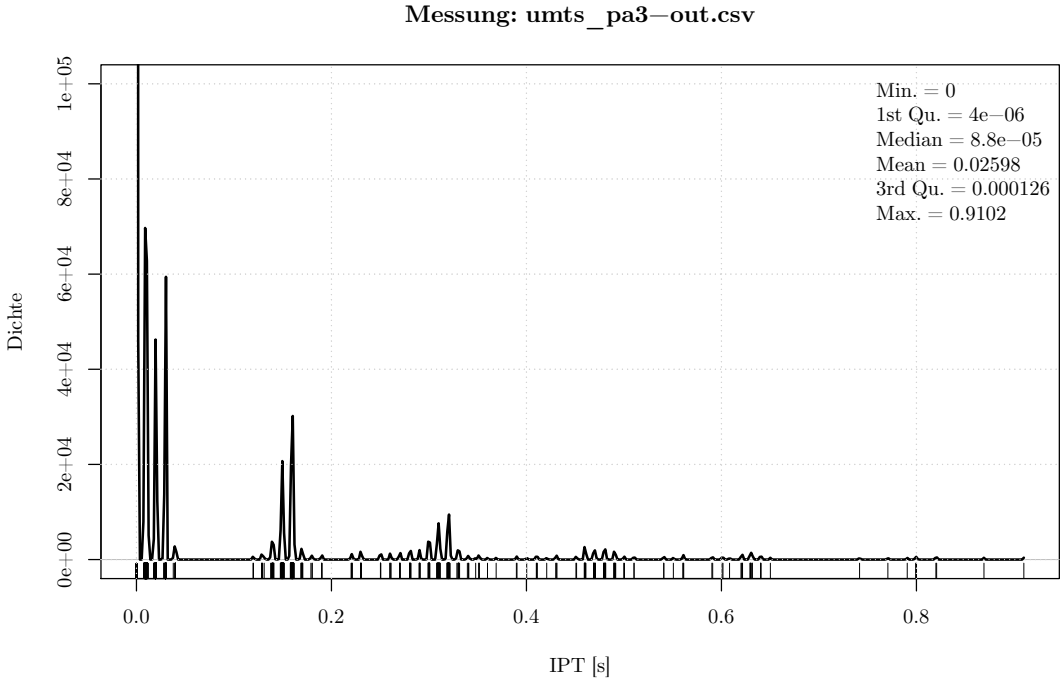


Abbildung 4.4: *Kerndichteschätzung der Inter-Packet Times bei UMTS.*

Die vorgestellte UMTS-Übertragungscharakteristik kann folglich als nochmals bestätigt betrachtet werden. Paketverluste durch Fading führen zu klar erkennbaren, diskreten Verzögerungen im oberen Millisekundenbereich (für *Release 99*). Dieses Verhalten ermöglicht es, auf die Ursache der Störung respektive die Güte des Funkkanals zurückzuschließen. Zusätzlich kann im neuen Messaufbau sowohl der TTI als auch der USB-Einfluss beobachtet werden.

4.2 WLAN-Kanalverhalten

Im Gegensatz zu UMTS liegt für WLAN bisher keine IPT-basierte Kanalcharakterisierung vor. Aus diesem Grund wird eine solche im Folgenden sowohl theoretisch als auch mithilfe von Messergebnissen erarbeitet. Nach einer kurzen Bewertung der WLAN-Standards hinsichtlich ihrer Verbreitung finden protokollspezifische Überlegungen zur Abschätzung der Paketlaufzeiten statt. Diese werden schließlich durch Messergebnisse – speziell zum Einfluss von Implementierungen, spezifischer Optionen und geeigneter Störungen – ergänzt.

4.2.1 Verbreitungsanalyse

Da WLAN über viele verschiedene Standards, Erweiterungen und diesbezügliche Einstellungsmöglichkeiten verfügt, wird anfangs eine kurze Verbreitungsanalyse durchgeführt. Hierfür werden WLAN-Netzwerke an ausgewählten Orten erfasst und die so gewonnenen Daten anschließend mithilfe eines entsprechenden Skripts ausgewertet. Weiterhin fließen Informationen aus öffentlich verfügbaren Nutzungsdaten und aus Gesprächen mit technisch verantwortlichen Mitarbeitern der Hochschul-IT in die Bewertung mit ein.

	Anz.	**802.11n**	**WMM**	**MIMO**	**5 GHz**	**40 MHz**	**Interf.**
Dorf	5	4	3	3	0	1	4
Stadt	8	8	8	6	0	7	8
Hbf M	6	5	6	4	3	3	3
Hbf IN	5	5	5	3	1	3	3
HM	9	0	0	/	/	/	8
TUM	318	311	306	318	239	1	79

Tabelle 5: *Analyse von WLAN-Netzwerken in verschiedenen Anwendungsbereichen.*[30]
Hbf *steht für Hauptbahnhof und* M *für München beziehungsweise* IN *für Ingolstadt.*
HM *steht für die Hochschule,* TUM *für die Technische Universität München.*

Das Ergebnis der im Frühling 2014 durchgeführten Netzwerksauswertung ist in Tab. 5 dargestellt. Die Orte zur Datenerfassung werden dabei gezielt in den Bereich des privaten Einsatzes im Wohngebiet, des gemischten Einsatzes im öffentlichen Raum und des professionellen Einsatzes im Hochschulnetz eingeteilt. Insgesamt werden sechs Messungen durchgeführt, die zur Beurteilung der Verbreitung von 802.11n dienen und Aussagen zur WMM-, MIMO- und

[30] Basierend auf Rohdaten aus eigenen Aufzeichnungen mittels `iw scan`.

5 GHz-Unterstützung sowie zur Kanalbündelung ermöglichen. Aufgrund der Kanalverteilung können des Weiteren auch Erkenntnisse zu den jeweils auftretenden WLAN-Interferenzen gewonnen werden. Speziell zur Lage an der *Hochschule München* sei vermerkt, dass im Laufe der Arbeit eine Umstellung von 802.11g auf n durchgeführt wird. Laut Aussage der IT sind im April 2014 hochschulweit fast 400 APs im Einsatz, von denen die Hälfte über eine Dualbandunterstützung verfügt. Die Migration auf den n-Standard ist dabei zu ca. 40% abgeschlossen. Entsprechend sind die erfassten Daten als demnächst veraltet zu betrachten.

Als weitere Quelle zur aktuellen Verbreitung der WLAN-Standards wird die öffentliche Nutzungsstatistik des LRZ[31] verwendet. Hierzu werden die AP-Daten an einem Vorlesungsvormittag über 30 min gemittelt und gerundet. Von insgesamt 20.000 angemeldeten Clients nutzen noch knapp die Hälfte der Geräte die Standards abg. Die mit 802.11n angemeldeten Nutzer teilen sich auf je 7.500 STAs im 2,4 GHz- und je 3.100 im 5 GHz-Bereich auf.

Insgesamt lässt sich also feststellen, dass die 802.11n-Unterstützung mittlerweile weit verbreitet ist. Oft verfügen die installierten APs dabei über 2×MIMO und bieten die Kanalbündelung an. Der 5 GHz-Bereich wird bisher hauptsächlich im professionellen Umfeld genutzt. Obwohl die meisten Netzwerke über WMM-Unterstützung verfügen, werden zu keinem Zeitpunkt QoS-Pakete beobachtet. Auch aufgrund dieser Analyse wird im Folgenden hauptsächlich das 802.11n-WLAN im 2,4 GHz-Bereich mit einfacher Kanalbandbreite und WMM-Unterstützung (aber ohne QoS-Pakete) als Standardnetzwerk für diese Arbeit betrachtet. Dennoch werden auch die anderen Optionen weiterhin berücksichtigt.

4.2.2 Theoretische Überlegungen

Wie in den Grundlagen (Abschnitt 2.2) herausgestellt, arbeitet WLAN mit verschiedenen Paketabständen zur Kollisionsvermeidung. Dies führt dazu, dass vor dem Senden eines Testpakets gewartet und anschließend, nach einem weiteren Abstand, das `ACK` zur Quittierung empfangen werden muss. Kommt es zu Übertragungsproblemen, ist eine Paketwiederholung vorgesehen. Meist ist hierbei ein Limit von sieben Retransmissionen[32] festgesetzt, zwischen denen die Wartezeit exponentiell ansteigt (vgl. hierzu nochmal [Mar09, Seite 16 f.]). Das Wissen über dieses grundlegende Verhalten ermöglicht eine quantitative Abschätzung der Paketlaufzeiten im WLAN-Netzwerk.

[31] Quelle: `http://apstat.lrz-muenchen.de/AP_Statistik.html` (abgerufen am 15.04.2014)

[32] Entspricht den mittels `iwconfig` überprüften Treibereinstellungen aller getesteten Netzwerkkarten.

Die WLAN-Übertragungsstrecke besteht – im Gegensatz zur komplexen Systemebene bei UMTS – praktisch nur aus der Luftschnittstelle. Vernachlässigt man hierbei die reinen Verarbeitungs- und Übertragungszeiten – wie die höchstens 800 ns *Guard Interval* – ergibt sich für die DCF folgender, kürzester Empfangszeitraum (vgl. besonders auch Abb. 2.7):

$$D_{min} = T_{DIFS} + T_{Data} + T_{SIFS} + T_{ACK} \tag{4.6}$$

Für 802.11n liegt die Summe der hier verwendeten *Interframe Spaces* bei bis zu 60 μs (siehe [Mar09, Seite 15 ff.]). Auswertungen von Testpaketen im Monitor-Modus ergeben des Weiteren eine Datenlänge von zirka 50 μs und ein vernachlässigbares T_{ACK}.[33] Es ergibt sich also insgesamt eine Paketlaufzeit im mittleren bis oberen Mikrosekundenbereich.

Kommt es zu Übertragungsfehlern, werden diese spätestens mit dem Ausbleiben des `ACK`s erkannt. Der entsprechende Timeout liegt meistens ebenfalls im Bereich einiger Mikrosekunden.[34] Bei der Neuübertragung muss dann allerdings auch die Backoffzeit berücksichtigt werden. Folglich ergibt sich für Retransmissionen eine Zeitspanne von:

$$D_{retry} \approx CW \cdot SlotTime + D_{min} \tag{4.7}$$

Hierbei ist die Backoffzeit als mit der Wiederholungsanzahl ansteigend definiert:

$$CW = 2^{\tilde{k}} - 1 \tag{4.8}$$

Standardmäßig ist das Contention Window zwischen $CW_{min} = 15$ und $CW_{max} = 1023$ beschränkt. Durch diese Einschränkung ergibt sich der Definitionsbereich von k:

$$\tilde{k} \in \mathbb{N}\ ,\ 4 \leq \tilde{k} \leq 10 \tag{4.9}$$

Nimmt man weiterhin ein k_{max} von sieben Wiederholungen an, ist eine Worst Case-Abschätzung der Paketverzögerungszeit im Fehlerfall möglich:

$$D_{retry,max} \approx D_{min} + \sum_{k=1}^{7} (2^{k+3} - 1) \cdot SlotTime + D_{min} \tag{4.10}$$

Bei einer *Slot Time* von 20 μs ergibt sich für 802.11n somit eine theoretisch maximale Laufzeitverlängerung von 42 ms. Da im Versuchsaufbau jedoch nur selten mehr als drei Wiederholungen beobachtet werden, liegt die Paketlaufzeit meist unterhalb dieses Werts. Für größere Pakete sind diese Zeiten entsprechend höher, bleiben aber in der berechneten Größenordnung.

[33] Diese Beobachtung gilt nur für payload-freie UDP-Pakete und MCS-Übertragungsraten.

[34] Quelle: `http://www.air-stream.org.au/technical-references/ack-timeouts-and-effects-distance-links` (abgerufen am 08.10.2014)

Aufgrund der Tatsache, dass bei WLAN keine Priorisierung der Retransmissionen vorgesehen ist und 802.11n zusätzlich auch die Paketaggregation erlaubt, ist das Verzögerungsverhalten dabei nicht deterministisch festgelegt. Daher ist eine Diskretisierung der IPTs bei Paketwiederholungen – wie sie bei UMTS auftreten – aus theoretischer Sicht nicht zu erwarten.

4.2.3 Konkrete Messergebnisse

Wie in Kapitel 3 beschrieben, sind die Versuche in mehrere Messreihen eingeteilt. In einem ersten Schritt wird dabei der allgemeine Einfluss des Messaufbaus und der dabei verwendeten Hardwareimplementierungen untersucht. Anschließend wird die Auswirkung standardspezifischer Einstellungen überprüft und es werden spezielle Messungen zum Störverhalten – sowohl durch WLAN-Interferenzen als auch durch Fading – durchgeführt. Die Messdaten aller hier erwähnten Versuche sind in entsprechenden Unterordnern in Anhang A hinterlegt.

a) Ungestörter Messaufbau

(i) Vorversuche:

Aufgrund der Tatsache, dass bereits die ersten, ungestörten Messungen unterschiedliche IPT-Verläufe ergeben, werden verschiedene Vergleichsmessungen durchgeführt. Diese umfassen Versuche mit der im Messaufbau verwendeten Software – insbesondere zur Parametrisierung der Paketquelle – und der genutzten Hardware. Im Rahmen dieser Messungen wird ausschließlich der einfache, direkte und ungestörte *NetQoS*-Messaufbau verwendet.

Bezüglich der Paketquelle wird in diesem Schritt der Einfluss von Paketabstand und Größe des verwendeten UDP-Payloads untersucht. Hierfür werden jeweils 10.000 Pakete übertragen und das Ergebnis anschließend hinsichtlich der Aussagekraft bewertet. Als geeignetste IPT am Sender stellt sich hierbei ein Abstand von 1 ms heraus. Damit ist eine gute Beobachtbarkeit des Kanalverhaltens möglich, ohne dass die Messgenauigkeit in einem problematischen Bereich liegt. Die Paketgröße wird für die weiteren Versuche jeweils auf einen kleinst- und einen größtmöglichen Payload – nämlich 0 beziehungsweise 1450 Byte[35] – beschränkt. Durch dieses Vorgehen lässt sich der Einfluss unterschiedlicher Datenraten einfach untersuchen. Da die Messungen mit kleinen Testpaketen stabiler[36] sind und somit eine bessere Vergleichsbasis erzeugen, werden im Folgenden besonders diese besprochen.

[35] Die obere Grenze ergibt sich durch die *Maximum Transmission Unit* der Vermittlungsschicht. In Computernetzen (Ethernet/WLAN) liegt diese oft bei um 1500 Bytes.

[36] Für größere Pakete werden höhere IPTs, mehr Paketverluste und Übertragungsfehler beobachtet.

Aus messtechnischer Sicht finden darüber hinaus noch Versuche mit verschiedenen Kabeln und Leistungsteilern statt. Im Rahmen dieser Messungen wird auch der einfache Versuchsaufbau und der Einfluss der Ethernetübertragung überprüft. Des Weiteren wird festgestellt, dass es trotz der direkten HF-Verkabelung zu keiner Übersteuerung der Netzwerkkarten kommt. Auch können keine weiteren, unerwünschten Effekte festgestellt werden.

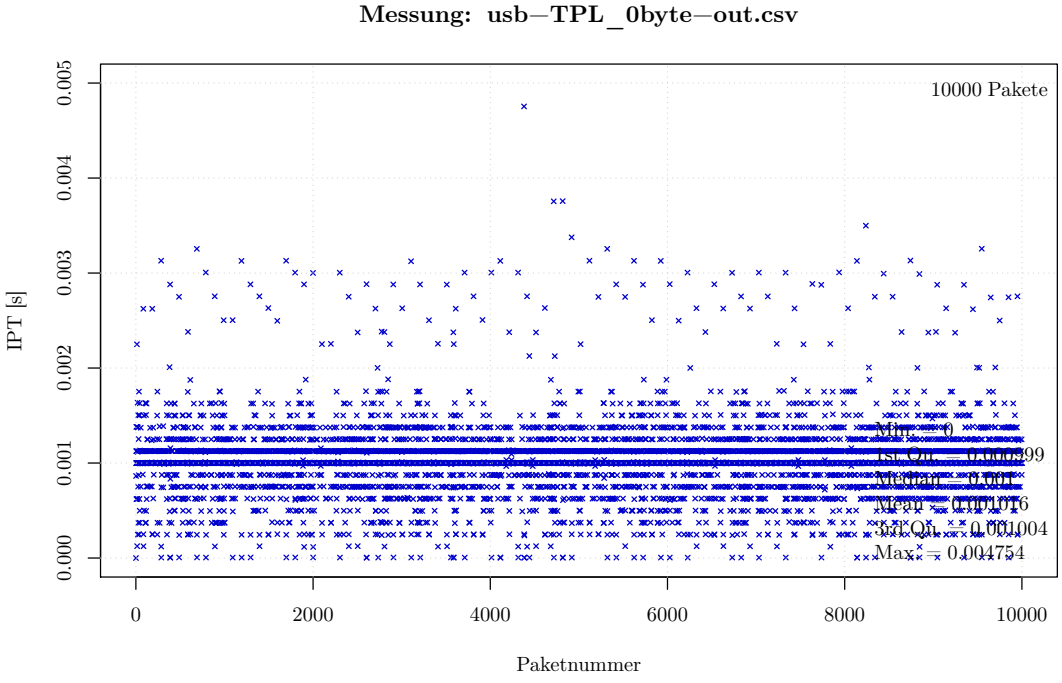
(ii) Hardwareanalyse:

Nach den ersten Vorversuchen wird genauer untersucht, inwiefern die Paketlaufzeiten hersteller- und busspezifischen Einflüssen unterliegen. Auch hier kommt der störungsfreie Messaufbau zum Einsatz. Die Testpakete entsprechen den oben genannten Kriterien.

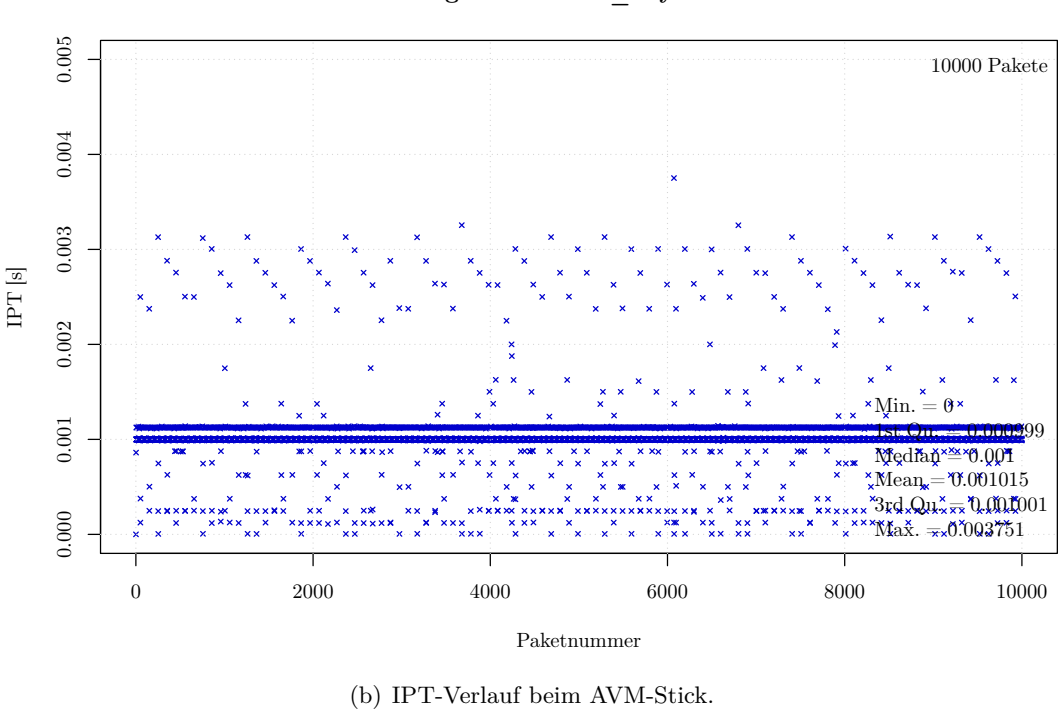
Im Rahmen dieser Messungen fällt als erstes das bereits bei UMTS beobachtete USB-Busverhalten auf. Bei allen drei vermessenen WLAN-Sticks kommt es zu Diskretisierungen mit je 125 μs Abstand. Trotz dieser Gemeinsamkeit unterscheidet sich das beobachtete Übertragungsverhalten der Sticks untereinander. Stellt man die Messergebnisse – wie in Abb. 4.5 – direkt gegenüber, so werden diese Differenzen offensichtlich. Aufgrund der Messdaten muss von herstellerübergreifenden und chipsatzspezifischen Unterschieden ausgegangen werden.

Zwar ist ein ähnliches Busverhalten bei den PCIe-Karten nicht ersichtlich (oder zumindest bisher nicht erklärbar), doch unterscheiden sich auch hier die Paketverzögerungen je nach getesteter Hardwareimplementierung voneinander. Dies ist in Abb. 4.6 veranschaulicht. Während die *TP-Link*-Karte relativ wenige und gleichmäßige IPT-Schwankungen erzeugt, verhält sich die *Realtek*-Hardware weitgehend unvorhersehbar. Aufgrund der Tatsache, dass es bei der Realtek-Messreihe immer wieder zu kompletten Verbindungsabbrüchen kommt – bei denen zudem nur ein Neustart des Versuchsrechners Abhilfe schafft – wird hierbei allerdings von einem Treiberproblem ausgegangen. Da somit nur eine einzige zuverlässig vermessbare WLAN-Karte zur Verfügung steht, werden auch die Router entsprechend in den Versuchsaufbau mit einbezogen. Insbesondere kommt auch ein umgedrehter Messaufbau zum Einsatz. Dadurch, dass die Testpakete auch von der STA zum AP gesendet werden, kann sowohl das Sende- als auch das Empfangsverhalten der jeweiligen Chipsätze miteinander verglichen werden. Somit lassen sich schließlich die herstellerübergreifenden und chipsatzspezifischen Unterschiede auch für die per PCIe-Bus angeschlossenen WLAN-Karten bestätigen.

Mit Ausnahme der *Realtek*-Karte bleiben bei Hardware-Messungen mit kleinen Testpaketen die maximalen Laufzeitverzögerungen unter 10 ms; der Mittelwert liegen bei 1 ms.

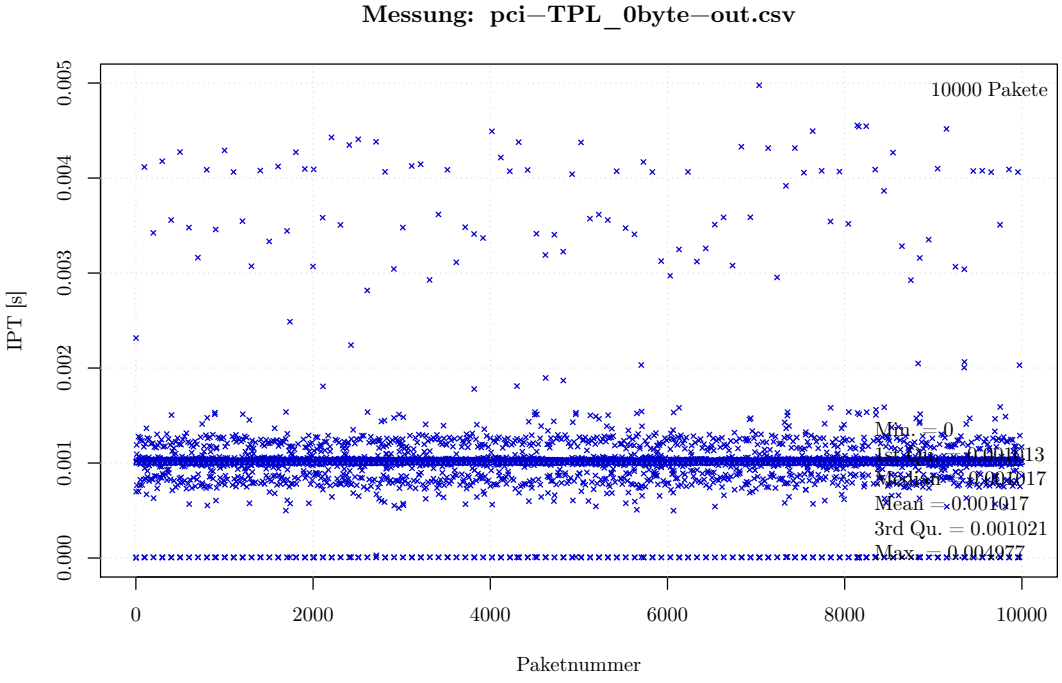


(a) IPT-Verlauf beim TP-Link-Stick.

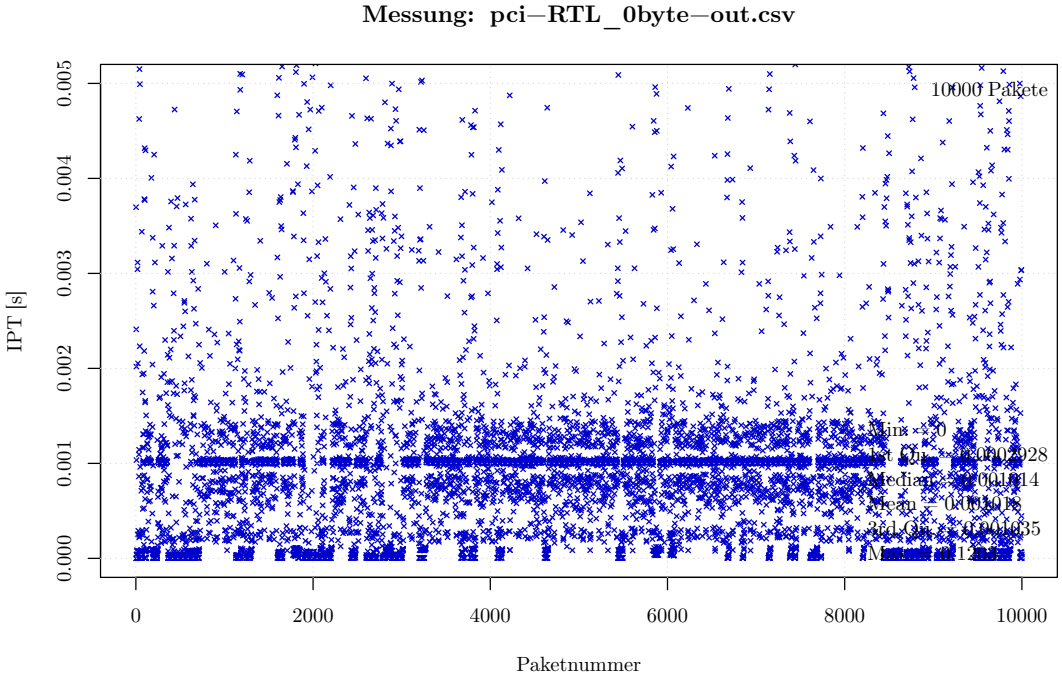


(b) IPT-Verlauf beim AVM-Stick.

Abbildung 4.5: *Gegenüberstellung der USB-Sticks.*



(a) IPT-Verlauf der TP-Link-Karte.



(b) IPT-Verlauf der Realtek-Karte.

Abbildung 4.6: *Gegenüberstellung der PCIe-Karten.*

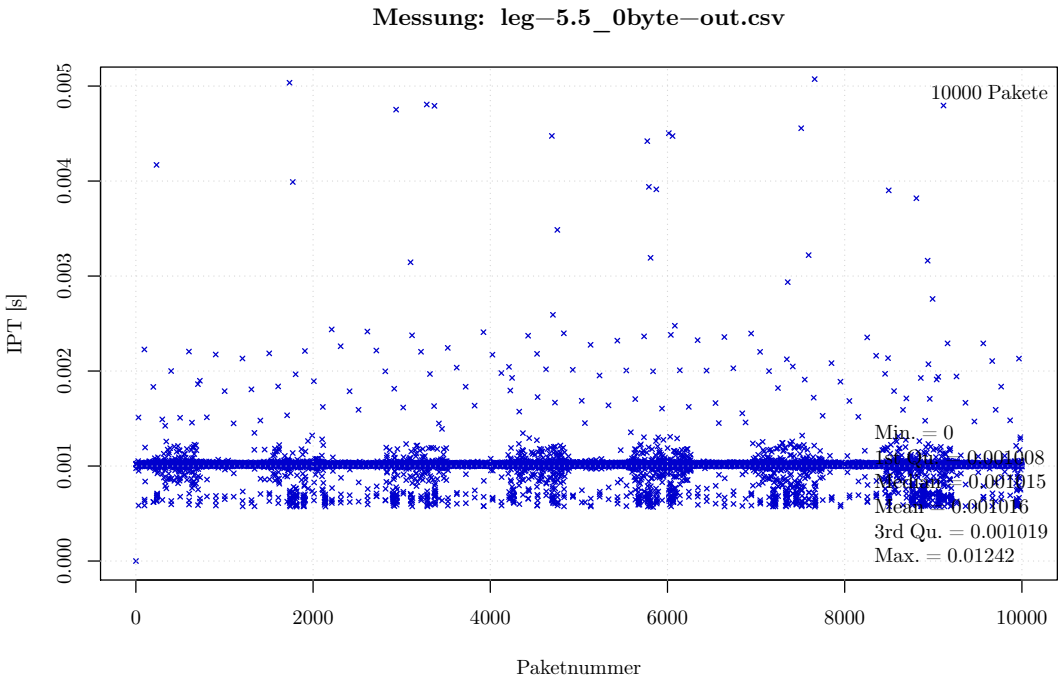
(iii) Standardspezifische Einflüsse:

Da bereits die Hardware das Übertragungsverhalten deutlich beeinflusst, werden auch die möglichen Treiberoptionen vorerst ohne zusätzliche Störungen untersucht. Hierbei stehen die konfigurierbaren WLAN-spezifischen Einstellungsmöglichkeiten – wie zum Beispiel die Kanalauswahl oder die Datenrate – im Fokus der Untersuchung. Aufgrund der beschriebenen Treiberprobleme werden im Folgenden nur Messungen mit der *TP-Link*-Karte besprochen.

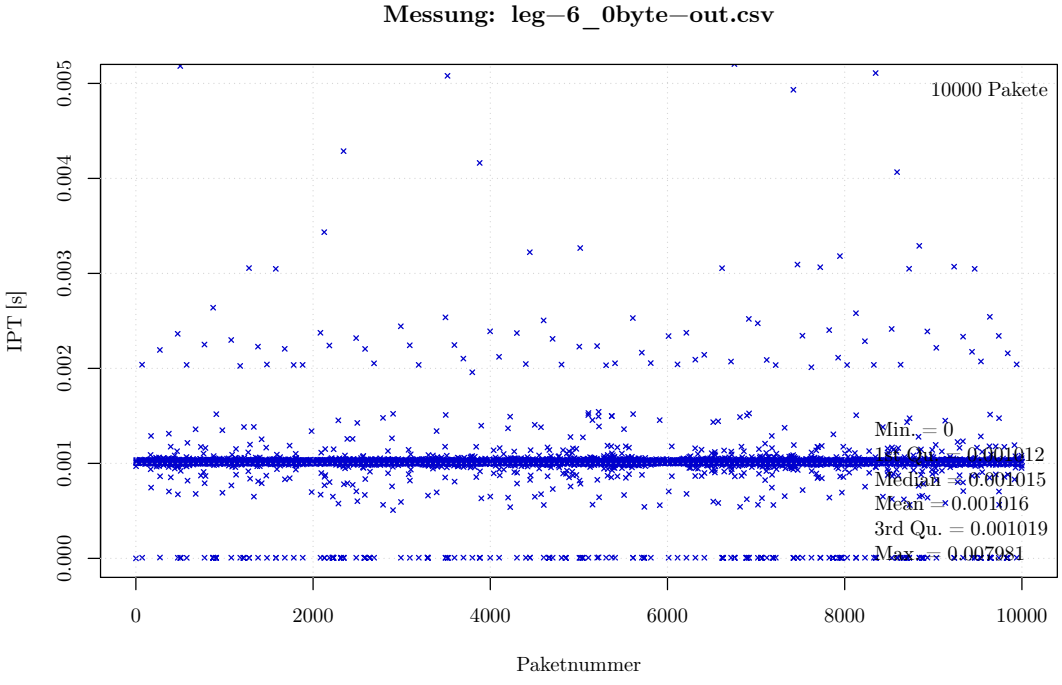
Als erstes wird in dieser Messreihe untersucht, inwiefern das Übertragungsverhalten vom gewählten Frequenzbereich beeinflusst wird. Hierbei ergeben sich Unterschiede dahingehend, dass die IPTs im 2,4 GHz-Bereich weniger stark streuen als es bei einem Kanal im 5 GHz-Band der Fall ist. Aufgrund der beschränkten Auswahl an Hardware mit Dualbandunterstützung wird allerdings keine Vergleichsmessreihe durchgeführt. Da weiterhin der *Spectrum Analyzer* nicht zur Überprüfung dieses Messaufbaus geeignet ist und somit Störungen nicht zuverlässig ausgeschlossen werden können, wird auf weitere Versuche verzichtet. Auch wegen der geringeren Verbreitung werden im Folgenden nur noch 2,4 GHz-Kanäle betrachtet.

Einen ausgeprägten Einfluss auf den IPT-Verlauf hat die Übertragungsgeschwindigkeit. Diesbezüglich werden sowohl die Datenraten des Kompatibilitätsmodus als auch die MCS-Indizes überprüft. Die Übertragungsverfahren von 802.11b, g und n wirken sich hierbei jeweils unterschiedlich auf den IPT-Verlauf aus. Abb. 4.7 veranschaulicht Unterschiede im Übertragungsverhalten zwischen 802.11b und g. Während bei b die IPTs phasenweise streuen (Abb. 4.7a), verlaufen sie bei g konstant (Abb. 4.7b). Zum Vergleich der Datenraten desselben Standards sind in Abb. 4.8 zwei 802.11n-Modulationsstufen gegenübergestellt. Die IPT-Streuung nimmt dabei mit höheren Übertragungsraten immer mehr zu. So liegt die maximale Laufzeitverzögerung bei MCS 0 unter 5 ms und bei MCS 5 über 10 ms. Auch hier unterscheiden sich jedoch die Mittelwerte kaum. Bei höheren Indizes als MCS 5 kommt es schließlich zu Paketverlusten, sodass die entsprechenden Messungen nicht mehr aussagekräftig sind. Somit sind im Messaufbau mit der *TP-Link*-Karte auch keine MIMO-Messungen möglich. Aufgrund der gefundenen Unterschiede sollte es aber prinzipiell möglich sein, einen Wechsel der Datenrate anhand des IPT-Verlaufs festzustellen. Weitergehende Aussagen sind wegen des starken Hardwareeinflusses nicht möglich.

Bei weiteren Messungen ergibt sich, dass die Verwendung von RTS/CTS die Übertragungscharakteristik im störungsfreien Fall kaum verbessert. Auch für QoS-Pakete können lediglich äußerst schwache Auswirkungen beobachtet werden. Bei Verschlüsselung schließlich können keine Auswirkungen auf die IPTs gefunden werden.

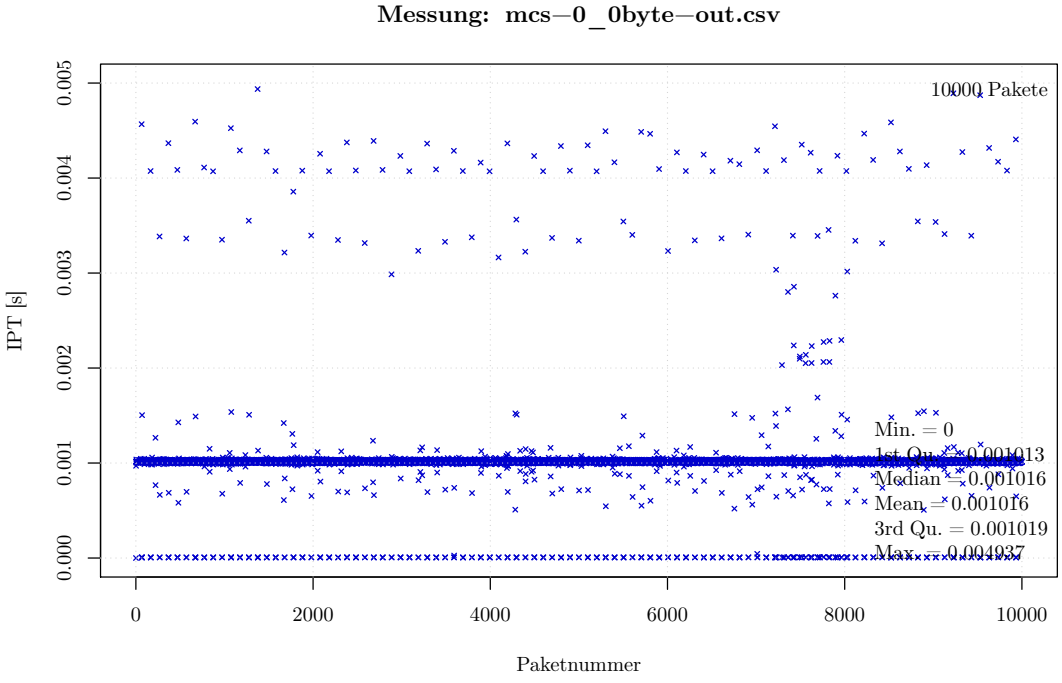


(a) IPT-Verlauf bei 5,5 Mbit/s (802.11b).

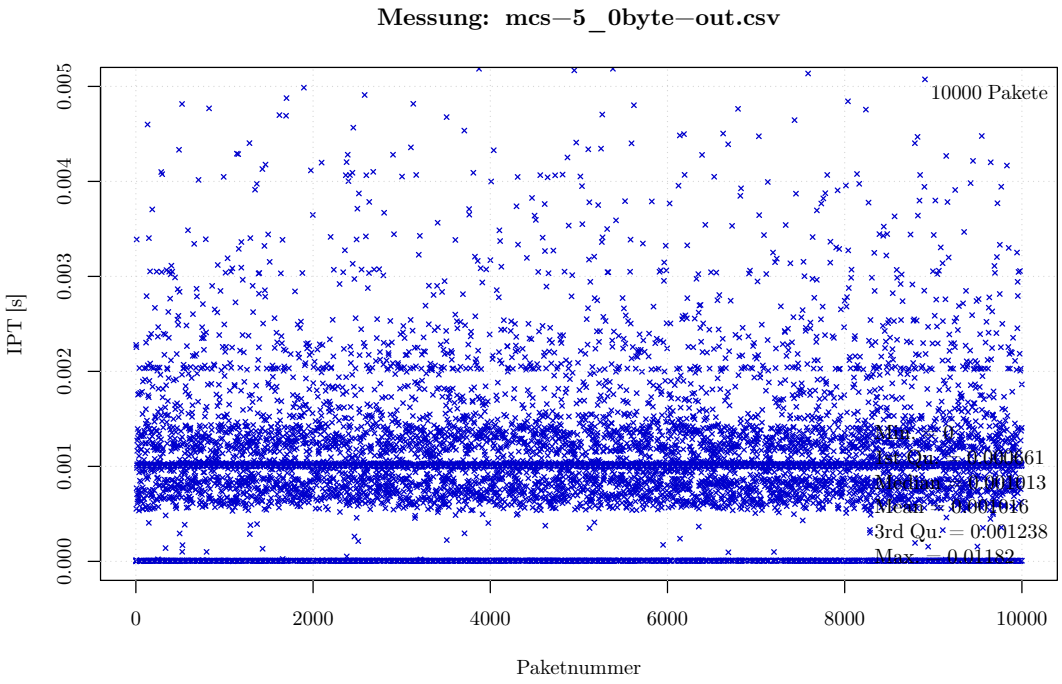


(b) IPT-Verlauf bei 6 Mbit/s (802.11g).

Abbildung 4.7: *Einfluss der Übertragungsrate auf das Paketverhalten.*



(a) IPT-Verlauf bei MCS 0.



(b) IPT-Verlauf bei MCS 5.

Abbildung 4.8: *Einfluss des MCS-Indizes auf das Paketverhalten.*

b) Messaufbau mit Störungen

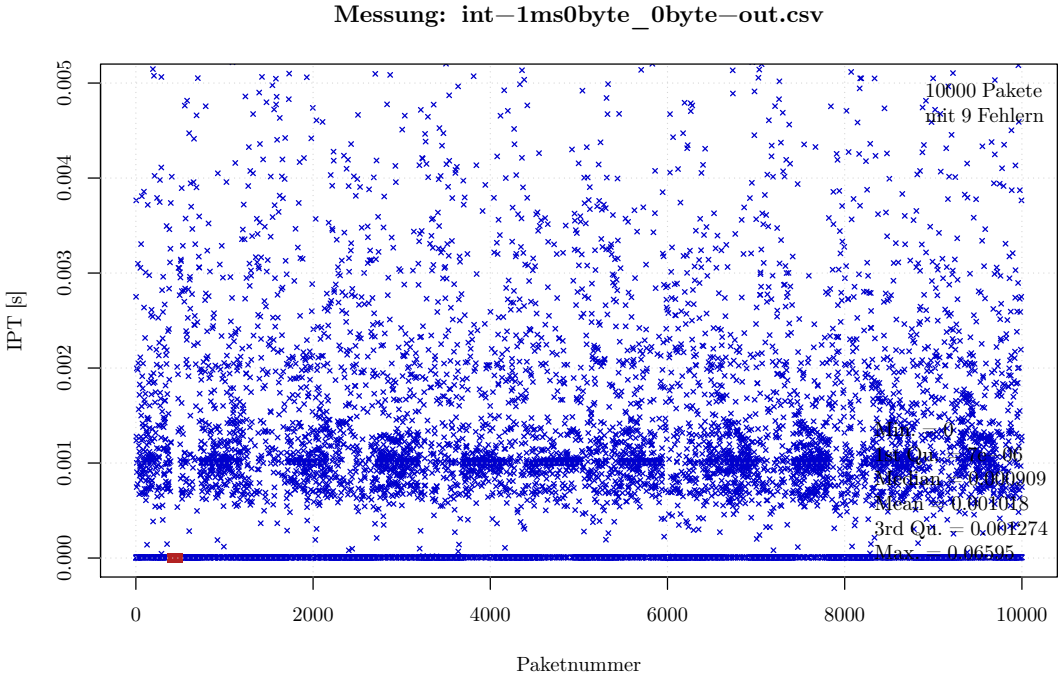
(i) Interferenzverhalten:

Zur Untersuchung des Einflusses von Interferenzen auf das Übertragungsverhalten wird die Teststrecke um ein zusätzliches Störnetzwerk erweitert. Zur gleichförmigen Störung wird eine zweite Paketquelle eingesetzt. Mittels entsprechender Kanalbelegung und unterschiedlich starker Auslastung werden so verschiedene Szenarien simuliert. Wie bereits aus der Konzeption hervorgeht, ermöglicht dieser Aufbau nur die Analyse WLAN-spezifischer Interferenzen. Weitere Störquellen werden vorerst also nicht berücksichtigt.

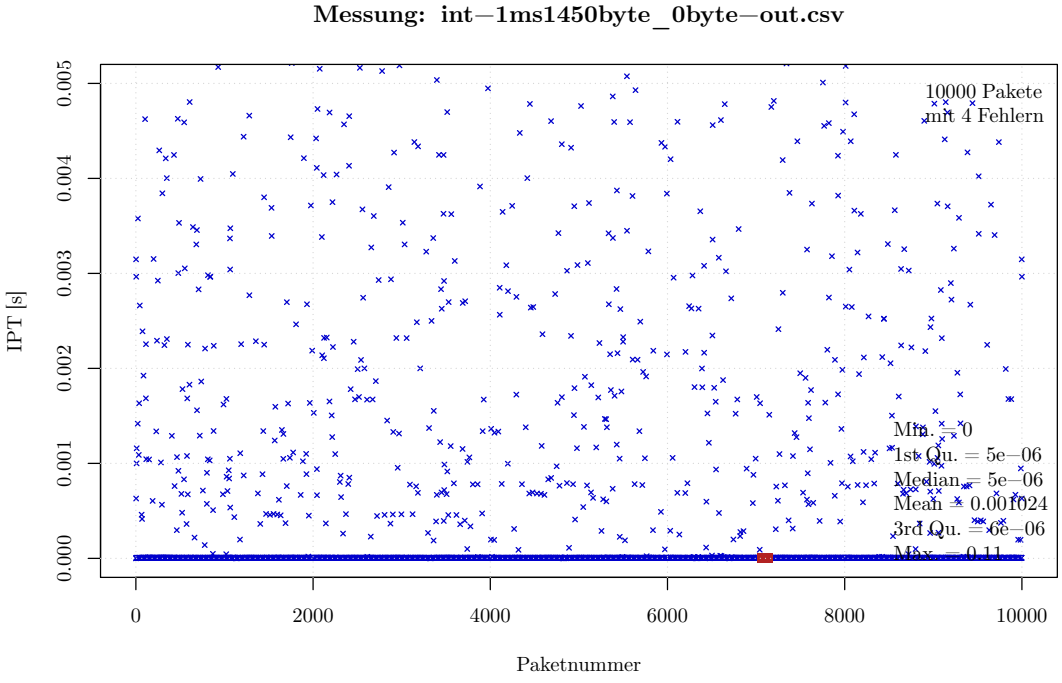
Wie in Abb. 4.9 ersichtlich, führen Paketkollisionen dazu, dass die IPTs verstärkt streuen und es zu Paketverlusten kommt. Die dargestellten Messungen zeigen die Auswirkungen unterschiedlicher Datenraten im Störnetzwerk (≈ 1 *bzw.* $12\,Mbit/s$) bei direkter Kanalüberlappung. Obwohl der Mittelwert – wie in den vorherigen Messungen auch – bei 1 ms bleibt, erhöht sich die maximal gemessene Laufzeitverzögerung auf bis zu 110 ms. Wie bei UMTS macht sich dies in den Diagrammen auch durch die allgemein beobachtbare Zunahme an „0er"-IPTs ($IPT_{in} = 1\,ms \Rightarrow IPT_{out} \ll 1\,ms$) bemerkbar. Dabei deckt sich dieses Verhalten teilweise mit den Auswirkungen höherer MCS-Indizes (vgl. Abb. 4.9a und Abb. 4.8d). Allerdings ist das Streuverhalten bei direkten Interferenzen weniger konstant und vor allem stärker ausgeprägt ($IPT_{max,MCS5} = 12\,ms < IPT_{max,Int1} = 66\,ms$). Auch kommt es durch Paketkollisionen nur zu vergleichsweise wenigen Komplettverlusten an Testpaketen, wie sie beispielsweise bei Messungen ab MCS 5 problematisch sind.

Versuche mit teilüberlappenden Kanälen zeigen, dass das beschriebene Interferenzverhalten in erster Linie bei direkten Kanalüberlagerungen und hohen Netzwerkauslastungen beobachtbar ist. Abb. 4.10a zeigt den IPT-Verlauf einer entsprechenden Messung, unter Nutzung der WLAN-Kanäle 11 und 13 (Stördatenrate $\approx 12\,Mbit/s$). Die Laufzeitverzögerungen liegen dabei unter 10 ms und somit im Bereich der hardwarespezifischen Einflüsse. Sollte diese Beobachtung auf Interferenzen anderer Herkunft übertragbar sein, so ist auch hierbei nur mit geringen Störungen im Übertragungsverhalten von WLAN zu rechnen.

Auch RTS/CTS wirkt sich insbesondere bei größerer Auslastung des Störnetzwerks aus. Bei kleinerer Störrate kommt es zu abschnittsweisen Schwankungen des IPT-Verlaufs, wie sie in Abb. 4.10b dargestellt sind. Insgesamt wird bei der Verwendung von RTS/CTS neben dem Absinken der maximale Paketlaufzeit ($IPT_{max,RTSCTS} = 79\,ms < IPT_{max,Int2} = 110\,ms$) vor allem eine ausgeprägte Reduktion der tatsächlichen Paketverluste beobachtet.

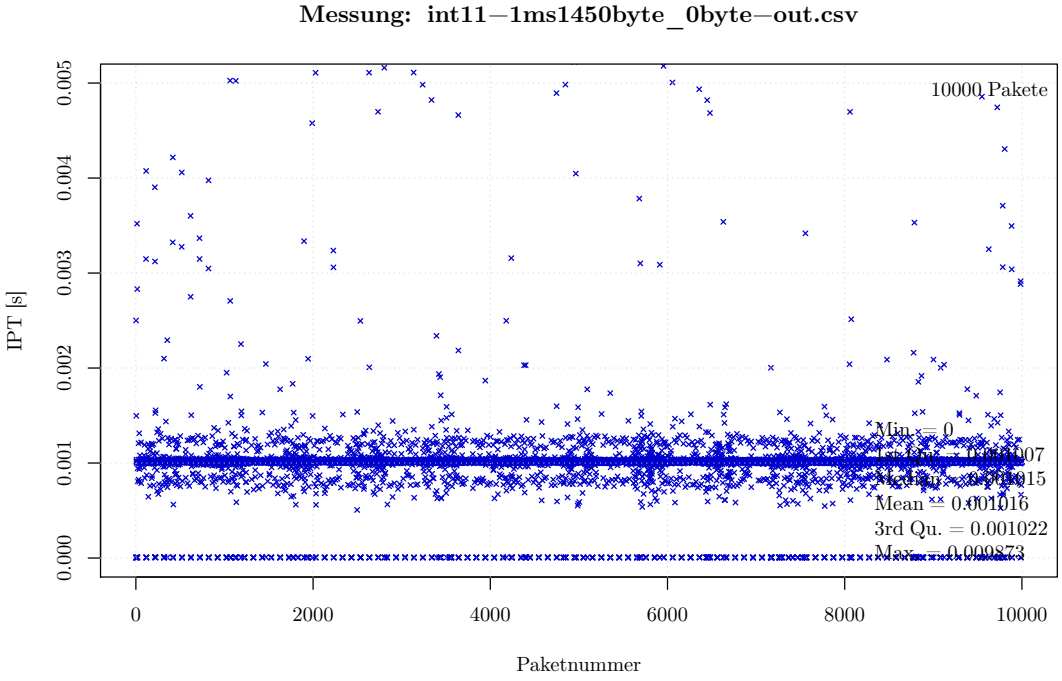


(a) IPT-Verlauf bei niedriger Stördatenrate (ca. 100 Byte/ms).

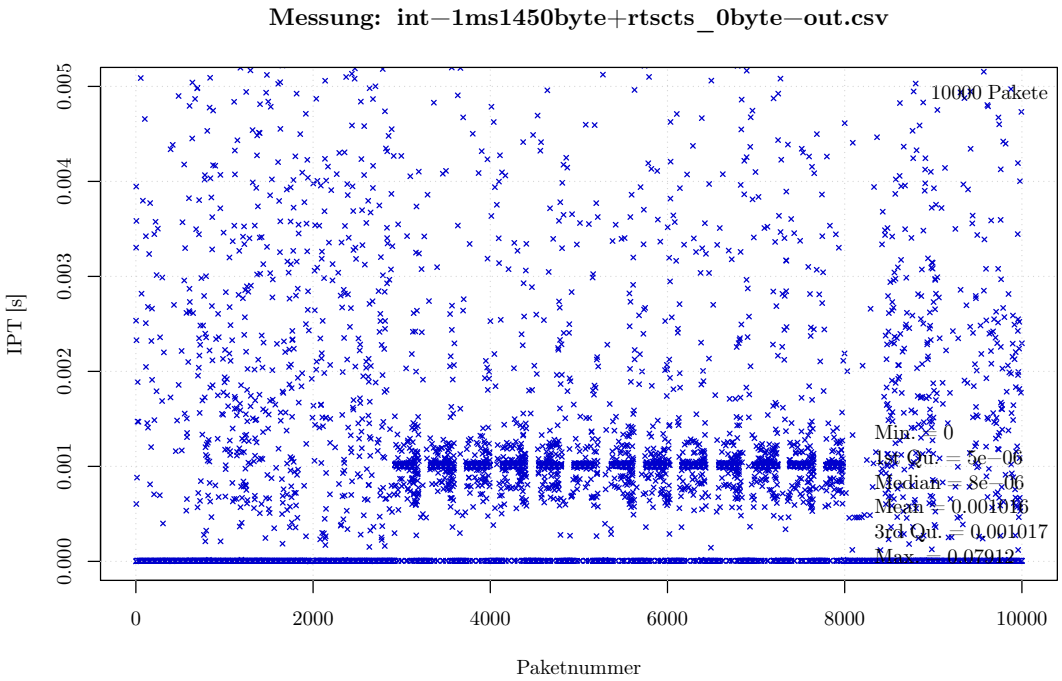


(b) IPT-Verlauf bei hoher Stördatenrate (ca. 1500 Byte/ms).

Abbildung 4.9: *Messergebnisse zu den Auswirkungen des Interferenzverhaltens.*



(a) IPT-Verlauf bei indirekten Interferenzen (hohe Stördatenrate).



(b) IPT-Verlauf mit aktiviertem RTS/CTS (hohe Stördatenrate).

Abbildung 4.10: *Messergebnisse zu den Einflüssen auf das Interferenzverhaltens.*

(ii) Fadingverhalten:

Um einen direkten Vergleich zum Kanalverhalten von UMTS herstellen zu können, wird auch der WLAN-Kanal mittels Fading gestört. Hierfür wird die *SR5500*-Messstrecke des *NetQoS*-Messaufbaus verwendet. Als Fading-Modell kommen die in Abschnitt 3.2 vorgestellten, neun verfügbaren *JTC '94*-Profile zum Einsatz. Zur genauen Auswertung des Wiederholverhaltens wird zusätzlich der *TP-Link*-Stick zum Sniffing im Monitor-Modus genutzt. Wie in Abb. 4.11 veranschaulicht ist, lassen sich somit zusätzliche Informationen – wie über konkrete Paketwiederholungen und das pro Paket verwendete Kodierungsschema – gewinnen.

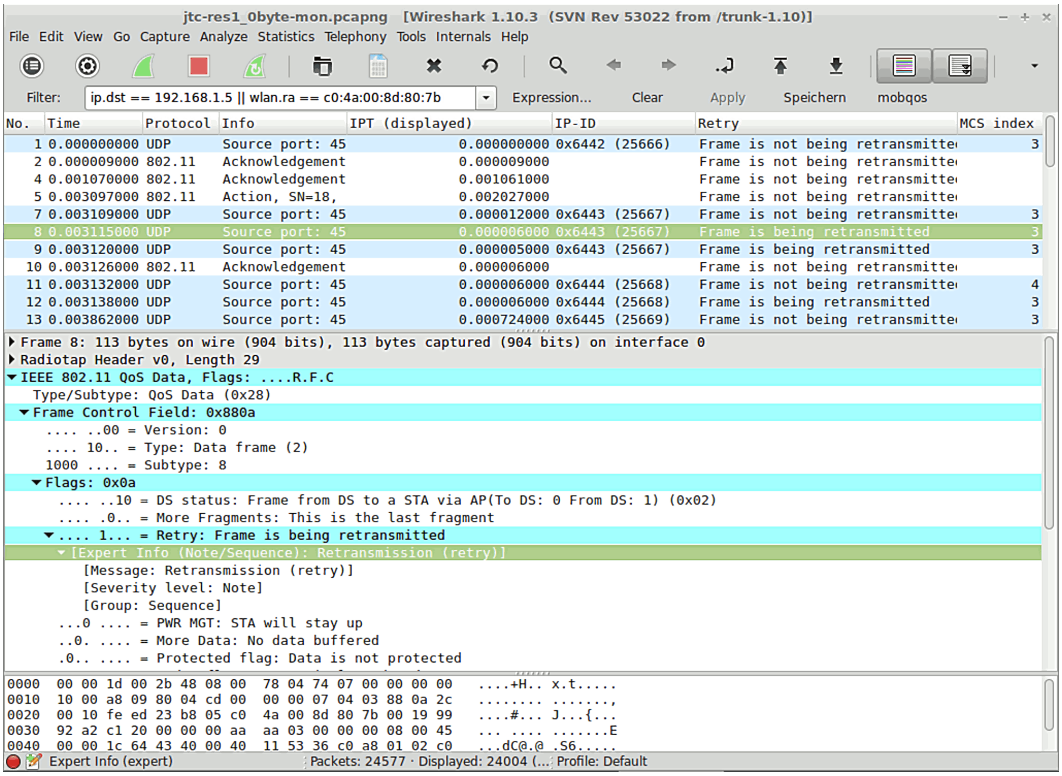
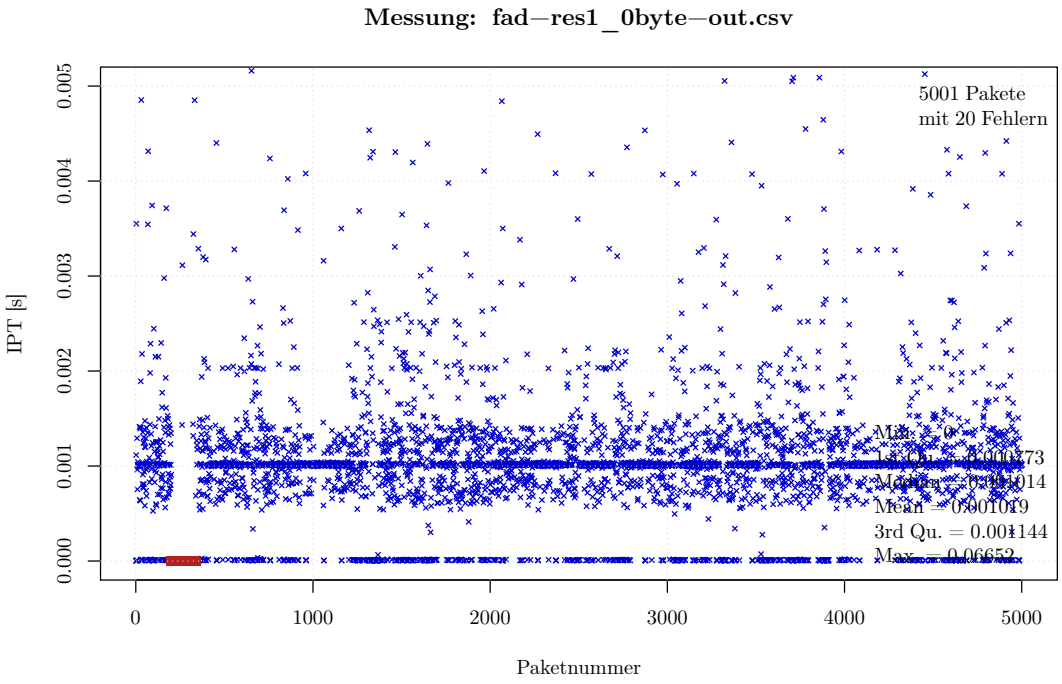
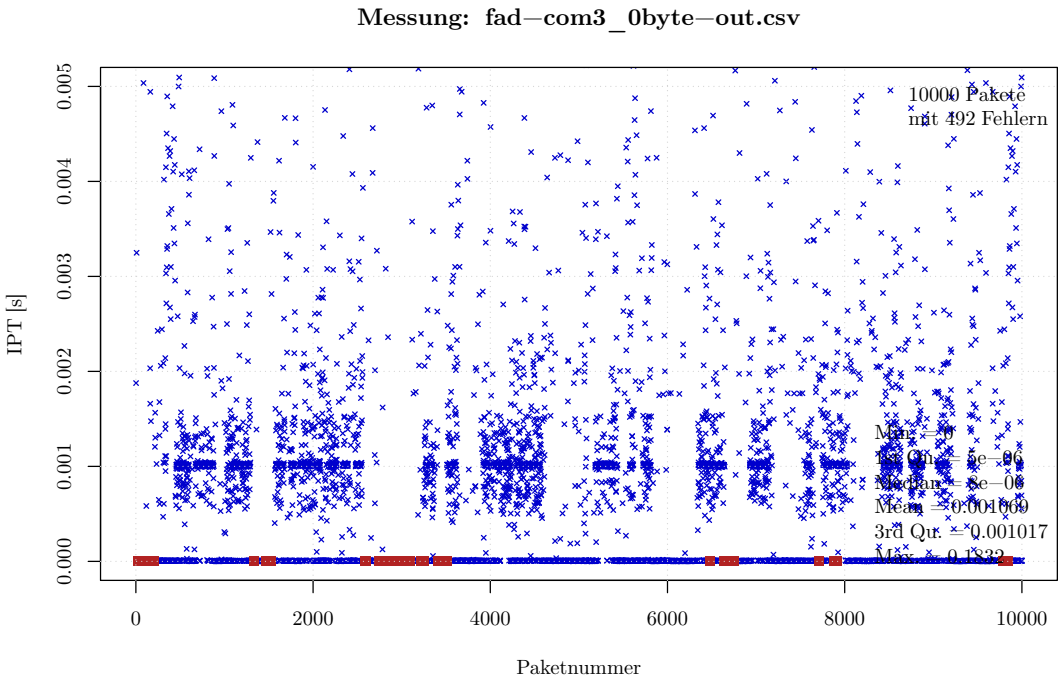


Abbildung 4.11: *Auswertung der Retry- und MCS-Flags.*

Abb. 4.12 zeigt, wie die Streuung der IPTs durch zwei verschieden intensive Fading-Modelle beeinflusst wird. Auffällig sind dabei die abschnittsweisen Schwankungen im Verlauf, die mithilfe der Sniffinginformationen auf einen Wechsel der Übertragungsraten zurückgeführt werden können. Während auch bei starken WLAN-Interferenzen die „0er"-IPTs gleichmäßig verteilt bleiben, kommt es so beim Fading zu einem phasenhaften Verhalten. Und obwohl die maximalen Laufzeitverzögerungen in beiden Fällen vergleichbar sind, führt bereits schwaches Fading zu im Vergleich deutlich höheren Testpaketverlusten ($L_{Int1} = 9 < L_{Fad1} = 20 \ll L_{Fad2} = 492$). Insbesondere bei starken Störungen ist dies somit ein gutes Unterscheidungskriterium.



(a) IPT-Verlauf bei schwachem Fading (Modell für Wohngebäude).



(b) IPT-Verlauf bei starkem Fading (Modell für Geschäftsgebäude).

Abbildung 4.12: *Messergebnisse aus der Untersuchung des Fadingverhaltens.*

c) Zusammenfassung der Messergebnisse

Insgesamt lässt sich für WLAN feststellen, dass das Übertragungsverhalten bisher nur in Teilen erklärbar ist und bereits im störungsfreien Fall erhebliche Unterschiede auftreten. Den deutlichsten Einfluss auf den ungestörten Kanal haben dabei die Hardwareimplementierung und die verwendete Datenrate. Aufgrund der hohen Messauflösung lässt sich auch hier das USB-Busverhalten erkennen. Bei Störungen durch WLAN-Interferenzen und Fading kommt es schließlich zu Laufzeitverzögerungen und zu Komplettverlusten von Testpaketen. Insbesondere die Streuung der IPTs ist dabei abhängig von der Intensität der jeweiligen Störung. Auch lässt sich beobachten, dass Paketkollisionen zu einem gleichmäßigen Anstieg der Paketlaufzeiten führen, die IPT-Verteilung bei Fading jedoch phasenhaft ist. Dieses Verhalten ist auf den fortwährenden Wechsel der MCS-Indizes im Fadingfall zurückzuführen und kann möglicherweise als Unterscheidungskriterium zwischen den Störursachen dienen. Wichtigstes Unterscheidungsmerkmal sind in diesem Fall jedoch die Paketverluste, die bereits bei schwachem Fading beobachtbar sind, bei WLAN-Interferenzen jedoch nur selten auftreten. Dies könnte daran liegen, dass das Medienzugriffsverfahren von WLAN von vornherein speziell auf Paketkollisionen ausgelegt und von daher diesbezüglich entsprechend robust ist (vgl. auch Abschnitt 2.2). Des Weiteren wird beobachtet, dass die Auswirkungen von Interferenzen hauptsächlich bei direkter Kanalüberlappung auftreten. Als mögliche Begründung hierfür bietet sich die Störsicherheit der OFDM-Modulation an (siehe diesbezüglich Abschnitt 2.4).

Des Weiteren können auch bei WLAN – wie schon bei UMTS, wahrscheinlich aufgrund von Pufferung – „0er“-IPTs beobachtet werden. Da deren Verlauf teilweise die Gesamtverteilung der Verzögerungen widerspiegelt, könnten sie sich als einfaches Unterscheidungskriterium zwischen den Störungen eignen.

Obwohl die IPTs theoretisch höchstens im Bereich von 42 ms liegen sollten, werden in Versuchen mit intensiven Störungen solche über 100 ms beobachtet. Eine genauere Auswertung der Messdaten ergibt jedoch, dass es sich hierbei um Ausreißer im Promillbereich (konkret $\lesssim 2\,‰$) handelt. Filtert man diesen heraus, liegen die maximalen Laufzeitverzögerungen exakt im theoretisch berechneten Bereich. Eine Begründung für dieses Verhalten kann im Rahmen der Arbeit nicht gefunden werden.

4.3 Vergleich der Übertragungscharakteristiken

In diesem Abschnitt wird das Kanalverhalten von UMTS und WLAN sowohl theoretisch als auch praktisch gegenübergestellt. Hierzu werden die bisher erarbeiteten Eigenschaften und diesbezüglich gemachte Beobachtungen zusammengefasst und miteinander verglichen.

4.3.1 Theoretische Gegenüberstellung

Offensichtlichster Unterschied zwischen WLAN und UMTS ist die Größe respektive der Einfluss der jeweils spezifizierten Systemebene. Wie in Abb. 4.13 veranschaulicht ist, müssen Testpakete im Mobilfunk allgemein einen weit komplexeren Weg zurücklegen als dies bei lokalen Funknetzwerken der Fall ist. Während die Verzögerungen innerhalb eines WLAN-Netzwerkes in Mikrosekunden angegeben werden, liegen sie bei UMTS im Bereich von hunderten Millisekunden. Die in der Arbeit theoretisch berechnete, maximale Übertragungsdauer bei 802.11n ist ein Bruchteil der einfachen Paketlaufzeit bei UMTS.

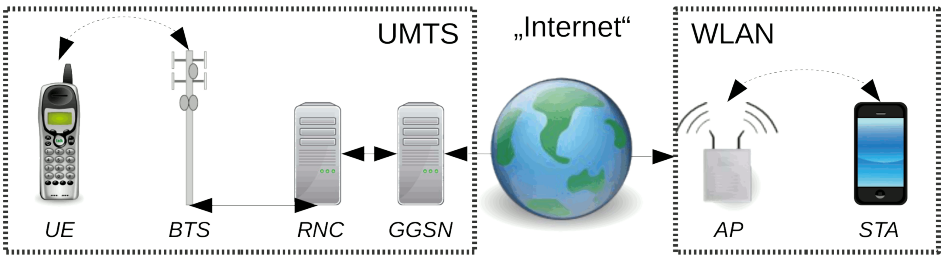


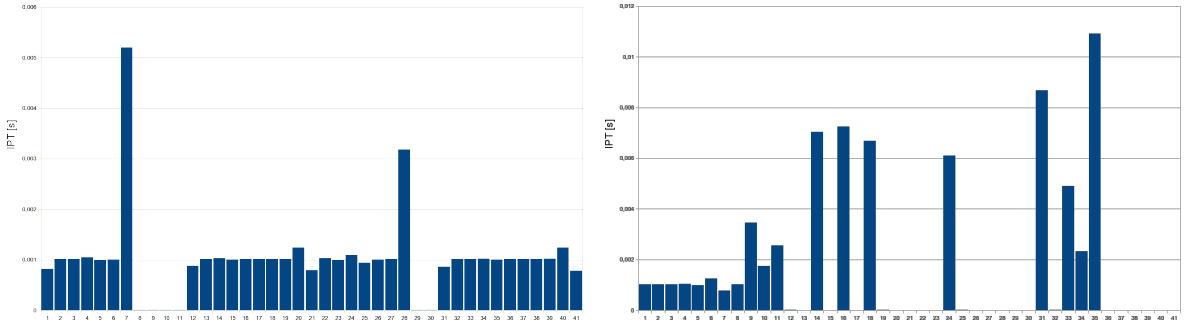
Abbildung 4.13: *Schematische Gegenüberstellung von UMTS und WLAN.*

Auch unterliegt das Kanalverhalten bei 802.11n verschiedenen Einflüssen wie den speziellen, WLAN-spezifischen Einstellungen. Im Mobilfunk hingegen liegt ein klar standardisiertes, deterministisches Verhalten vor. Dies führt dazu, dass Retransmissionen ein grundlegend anderes zeitliches Verhalten aufweisen. Konkret ist im WLAN keine Priorisierung wiederholter Pakete vorgesehen. Somit kann sich in der Theorie auch kein diskretes Verzögerungsverhalten wie im Mobilfunk ergeben. Weiterhin ist bei WLAN keine Unterteilung in Systemebenen- und Retransmissions-spezifisches Verhalten durchführbar.

Insgesamt unterscheiden sich beide Kanäle also bereits in der Theorie – sowohl qualitativ als auch quantitativ. Während für UMTS ein hinreichend gutes Kanalmodell erstellt werden kann, sind für WLAN bisher nur allgemeine Aussagen zum Verzögerungsverhalten möglich.

4.3.2 Praktische Erkenntnisse

Auch in der Realität unterscheidet sich das Kanalverhalten von UMTS und WLAN insbesondere dadurch, dass sich der Mobilfunk insgesamt vorhersehbarer verhält. Während dort ein klar diskretes Wiederholungsverhalten beobachtbar ist, ähnelt der IPT-Verlauf bei WLAN eher einem allgemeinen Fingerabdruck[37]. Dennoch lassen sich in beiden Fällen Störeinflüsse mithilfe der IPTs charakterisieren. Inwiefern für WLAN aber auch die tatsächliche Ursache aus den Paketlaufzeiten rückgeschätzt werden kann, ist bisher nicht bekannt.



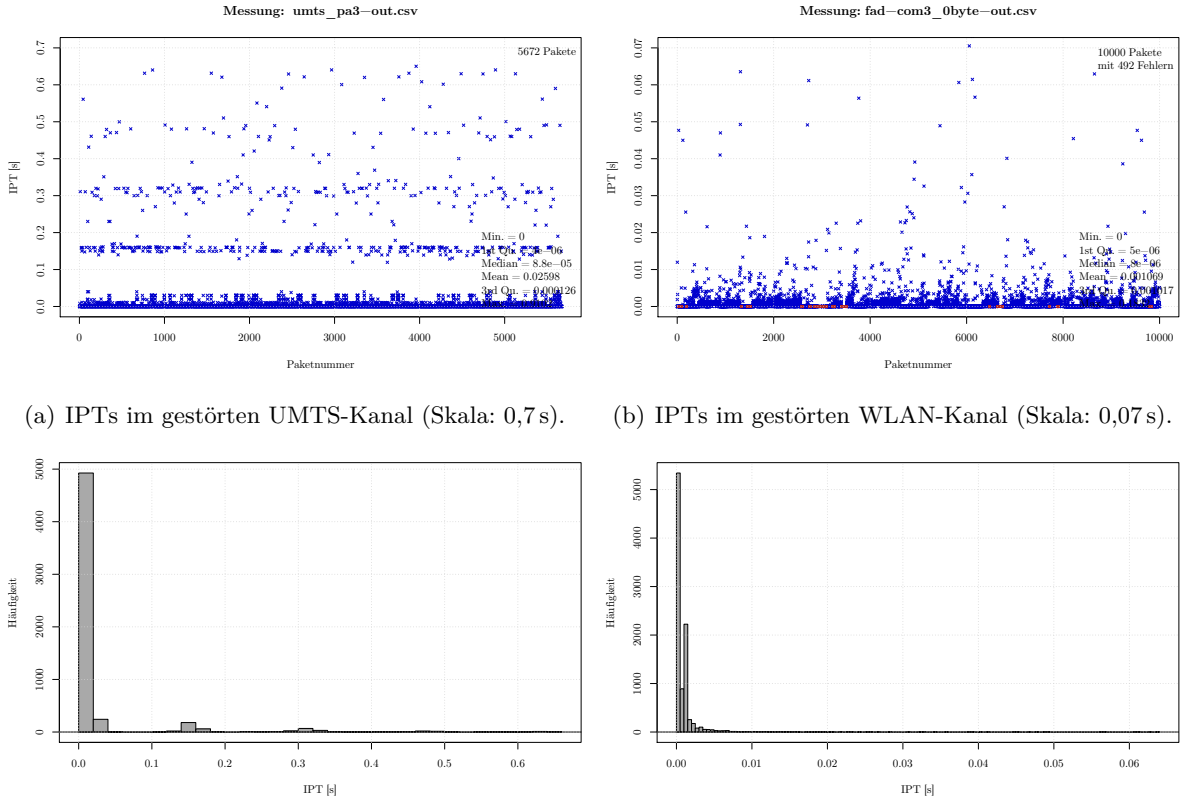
(a) Paketverzögerungen im ungestörten Messaufbau. (b) Paketverzögerungen bei mittelstarkem Fading.

Abbildung 4.14: *Dateilausschnitt aus dem WLAN-spezifischen IPT-Verhalten.*

Wie in Abb. 4.14a zu sehen ist, ähnelt das Paketverzögerungsverhalten des ungestörten WLAN-Kanals dem Retransmissionsverhalten bei UMTS (vgl. Abb. 4.2a). Auffällig ist dabei die mutmaßliche Pufferung, die in beiden Fällen zu den einer vorherigen Verzögerung folgenden „0er“-IPTs führt. Bei 802.11n sind hierfür allerdings keine Kanalstörungen, sondern implementierungsspezifisches Verhalten verantwortlich. Wird das Funknetzwerk zusätzlich gestört, kommt es zu einem – in Abb. 4.14b veranschaulichten – unerklärlichen IPT-Verlauf. Zwar ist auch hier das Pufferungsverhalten ersichtlich, jedoch sind die Verzögerungen unvorhersehbar verteilt. Zusammenhänge zwischen Störursache und Übertragungsverhalten lassen sich daher bislang nur anhand der Gesamtverteilung und unter Einbezug der Sequenzfehler erkennen.

Auch die Paketlaufzeit kann als praktisches Unterscheidungsmerkmal zwischen UMTS und WLAN bestätigt werden. Hierbei ist jedoch zu beachten, dass es bei Störungen zu unerklärlichen Ausreißern kommen kann. Werden diese herausgefiltert, entsprechen die übrigen IPTs der berechneten Größenordnung und können somit als zuverlässige Vergleichsgröße verwendet werden.

[37] Die Verteilung der IPTs ist jeweils symptomatisch für die genauen Parameter einer Messung.



(a) IPTs im gestörten UMTS-Kanal (Skala: 0,7 s). (b) IPTs im gestörten WLAN-Kanal (Skala: 0,07 s).

Abbildung 4.15: *Gegenüberstellung der Übertragungsverfahren im Streudiagramm und Histogramm.*

Zusammenfassend lässt sich WLAN und UMTS also sowohl theoretisch als auch praktisch anhand der IPTs unterscheiden. Wichtigstes Unterscheidungsmerkmal ist hierbei die Paketlaufzeit, die bei 802.11n mindestens um eine Größenordung geringer ist als beim *Release 99* (vgl. Abb. 4.15). Auch sind die bei UMTS beobachtbaren Retransmissionslinien bei WLAN nicht zu finden. Ähnlich wie beim Mobilfunk beeinflussen auch bei WLAN verschiedene Störungen die IPTs auf eine unterschiedliche Art und Weise. Allerdings ist das Übertragungsverhalten deutlich komplizierter und zugleich implementierungsabhängiger als bei UMTS.

Aus QoS-Sicht ist festzuhalten, dass bei WLAN die Paketlaufzeiten deutlich kürzer sind als bei UMTS. Als problematischer sind somit tatsächliche Paketverluste zu erachten, die insbesondere auch von der eingesetzten Hardware und der Datenrate abhängig sind. Insgesamt ist QoS in 802.11n-Netzen eher aus Sicht der Netzwerkauslastung ein Thema, wohingegen bei UMTS auch systemebenenspezifische Einflüsse eine Rolle spielen. Weiterhin ist 802.11n bei Nutzung der DCF ein *Best Effort*-Netzwerk, entsprechend werden alle Pakete gleich behandelt. Die HCF spezifiziert zwar eine Dienstgüte-Zusicherung mittels entsprechender Verkehrsklassen, ist bisher aber nicht weit verbreitet.

5 Zusammenfassung

Um den Vergleich spezifischer Übertragungscharakteristiken zwischen WLAN und UMTS zu ermöglichen, werden im Rahmen dieser Arbeit verschiedene theoretische Überlegungen gemacht und entsprechende Messungen durchgeführt. Diese stehen dabei in engem Zusammenhang zu den Forschungen des *NetQoS*-Projekts der *Hochschule München*.

Zu Beginn der Arbeit wird die Inter-Packet Time – von zeitlich konstant versendeten UDP-Paketen – als Charakterisierungsmaß eingeführt und es werden die zum Verständnis der Arbeit benötigten Hintergründe zu WLAN, UMTS und zur Funkübertragung zusammengetragen. Auf diesen Grundlagen aufbauend wird ein Konzept für entsprechende WLAN-Versuche erarbeitet. Diesbezüglich findet auch eine Einarbeitung in die im Rahmen des Messaufbaus genutzte Hard- und Software statt und es wird eine beispielhafte Versuchsdurchführung nachvollzogen. Bei den Messungen wird neben eigens entwickelten Programmen – wie der echtzeitfähigen *udp.c*-Paketquelle und dem *R*-Skript zur Datenauswertung – auch ein projektspezifisches Messprotokoll verwendet.

Im Rahmen der Ergebnisanalyse wird das bereits bekannte, im Paketwiederholungsfall diskretisierte Übertragungsverhalten von UMTS beschrieben und mithilfe eigener Messungen verifiziert. Weiterhin können auch neue Erkenntnisse zum USB-Busverhalten gewonnen werden. Die anschließende Erforschung des WLAN-Kanalverhaltens für 802.11n ergibt eine nichtdeterministische IPT-Verteilung. Hier treten bereits im störungsfreien Fall erhebliche, implementierungsabhängige Unterschiede auf. Aber auch Störungen durch WLAN-Interferenzen und Fading wirken sich unterschiedlich auf das beobachtete Übertragungsverhalten aus. Dies wird unter anderem damit zu begründen versucht, dass der WLAN-Standard auf Paketkollisionen ausgelegt ist und sich daher diesbezüglich stabiler verhält. Aufgrund von beobachteten IPT-Schwankungen bei den Fading-Messungen wird weiterhin die These aufgestellt, dass sich Störursachen auch anhand des Verlaufs der „0er“-IPTs unterscheiden lassen.

In der abschließenden Gegenüberstellung von WLAN und UMTS werden die unterschiedlich großen Paketlaufzeiten sowie die Vorhersehbarkeit des IPT-Verlaufs als klare Unterscheidungsmerkmale benannt. Zusätzlich werden die Ergebnisse kurz aus QoS-Sicht diskutiert, wobei für 802.11n hauptsächlich die Netzwerkauslastung als kritisch betrachtet wird.

6 Fazit und Ausblick

Obwohl im Rahmen dieser Masterarbeit keine mit den Erkenntnissen bei UMTS vergleichbare Kanalklassifizierung für WLAN gefunden werden konnte, können sich dennoch manche über die eigentliche Aufgabenstellung hinausgehende Resultate im Rahmen des *NetQoS*-Projekts als nützlich erweisen.

Beispielsweise sollte aufgrund der Beobachtung, dass das bisher beschriebene UMTS-Übertragungsverhalten nur spezifisch gilt, ein allgemeinerer Forschungsansatz verfolgt werden. Neben den bisherigen Erkenntnissen zum *Release 99* und den am Rande dieser Arbeit durchgeführten HSDPA-Vergleichsmessungen sind unbedingt auch andere Netzwerkspezifikationen zu untersuchen. Diesbezüglich sind sowohl die Auswirkungen der Systemebene – insbesondere real existierender Implementierungen – als auch mögliche, hardwarebedingte Einflüsse zu berücksichtigen. In gleicher Weise sollte die Basis an Messdaten zur Erforschung des WLAN-Kanalverhaltens weiter erhöht werden. Wichtig ist in diesem Zusammenhang ein sauberes, wissenschaftliches Vorgehen, bei dem die jeweiligen Versuche klar beschrieben und die Messergebnisse archiviert werden. Entsprechend ausführlich sind im Rahmen des *NetQoS*-Projekts weitere Übertragungsverfahren – wie neuere Mobilfunkstandards oder Festnetzanschlüsse – zu untersuchen. Mit den in dieser Arbeit entwickelten Programmen stehen hierfür geeignete Werkzeuge zur Verfügung.

Zwar ist die WLAN-spezifische Übertragungscharakteristik nicht so einfach und klar wie bei UMTS, doch lässt sich die Kanalqualität beziehungsweise die Störursache möglicherweise auch in einem 802.11n-Funknetzwerk anhand der IPT-Verteilung bewerten. Insgesamt entspricht das Paketverhalten hier aber eher einem Fingerabdruck. Somit ist keine einfache Fehlersequenzableitung durch Thresholding – wie sie im *MobQoS*-Projekt zur Erstellung der HMM-Kanalmodelle genutzt wurde – mehr möglich. An dieser Stelle gilt es, über einen neuen Modellierungsansatz nachzudenken. Eventuell lässt sich das Übertragungsverhalten auf IP-Ebene auch durch Floatingpoint-basierte HMM-Modelle beschreiben. Oder die Modellierung ist sogar nur unter Verwendung der im Rahmen der Arbeit eingeführten „0er“-IPTs möglich.

Insgesamt bieten sich somit folgende Ansätze für weitere Forschungen an:

- Erweiterung des Wissens über UMTS auf allgemeinere und realistische Szenarien.
- Weitere Erforschung und Verifizierung des hier beschriebenen WLAN-Verhaltens.
- Zusätzliche Untersuchungen anderer Übertragungsverfahren, wie LTE oder DSL.

Konkret für WLAN sollte dabei noch untersucht werden:

- Auswirkungen von AWGN-Rauschen und Fremdinterferenzen.
- Bestätigung des vorgestellten IPT-Verlaufs für weitere Hardware (insbesondere die Übertragung der Ergebnisse dieser Arbeit auf USB-Sticks).
- Weitere Nachforschungen zum Einfluss des PCIe-Busses und der Rechnerhardware (zum Beispiel durch die Substitution des externen APs durch eine interne WLAN-Karte).

Die Kanalmodellierung im *NetQoS*-Projekt betreffend ergeben sich folgende Punkte:

- Studie der Aussagekraft der „0er“-IPTs.
- Machbarkeitsanalyse für Gleitkomma-basierte HMMs.
- Allgemeines Überdenken der bisherigen Modellbildung.

Bei den genannten Vorschlägen sollte nie das „Große und Ganze“ – nämlich die Modellierung und Klassifizierung heterogener Netzwerke – aus den Augen verloren werden.

Abschließend kann festgestellt werden, dass die Ergebnisse dieser Arbeit sowohl zu einem *NetQoS*-spezifischen Verständnis des WLAN-Kanals beitragen als auch neue Herausforderungen für die Forschung aufzeigen. Hierfür werden die im Rahmen dieser Masterarbeit entwickelten Tools und die entsprechende Projektdokumentation zur Verfügung gestellt.

„We can only see a short distance ahead,
but we can see plenty there that needs to be done.“ – Alan Turing[38]

[38] Aus *Computing machinery and intelligence* (1950)

Literatur

[Air08] AirMagnet: *802.11n Primer*. White Paper, AirMagnet Inc., August 2008. http://airmagnet.flukenetworks.com/assets/whitepaper/WP-802.11nPrimer.pdf.

[Bar07] Baris Güzelarslan: *Auswirkungen des UMTS Kanalverhaltens auf IP basierte Kommunikation*. Masterarbeit, Fachhochschule München, September 2007.

[Bar11] Baris Güzelarslan, S. Struck, M. Dippold, M. Paul, T. Michael: *A Hidden Markov based End-to-End Architecture to Measure, Model, Emulate, and Estimate Wireless Access Network Characteristics*. In: *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*, Oktober 2011. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6078903.

[Bar12] Baris Güzelarslan, Michael Dippold, Manfred Paul: *Efficient and automatized error pattern modelling with hidden Markov models in digital communication*. International Journal of Electronics and Communications (AEÜ), Mai 2012. http://www.sciencedirect.com/science/article/pii/S1434841111002524.

[Bun13] Bundesnetzagentur: *Jahresbericht 2013*. Technischer Bericht, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mai 2013. https://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/Publikationen/Berichte/berichte-node.html.

[Car02] Carlo Demichelis, Philip Chimento: *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)*. RFC 3393 (Proposed Standard), November 2002. http://www.ietf.org/rfc/rfc3393.txt.

[Cis07] Cisco Systems: *802.11n: The Next Generation of Wireless Performance*. White Paper, Cisco Systems Inc., August 2007. http://faculty.ccri.edu/jbernardini/JB-Website/ETEK1500/1500Notes/802.11n-NextGen-Cisco.pdf.

[Fab10] Fabian Harrer: *Auswertung und Modellierung von Fadingmessungen*. Bachelorarbeit, Hochschule München, März 2010.

[Har10] Harri Holma, Antti Toskala: *WCDMA for UMTS: HSPA Evolution and LTE*. John Wiley & Sons, Chichester, 5 Auflage, September 2010. http://proquest.tech.safaribooksonline.de/9781119991908.

[Hew11] Hewllet-Packard Company: *HP MSM3xx / MSM4xx Access Points – Management and Configuration Guide*, v5.5.0 Auflage, Mai 2011. h20564.www2.hp.com/bc/docs/support/SupportManual/c02702808/c02702808.pdf.

[Int01] Intersil: *Multipath Measurement in Wireless LANs*. Application Note, Intersil Americas Inc., Oktober 2001. http://airmagnet.flukenetworks.com/assets/whitepaper/WP-802.11nPrimer.pdf.

[Jü09] Jürgen Plate: *Grundlagen Computernetze*. http://www.netzmafia.de/skripten/netze/index.html, März 2009.

[Kla10] Klaus Wehrle, Mesut Günes, James Gross: *Modeling and Tools for Network Simulation*. Springer, Berlin, September 2010. http://link.springer.com/book/10.1007%2F978-3-642-12331-3.

[LAN09] LANCOM: *IEEE 802.11n im Überblick*. Tech Paper, LANCOM Systems GmbH, September 2009. http://www.lancom-systems.de/fileadmin/pdfs/techpapers/TP-80211n_overview-DE.pdf.

[Mar09] Marcus Burton: *802.11 Arbitration*. White Paper, Certified Wireless Network Administrator, September 2009. http://www.cwnp.com/wp-content/uploads/pdf/802.11_arbitration.pdf.

[Mar13] Martin Sauter: *Grundkurs Mobile Kommunikationssysteme*. Springer Vieweg, Wiesbaden, 5 Auflage, 2013. http://link.springer.com/book/10.1007%2F978-3-658-01461-2.

[Mic07] Micro/sys: *Interrupts and USB*. White Paper, Micro/sys Inc., Mai 2007. http://www.embeddedsys.com/subpages/resources/images/documents/InterruptsAndUSB.pdf.

[Mus02] Mustafa Ergen: *IEEE 802.11 – Tutorial*. Monographie, University of California Berkeley, Juni 2002. http://www.eecs.berkeley.edu/~ergen/docs/ieee.pdf.

[ORB06] Orebaugh, Angela, Gilbert Ramirez und Jay Beale: *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress Publishing, Rockland, Dezember 2006. http://proquest.safaribooksonline.com/9781597490733.

[Paw14] Pawel Lüse: *Anordnung zur Untersuchung und Vermessung von Funkkanalmodellen im Mobilfunk*. Masterarbeit, Hochschule München, März 2014.

[PCI02] PCI-SIG: *PCI Express*. Base Specification, PCI-SIG, April 2002. http://home.mit.bme.hu/~feher/MSC_RA/External_Bus/pci_express_10.pdf.

[Raj07] Raj Jain: *Channel Models – A Tutorial*. Monographie, WiMAX Forum, Februar 2007. http://www.cse.wustl.edu/~jain/cse574-08/ftp/channel_model_tutorial.pdf.

[Roh07] Rohde & Schwarz: *Handheld Spectrum Analyzer – R&S FSH*, v5.5.0 Auflage, August 2007. http://cdn.rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_manuals/gb_1/f/fsh_1/archive_27/FSH_Bedienhandbuch_15.pdf.

[Spi10] Spirent Communications: *Spirent Wireless Channel Emulator – SR5500 Wireless Channel Emulator*, Rev. J Auflage, September 2010. h20564.www2.hp.com/bc/docs/support/SupportManual/c02702808/c02702808.pdf.

[Xia12] Xiaomin Chen: *Coding in 802.11 WLANs*. Doktorarbeit, National University of Ireland, Maynooth, September 2012. http://www.hamilton.ie/publications/xiaomin_thesis.pdf.

Abbildungsverzeichnis

Tabellenverzeichnis

A CD-Rom

A.1 /

↪ Vergleich_spezifischer_Übertragungscharakteristiken_zwischen_WLAN_und_UMTS.pdf

A.2 /Datenbätter/

↪ **Messgeräte**
↪ **WLAN-Hardware**

A.3 /LaTeX/

↪ compile.sh
↪ document.tex
↪ referenzen.bib
↪ _pdfcreator.R
↪ _pdfcreator.sh
↪ _pdfcrop.sh

A.4 /Messdaten/

↪ IPT-Beispiel.csv
↪ **Fading**
↪ **Hardwareeinfluss**
↪ **Interferenzen**
↪ **Mobilfunk**
↪ **Sniffing**
↪ **Standardeinfluss**
↪ **Verbreitungsanalyse**
↪ **Vorversuche**

A.5 /Programme/

↪ Messprotokoll.pdf
↪ R-Skript.zip
↪ udp.c
↪ _auswertung.sh
↪ _routing-quick.sh

A.6 /Projektdokumentation/

↪ Accuracy-Analysis.pdf
↪ Bestellungen.pdf
↪ Datengewinnung.pdf
↪ Datenverarbeitung.pdf
↪ Einarbeitung.pdf
↪ Infrastruktur.pdf
↪ Kanalmodellierung.pdf
↪ Projektdokumentation.pdf
↪ Spickzettel.pdf
↪ Veraltetes.pdf

A.7 /Quellen/

↪ AN_Intersil.pdf
↪ AR_BNetzA.pdf
↪ BK_Grundkurs.pdf
↪ BK_Modeling.pdf
↪ BK_UMTS.pdf
↪ BK_Wireshark.pdf
↪ BT_Fabian.pdf
↪ BT_Talal.pdf
↪ DS_SR5500.pdf
↪ Man_FSH.pdf
↪ Man_HP.pdf
↪ MT_Baris.pdf
↪ MT_Luese.pdf
↪ PA_MobQoS-AEÜ.pdf
↪ PA_MobQoS-IEEE.pdf
↪ PCI_Express.pdf
↪ PhD_Xiaomin.pdf
↪ RFC_3393.pdf
↪ SC_Netze#Einführung.pdf
↪ SC_Netze#TCPIP.pdf
↪ TP_LANCOM.pdf
↪ TU_80211.pdf
↪ TU_Models.pdf
↪ WP_Cisco.pdf
↪ WP_CWNA.pdf
↪ WP_MicroSys.pdf
↪ WP_Primer.pdf

A.8 /Webseiten/

↪ 3gpp_release-1999.pdf
↪ air-stream_ack-timeout.pdf
↪ debian_manpages.pdf
↪ filibeto_realtime.pdf
↪ filibeto.zip
↪ heise_telekom.pdf
↪ hm_mobqos.pdf
↪ kernel_iw.pdf
↪ kernel_realtime.pdf
↪ lrz-muenchen_apstat.pdf
↪ mcsindex.pdf
↪ microsoft_technet.pdf
↪ osdev_usb.pdf
↪ pcisig_faq.pdf
↪ redhat_clocksource.pdf
↪ r.pdf
↪ wifi-insider_wmm.pdf
↪ wikidevi_main.pdf
↪ wikipedia_ism-interference.pdf
↪ wikipedia_koaxiale-steckverbinder.pdf
↪ wikipedia_umts-frequency.pdf
↪ wikipedia_wlan-channels.pdf
↪ wireshark.pdf

Lizenz