Energieeffiziente Netzwahl für mobile Geräte

von Dominik Winkelmeyer

Diplomarbeit im Fach Informatik

Betreut wurde die Arbeit durch
Prof. Dr. Frank Bellosa und Andreas Merkel
am Institut für Betriebs- und Dialogsysteme
der Universität Karlsruhe

7 . Januar . 2008

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation

Die Einsatzmöglichkeiten und die Verbreitung von mobilen und tragbaren Geräten haben in den letzten Jahren stark zugenommen und es ist anzunehmen, dass sich dieser Trend fortsetzen wird. Die Geräte wie beispielsweise Handy, Laptop oder Organizer werden oft dafür eingesetzt, dem Benutzer eine möglichst große Bandbreite an Kommunikationsmöglichkeiten zur Verfügung zu stellen. Besonders häufig kommen dabei drahtlose Übertragungstechniken, unter anderem Funktechnologien, zum Einsatz. Mittlerweile existiert eine große Anzahl verschiedener Funktechnologien, die alternativ zueinander nutzbar sind. Es stellt sich also aktuell die Frage, welche von diesen in einer speziellen Situation genutzt werden kann oder sollte, um ein Gerät mit anderen Geräten oder einem Netzwerk zu verbinden. Ein wesentliches Kriterium zur Beantwortung dieser Frage ist die Energieeffizienz. Da mobile und tragbare Geräte üblicherweise nur über begrenzte Energieressourcen verfügen, ist eine energiesparende und somit ökonomische Nutzung von großem Vorteil. Auf diese Weise kann die Betriebsdauer erhöht und insgesamt Kosten eingespart werden.

In dieser Arbeit werden zwei Funktechnologien hinsichtlich ihrer Energieeffizienz untersucht: Wlan und Bluetooth. Diese beiden Übertragungsstandards wurden ausgewählt, da sie derzeit in vielen mobilen und tragbaren Geräten eingesetzt werden. In der folgenden Arbeit wird ein Modell aufgestellt, das konkret beleuchtet, in welchen Fällen ein Umschalten zwischen diesen beiden möglich und sinnvoll ist. Dabei zeigt sich, dass sich eine geschickte Auswahl der zu nutzenden Übertragungstechnik positiv auf die für die Kommunikation benötigte Energie auswirkt.

1.2 Übersicht

Im Kontext dieser Arbeit werden die beiden Funktechnologien Wlan und Bluetooth untersucht. Dabei wird ein Energiemodell eingeführt, dass es ermöglichen soll, die Ergebnisse dieser Arbeit auch auf andere paketorientierte Übertragungsstandards zu übertragen. Zudem befähigt es hier zwei Netzwerkadapter (für jeweils eine der beiden Technologien) exemplarisch hinsichtlich ihrer Energieeffizienz zu vergleichen. Dabei wird herausgestellt in welchen Situationen der Einsatz eines der beiden Adapter vorzuziehen ist. Da mobile und tragbare Geräte ein potentiell sehr breites Spektrum von Diensten über ein Netzwerk nutzen können, kann sich die Nutzung der Funkverbindung sehr dynamisch ändern. Um auf solche Änderungen zu reagieren, bietet sich unter Umständen die Nutzung eines anderen Übertragungsstandards an. Dies ist jedoch nicht ohne weiteres möglich, ohne dabei laufende Datenübertragungen zu unterbrechen. Daher wurden im Kontext dieser Arbeit Strategien entwickelt, die diesem Umstand begegnen. Dies geschah insbesondere in Hinblick auf die Nutzung des Internet Protokolls (IP).

1.3 Kontext und verwandte Arbeiten

Um Datentransfers über einen Wechsel des Zugangspunktes zu einem IP Netzwerk hinweg aufrecht zu erhalten, existieren bereits einige andere Methoden als, die hier vorgestellte. Diese zeichnen sich jedoch dadurch aus, dass der jeweilige Zugriffspunkt eine direkte Unterstützung für diesen Mechanismus anbieten muss. Ziel der in dieser Arbeit dargestellten Strategie ist es jedoch, auf diese Unterstützung weitestgehend verzichten zu können. Eine genauere Beschreibung der hier eingesetzten Methode sowie deren Legitimation ist in Kapitel 4.2 zu finden.

Insbesondere bei drahtlosen Übertragungstechniken sind oftmals schon durch das eingesetzte Protokoll Maßnahmen vorgesehen, um sie möglichst energieeffizient nutzen zu können. In dieser Arbeit werden einige solcher Strategien aufgegriffen, allerdings nicht mit Fokus darauf den Energiebedarf einer einzelnen Funkverbindung zu senken. Vielmehr werden sie auf Situationen übertragen, in denen mehrere Übertragungsstandards zur Verfügung stehen.

2 Einführung in die verwendeten Funkstandards

Es soll nun eine kurze Einführung erfolgen, die herausstellt, welche die Gemeinsamkeiten, die Funktechnologien Bluetooth und Wlan aufweisen, sind und in welchen Punkten sie sich unterscheiden. Zunächst sollen jedoch diese beiden Begriffe, wie sie auch durch die gesamte Arbeit hindurch verwendet werden, genauer spezifiziert werden. Wenn hier von Wlan die Rede ist, so ist damit primär der Standard IEEE 802.11g gemeint. Dieser ist einerseits so angelegt, dass er zu IEEE 802.11b abwärtskompatibel ist, andererseits existieren noch zahlreiche auf ihm aufbauende wie auch herstellerspezifische Erweiterungen. Daher wird der Begriff Wlan an einigen Stellen etwas allgemeiner benutzt, insbesondere wenn er 802.11b mit einschließt.

Bezüglich der Erweiterungen des Standards bei Bluetooth stellt sich die gegenwärtige Situation anders dar. Produkte, die mit dem Bluetooth Wahrenzeichen zertifiziert sind, werben normalerweise nicht mit Dehnungen des zugrundeliegenden Standards, wie es etwa bei Wi-Fi lizenzierten oft zu finden ist. Dies begründet sich wohl darin, dass es Motivation für die Entwicklung von Bluetooth war, eine drahtlose Verbindung zwischen verschiedensten Arten von Geräten zu gewährleisten und damit die Einhaltung des Standards vor einer möglichst hohen bandbreite steht. So wurde Bluetooth mit besonderer Rücksicht auf unterschiedliche Dienste entwickelt, die solche Geräte anbieten oder nutzen können. In dieser Arbeit bezieht sich der Begriff Bluetooth auf die Version 1.1 dieser Spezifikation, es sei denn, etwas Gegenteiliges wird explizit gesagt. Hier soll noch angemerkt werden, dass die IEEE in Anlehnung an diese Version auch 802.15.1 verabschiedet hat, es jedoch auch konkurrierende Technologien wie etwa ZigBee (802.15.4) gibt, auf die aber nicht weiter eingegangen wird. Eine ähnliche Situation gilt natürlich auch für Wlan, doch an dieser Stelle soll es genügen, neben IEEE 802.11a noch auf HIPERLAN aufmerksam zu machen.

Die beiden nun abgegrenzten Übertragungsstandards bieten sich aus mehreren Gründen an, wenn es um die Frage geht, welche Strategien eingesetzt werden können, um energieeffizientes Arbeiten in Situationen zu unterstützen, in denen mehr als eine drahtlose Funktechnik zur Verfügung steht. Zunächst einmal haben sowohl Wlan als auch Bluetooth eine starke Verbreitung in Endgeräten und gerade die Kombination dieser beiden ist etwa in mobilen und tragbaren Geräten wie PDAs oder Notebooks häufig zu finden. Wo dies nicht der Fall ist, kann eine Nachrüstung oft ohne großen Aufwand erfolgen. Darüber hinaus wird auch der Betrieb von IP Netzen, die in dieser Arbeit betrachtet werden, sowohl für Wlan als auch für Bluetooth durch Betriebssysteme und Treiber weitgehend unterstützt. Zudem weisen sie unter Umständen eine vergleichbare Sendeleistung auf, was im Folgenden noch kurz erläutert wird. Beide Technologien übertragen im ISM Band zwischen 2,400 GHz und 2,483 GHz (2,497 GHz in Japan). Dieses Band ist zwar in den meisten Ländern lizenzfrei (in einigen Ländern nur teilweise) jedoch in der effektiven isotropen Strahlungsleistung (EIRP) eines Senders nach oben begrenzt. Somit wurde für Bluetooth (Klasse 1) Geräte eine EIRP vom maximal 100mW vorgesehen, worauf auch Wlan Geräte in Europa beschränk sind. Da in mobilen und tragbaren Geräten normalerweise eine Vorzugsrichtung bei Funkübertragungen nicht erwünscht ist, kann also davon ausgegangen werden, dass die Antennengewinne verschiedener Übertragungseinheiten primär vom

Wirkungsgrad der jeweiligen Antenne abhängen und somit für solche Geräteklassen größenordnungsmäßig vergleichbar sein sollten.

2.1 Wlan

Der IEEE 802.11g Standard unterteilt das ISM Band (bei 2,4 GHz) in bis zu 14 nicht vollständig überlappungsfreie Kanäle. Die genaue Anzahl hängt davon ab, wie groß dieses lizenzfreie Band in den unterschiedlichen Ländern ist. Funkübertragungen in einem Wlan Netz finden auf einem dieser Kanäle statt. Dabei setzt 802.11b ein Frequenzspreizverfahren (DSSS - Direct Sequence Spread Spectrum) ein, um Daten auf den jeweils 20 MHz breiten Kanälen zu übertragen. Geräte, die dem Standard 802.11g entsprechen, können neben diesem auch auf ein Multiplexverfahren (OFDM - Orthogonal Frequency Division Multiplex) zurückgreifen. Dabei wird letzteres zur Kommunikation zwischen 802.11g Geräten eingesetzt, um einen höheren Durchsatz zu erreichen als dies mit DSSS möglich ist. Da ein voller Duplexbetrieb bei Funkübertragungen normalerweise nicht (nur mit deutlich erhöhtem Aufwand) möglich ist, müssen Maßnahmen ergriffen werden, um die fehlerfreie Übertragung von Informationen zu gewährleisten. Bei Wlan wird dabei CSMA/CA eingesetzt, bei dem der Netzwerkverkehr abgehört und erst gesendet wird, nachdem das Medium für eine gewisse Zeit DIFS (Distributed coordination function Inter Frame Spacing) nicht belegt war. Wurde Netzwerkverkehr festgestellt, so wird diese Zeit bei den sendebereiten Teilnehmern um einen zufälligen Betrag erhöht. Optional können auch kurze Pakete eingesetzt werden, um das Medium für eine gewisse Zeit zu reservieren; was der Empfänger zunächst noch bestätigt (RTS/CTS: Ready/Clear To Send). Auf diese Weise können auch an dem Transfer unbeteiligte Geräte die Reservierung des Netzes erkennen. Normalerweise wird diese Methode eingesetzt, bevor ein Teilnehmer ein Paket, das eine bestimmte Größe (RTS Threshold) überschreitet, senden möchte, um die Wahrscheinlichkeit einer Störung zu reduzieren. Bei einem Mischbetrieb von 802.11b/g gewährleisten RTS/CTS Pakete gleichzeitig auch die Funktion der Kollisionsvermeidung. Wenn zwei 802.11g Teilnehmer miteinander kommunizieren, setzen sie normalerweise OFDM ein. Diese Übertragung bleibt einem 802.11b Gerät jedoch verborgen, sodass es das Medium als unbelegt erkennt und eventuell zeitgleich eine eigene Übertragung startet. Wenn der OFDM Übertragung jedoch ein mittels DSSS übertragenes RTS/CTS Paar vorausgeht, welches die Dauer ankündigt, für die das Medium belegt sein wird, so kann das nachfolgende Paket übertragen werden, ohne dass gleichzeitig ein 802.11b Gerät das Medium nutzt. Eine Variante hiervon ist das sogenannte CTS-to-self. Dabei sendet ein 802.11g Teilnehmer unmittelbar vor der Übertragung ein CTS Paket an sich selbst, welches ausreicht, um die Belegung des Mediums zu propagieren. Dem Problem des versteckten Senders wird damit jedoch nicht begegnet. Dieses kann dann auftreten, wenn zwei verschiedene Sender weit genug voneinander entfernt sind, um die Übertragungen des jeweils anderen nicht erkennen zu können, und sich mindestens einer der Empfänger im Überlappungsbereich beider Signale befindet. Der Einsatz eines RTS/CTS Paares kann diese Situation entschärfen, weil der Empfänger in diesem Fall als Vermittler zwischen den Sendern auftritt.

Da eine Funkübertragung deutlich fehleranfälliger ist als eine drahtgebundene, wäre der Aufwand sehr groß, die Fehlerkorrektur allein den höheren Ebenen des ISO-OSI-Schichtenmodells zu überlassen. Daher muss jedes übertragene Paket vom Empfänger einer zyklischen Redundanzprüfung unterzogen und anschließend bestätigt werden. Erfolgt diese Bestätigung nicht, wird die Übertragung solange wiederholt, bis eine Empfangsbestätigung Empfangen wurde oder eine obere Grenze der Wiederholungen erreicht ist. Es ist auch möglich Pakete zu fragmentieren, um den Aufwand für eine erneute Übertragung herunterzusetzen.

Um ein Netz auffindbar zu machen, werden Leuchtfeuersignale (Beacons) verwendet, die auf dem jeweiligen Kanal ausgesendet werden und verschiedene Informationen über das Netz enthalten. Dazu zählen z.B. eine Zeichenkette, die es dem Nutzer erleichtert verschiedene Netze zu unterscheiden und semantisch einzuordnen, die MAC Adresse des Senders, die es ermöglicht verschiedene Teilnehmer auf demselben Kanal zu unterscheiden sowie Informationen über akzeptierte Verschlüsselungsmethoden und Übertragungsgeschwindigkeiten.

Generell ist bei Wlan zwischen zwei verschiedenen Betriebsmodi zu unterscheiden: dem Infrastruktur- und dem Ad-hoc-Modus. Letzterer zeichnet sich dadurch aus, dass die Teilnehmer des Netzes keine verschiedenen Rollen einnehmen sondern das Medium gleichberechtigt nutzen. Das bisher Beschriebene trifft auf beide Betriebsarten zu, wobei im Ad-Hoc Modus die einzelnen Teilnehmer den Versand der Beacons übernehmen. Dieser wird typischerweise verwendet, wenn kurzfristig eine drahtlose Verbindung zwischen wenigen Teilnehmern aufgebaut werden soll. In solchen Netzen werden normalerweise keine Routingprotokolle eingesetzt, um Pakete über mehrere Teilnehmer hinweg zu transportieren, sowie keine Unterstützung für Stromsparfunktionen der einzelnen Teilnehmer. Jedoch lassen sich die beiden zuletzt genannten Punkte nicht verallgemeinern, da es bereits einige Ansätze gibt, die solche Funktionalitäten implementieren ([RFC3626]). Der Infrastruktur-Modus findet normalerweise dort Verwendung, wo ein dauerhaftes, ortsgebundenes Netz aufgebaut werden soll. Dabei übernimmt mindestens ein Teilnehmer die Rolle eines Zugriffspunktes. Typischerweise sendet dieser die Leuchtfeuersignale, stellt eventuell eine Brücke zu anderen Netzwerken bereit, authentifiziert die Teilnehmer des Netzes und koordiniert die Stromsparfunktionen der einzelnen Teilnehmer. Darüber hinaus ist er berechtigt das Medium bevorzugt zu reservieren, indem er - vor einem Zugriff darauf - statt einer Zeitspanne von DIFS eine geringere Zeitspanne von PIFS (Point coordination function Inter Frame Spacing) wartet. Dieses Verfahren (PCF) wird genutzt, um eine wettbewerbsfreie Zeit zu initiieren, in welcher der Zugriffspunkt der Reihe nach allen anderen Teilnehmern eine Zeitspanne einräumt Daten zu senden. Bedingung hierfür ist jedoch, dass neben den wettbewerbsfreien Perioden auch noch solche bestehen, in denen ein verteilter Zugriff auf das Medium möglich ist.

Dies soll als kurze Übersicht von IEEE 802.11b/g genügen, um die wesentlichen Punkte, die in dieser Arbeit Verwendung finden, zu klären. Weitergehende Informationen hierzu findet man im World Wide Web, wo eine Vielzahl von Einführungen und Beschreibungen in dieses Thema existieren. Besonders soll an dieser Stelle jedoch auf die Internetseite des IEEE ([IEEE]) hingewiesen werden.

2.2 Bluetooth

Bluetooth Geräte, die miteinander kommunizieren, bilden ein sogenanntes Piconetz. Ein solches Netz besteht aus bis zu acht Teilnehmern, von denen genau einer die Rolle des Masters einnimmt, alle anderen fungieren als Slaves. Dabei ist nicht festgelegt, welches Gerät zum Master wird, da prinzipiell jedes dazu in der Lage ist. Das ISM-Band wird dabei in 79 sogenannte Hop-Kanäle von jeweils 1 MHz Breite eingeteilt bzw. in 23 solcher Kanäle in Ländern, in denen das Band weniger als 80 MHz breit ist. Alle Teilnehmer eines Piconetzes benutzen einen dieser Kanäle für 625 µs, danach wird nach einem Pseudo-Zufallsprinzip ein anderer Kanal ausgewählt. Dabei wird die Identität des Masters als Parameter für einen Zufallsgenerator benutzt, sodass verschiedene Piconetze auch verschiedene Sequenzen von Kanälen gebrauchen. Welcher Kanal zu einem bestimmten Zeitpunk genutzt wird, hängt dann von der Position innerhalb einer solchen Sequenz ab, die durch die interne Uhr des Masters repräsentiert wird. Damit können alle Teilnehmer in einem Piconetz zu jedem Zeitpunkt dieselben Kanäle benutzen, wenn ihnen die Identität des Masters und die Differenz ihrer eigenen Uhr sowie der des Masters bekannt ist. Innerhalb eines Slots, also solange ein bestimmter Kanal benutzt wird, wird in einem Piconetz genau ein Paket übertragen. Jedes Paket besteht aus einem Access-Code (72 Bit), einem Header (54 Bit) und optional aus bis zu 343 Bytes Nutzdaten. Der Access-Code leitet sich ebenfalls aus der Identität des Masters ab und ist damit für jedes Piconetz einzigartig. Der Header enthält unter anderem eine Medien-Zugriffs-Adresse mit einer Länge von 3 Bit, mit der jeder der acht Teilnehmer angesprochen werden kann. Die Kollisionsvermeidung innerhalb eines Piconetzes wird durch einen zentralen Poll-Mechanismus erreicht, den der Master gewährleistet. Dabei ist jeder Slave berechtigt in dem Slot Daten zu senden, nachdem ein Paket vom Master empfangen wurde. Es werden zwei verschiedene Arten von Verbindungen unterschieden: synchrone leitungsvermittelte (SCO - Synchronous Conection-Oriented) und asynchrone paketvermittelte (ACL – Asynchronous Connectionless Link).

Bei einer SCO-Verbindung wiederholt sich der Poll-Mechanismus in festen Intervallen. Das bedeutet, dass der Master in regelmäßigen Abständen seine Daten zum Slave sendet und dieser wiederum den nächsten Slot nutzt, um Daten zurückzusenden. Dadurch entsteht eine Verbindung zwischen Master und Slave, die eine feste und symmetrische Bandbreite (64 kbit/s) besitzt. Typischerweise wird SCO für die Übertragung von Sprache eingesetzt, wobei keine erneute Übertragung von fehlerhaften Paketen stattfindet sondern die Codierung (CVSD Modulation) so gewählt wird, dass Bit-Fehler sich als Hintergrundrauschen bemerkbar machen. Einhergehend mit einer Verringerung der Bandbreite kann jedoch eine Fehlerkorrektur genutzt werden.

Für den möglichst verlustfreien Transfer von Daten bei höheren Bandbreiten werden hingegen ACL-Verbindungen eingesetzt. Dabei ist es möglich Pakete zu verwenden, die einen, zwei oder drei aufeinanderfolgende Slots belegen. Damit sind sowohl symmetrische als auch asymmetrische Bandbreiten möglich. Wenn ein Pakete mehr als einen Slot verwendet, wird der Kanal während dessen Übertragung nicht gewechselt. Der nächste freie Kanal ergibt sich dann wieder aus der Identität und der Uhr des Masters. Auch bei dieser Art der Verbindung ist es möglich, eine Fehlerkorrektur zu Lasten der Bandbreite zu nutzen. Darüber

hinaus werden fehlerhafte Pakete erneut übertragen. Dies geschieht, indem im Header der Antwort eine fehlerhafte Übertragung signalisiert wird. Für die Übertragung ohne Fehlerkorrektur ergibt sich eine maximale Bandbreite von 172,8 kbit/s im symmetrischen Fall (Pakete belegen nur einen Slot) und 721 kbit/s bzw. 57,6 kbit/s bei asymmetrischen Verbindungen (Pakete einer Richtung belegen fünf Slots).

Um eine Verbindung zwischen zwei Bluetooth Geräten herzustellen, müssen also Informationen über deren Identitäten und interne Uhren ausgetauscht werden. Um dabei nicht von einem vorher festgelegten Kanal abhängig zu sein, der eventuell viele Störsignale trägt, wird auch hier eine Variante des Frequenzwechsels eingesetzt. Jedes Gerät, das nicht mit einem Piconetz verbunden ist, schaltet in einen Standby-Modus. Dabei benutzt es eine Untermenge von 32 aus den 79 verfügbaren Kanälen (bzw. 16 aus 23). Dann wird einer dieser Kanäle für 18 Slots auf eingehende Nachrichten untersucht. Wurde keine an dieses Gerät gerichtete Nachricht empfangen, so wird nach 2048 Slots ein anderer Kanal aus dieser Untermenge gewählt. Bei dieser Auswahl (wie auch bei der des ersten Kanals) wird wieder ein Pseudo-Zufallsverfahren eingesetzt, das von der Identität des Gerätes abhängt. Der momentan gewählte Kanal wird dann also – wie schon weiter oben beschrieben – von der Identität und der internen Uhr eines Gerätes bestimmt. Soll nun eine Verbindung zu einem Gerät mit bekannter Identität aufgebaut werden, so kann dessen Sequenz der 32 (16) Kanäle sowie dessen Zugriffscode abgeleitet werden. Da jedoch die interne Uhr nicht bekannt ist, wird der Zugriffscode in schneller Folge auf mehreren Kanälen dieser Sequenz übertragen. Empfängt das Gerät seinen Zugriffscode, so antwortet es mit einer kurzen Bestätigung. Danach werden ihm die Identität und die interne Uhr derjenigen Einheit übermittelt, die den Verbindungsaufbau initiiert hat. Letztere wird daraufhin zum Master des neuen Piconetzes. Ist die Identität eines Gerätes, welches sich im Standby befindet, nicht bekannt, so kann statt eines Zugriffscodes ein Abfragecode übermittelt werden. Wenn ein Gerät einen solchen empfängt, kann es diesen mit seiner Identität und seiner internen Uhr beantworten. Daraufhin ist es möglich eine Verbindung mit diesem Gerät herzustellen, wie es bereits beschrieben wurde, jedoch mit dem Unterschied, dass nun die Position innerhalb der Sequenz der 32 (16) Kanäle genauer ermittelt werden kann, was einen schnelleren Verbindungsaufbau zur Folge hat.

Zum Abschluss dieses Kapitel soll noch kurz beschrieben werden, wie eine Kommunikation mit mehr als den bis zu acht Teilnehmern eines Piconetzes realisierbar ist. So ist es möglich, dass ein Gerät sich für eine gewisse Zeit in einem Piconetz abmeldet und an einem anderen teilnimmt. Dabei kann es sogar seine Rolle wechseln: während es in einem Netz als Slave fungiert, kann es in einem anderen die Rolle des Masters übernehmen. Es ist jedoch nicht denkbar, dass ein Gerät in mehr als einem Piconetz gleichzeitig als Master auftritt. In diesem Fall währen beide Netze über dessen Identität und interne Uhr definiert, sodass sie nicht unterscheidbar währen. Ein solcher Verbund von Piconetzen, in denen einzelne Geräte an mehreren Netzen teilnehmen, wird als Scatternetz bezeichnet. Da sich die einzelnen Piconetze durch das Wechseln der Frequenzen kaum überlagern, ist die Bandbreite des gesamten Scatternetzes höher als die eines einzelnen Verbundes von bis zu acht Geräten.

Dieser Abschnitt soll nur als kurze Einführung in die Funktionsweise von Bluetooth dienen. Eine genauere Beschreibung dieses Standards ist auf der Seite der Bluetooth SIG ([BTSIG]) zu finden. Zusammenfassend kann gesagt werden, dass Wlan und Bluetooth zwar beide das ISM Band nutzen, sich jedoch in folgenden Punkten unterscheiden:

- Während des Betriebs benutzt Wlan einen festen Frequenzbereich von 22 MHz Breite, während Bluetooth das ISM Band gleichmäßig nutzt.
- Die Teilnehmerzahl ist in einem Wlan Netz im Wesentlichen nur durch die verfügbare Bandbreite beschränkt, währen sie bei Bluetooth (abgesehen von Scatternetzen) maximal acht betragen kann.
- Wlan unterstützt deutlich höhere Bandbreiten als Bluetooth.
- Die Möglichkeiten ein Netz für eine gewisse Zeit zu verlassen, um beispielsweise Energie zu sparen, sind bei Bluetooth „tiefer“ verankert als bei Wlan

3 Theoretischer Hintergrund

3.1 Abstraktion von paketorientierten Netzwerkadaptern

In diesem Kapitel wird untersucht, wie sich die Energieaufnahme einer Netzwerkschnittstelle mithilfe eines Modells abbilden lässt. Ein Modell ist deshalb nötig, da Hardware dieser Art normalerweise nicht mit einem Energiezähler ausgestattet ist. Ein sinnvoll gewähltes Modell weist darüber hinaus bereits automatisch auf signifikante Größen hin, welche für den energetischen Vergleich von Netzwerkschnittstellen relevant sind.

Bei der Untersuchung von deterministischer Hardware – wie sie i. d. R. bei Netzwerktechniken genutzt wird – ist zu erwarten, dass bei mehrmaliger Ausführung gleicher Vorgänge unter gleichen Voraussetzungen auch gleiche Ergebnisse hinsichtlich der aufgenommenen Energie beobachtet werden. Man könnte für jede dieser Voraussetzungen – also Konfigurationen – die Energieaufnahme messen. Mit dieser Datenbasis sollte es dann möglich sein, die Energieaufnahme der Hardware anhand der aktuellen Konfiguration zu bestimmen. Möchte man eine besonders genaue Datenbasis haben, so muss für jede erdenkliche Konfiguration ein Wert erhoben werden. Im engsten Sinne würde dies bedeuten, dass eine Konfiguration genau einen Hardwarezustand inklusive aller Register/ Speicherzellen/ Signale repräsentiert. Dies setzt wiederum voraus, dass die einzelnen Konfigurationen jeweils bekannt sind oder gemessen werden können. Darüber hinaus müssen auch alle möglichen Konfigurationsübergänge betrachtet werden, da bspw. beim Schalten eines Transistors Energie aufgenommen wird. Im Allgemeinen ist es aber nicht möglich, jeden dieser kleinschrittigen Übergänge zu erfassen. Außerdem ist zu erwarten, dass eine Auswertung der so erhobenen Daten selbst einen nicht zu vernachlässigenden Bedarf an Energie hat und somit für eine Echtzeitanalyse mit dem Ziel Energie einzusparen contraproduktiv sein dürfte. Betrachtet man die Funktionen eines Netzwerkadapters auf semantischer Ebene, so lässt sich feststellen, dass deren Menge begrenzt und überschaubar ist. Seine Funktionen beschränken sich im Wesentlichen auf: Herstellen, Halten und Trennen einer Netzwerkverbindung bzw. die Übermittlung von Paketen. Es gibt also offensichtlich Gruppen bzw. Ketten von Konfigurationsübergängen, die sich wiederholen. Insofern reicht es aus, eine solche Gruppe mit der aufgenommenen Energie zu korrelieren. Ein Beispiel hierfür ist der Versand eines Pakets, welcher eine Kette von Vorgängen auf Registerebene beinhaltet. Wird ein gleichartiges Paket ein weiteres Mal übertragen, so wird die dabei beobachtbare Kette bis auf wenige Unterschiede (z.B. bei der Berechnung einer Sequenznummer) gleich sein. Im Folgenden sollen nun die einzelnen Gruppen, wie sie bei Bluetooth bzw. Wlan zu erwarten sind, genauer beschrieben werden. Zunächst soll jedoch der Begriff „Energielevel“ (EL) eingeführt werden. Der Begriff wird in dieser Arbeit immer dann gebraucht, wenn keine Datenübertragung über die Netzwerkschnittstelle stattfindet. Das impliziert sowohl den Zustand, in dem nicht an einem Netzwerk partizipiert wird, als auch den Zustand, in dem der Adapter zwar mit einem Netzwerk verbunden ist, jedoch keine Daten (der Vermittlungsschicht) übertragen werden. Auf einem solchen Energielevel kann auch – wie oben beschrieben – von einer homogenen Kette von Zustandsübergängen ausgegangen werden. Das

ermöglicht die Bestimmung eines Mittelwerts für die Energieaufnahme auf dem jeweiligen Level. Erwähnt aber hier nicht weiter vertieft seien überdies Energiesparzustände der Netzwerkadapter, die als eigenständige Energielevels aufgefasst werden können. Die Vorhersagbarkeit der Energie auf einem solchen Level sollte so lange gewährleistet sein, bis die Kette durch ein neues Ereignis unterbrochen wird. Folgende Ereignisse sind hier zu erwarten: Senden oder Empfangen eines Paketes, Anpassung der Sendeleistung, Übergang in einen Energiesparmodus bzw. Änderung der Konnektivität.
An dieser Stelle sollen nun die verschiedenen Energielevels weiter beschrieben werden, wobei sich die Indizes auf den jeweiligen Zustand beziehen:

EL_d : Energielevel bei getrennter Netzwerkverbindung (disconnected)
EL_c : Energielevel bei bestehender Netzwerkverbindung (connected)
EL_s : Energielevel in einem Energiesparmodus (sleep)

Bei beiden untersuchten Funktechniken finden bei dem EL_c Paketübermittlungen statt, die nicht zuvor durch die Vermittlungsschicht angefordert wurden sondern Bestandteile der jeweiligen Protokolle sind. Wie bereits erwähnt wird Wlan in dieser Arbeit im Ad-Hoc-Modus betrieben. Das bedeutet, dass der Netzwerkadapter in regelmäßigen Abständen Beacons versendet. Auch bei Bluetooth finden kontinuierlich Übertragungen von Paketen durch den zentralen Pull-Mechanismus statt, wie er in Kapitel 2.2 beschrieben wurde. Beide Vorgänge haben zwar einen zyklischen Charakter, werden jedoch auch von dem Paketaufkommen im Netzwerk beeinflusst. Für den Versand von Beacons bedeutet dies, dass weniger Beacons pro Zeiteinheit versandt werden könnten, wenn das Medium von anderen Netwerkteilnehmern ausgelastet wird. Bei Bluetooth im Slave Modus kann der umgekehrte Fall auftreten: wenn andere Teilnehmer das Piconetz auslasten, können einem inaktiven Slave weniger Slots zugeteilt werden, sodass dieser auch weniger Poll-Anfragen bearbeiten muss. Agiert die betrachtete Bluetoothschnittstelle im Master-Modus, so verläuft der Poll-Mechanismus nur solange gleichartig zyklisch, wie es im gesamten Piconetz kein (oder ein gleich bleibendes) Transportaufkommen gibt.

Damit ist die erste sich wiederholende Kette von Konfigurationsübergängen als EL_c identifiziert und bereits etwas über dessen Grenzen ausgesagt, die noch einmal kurz zusammengefasst werden:

- Der Adapter wechselt in ein anderes Energielevel, etwa von EL_c nach EL_d.
- Es findet unvorhersagbarer Netzwerkverkehr statt.

Dabei enthält letzterer Punkt mit dem Begriff der Vorhersagbarkeit ein wesentliches Kriterium für die Grenzen der Ketten im Allgemeinen, bedarf aber noch einer genaueren Erläuterung. Betrachten wir einen hypothetischen Netzwerkadapter, der sich in EL_c befindet. Er sei so konfiguriert, dass er nach x Sekunden ohne Aktivität im Netzwerk automatisch in einen Energiesparmodus EL_s wechselt und diesen nach y Sekunden wieder verlässt. So kann der Zyklus $EL_c \rightarrow EL_s \rightarrow EL_c \rightarrow EL_s ...$ wiederum in einem eigenen Energielevel gemittelt werden und solange als gültig angenommen werden, bis die

Verbindung zum Netzwerk getrennt wird oder Pakete ausgetauscht werden. Allerdings leidet die Genauigkeit der Vorhersage bei diesem Vorgehen, wenn der Adapter bspw. alle x-1 Sekunden an einem Transfer von Daten beteiligt ist und somit niemals nach EL_s wechselt. Es mag sich in diesem Fall also anbieten zwischen EL_c und EL_s zu unterscheiden, womit eine wichtige Anforderung an die Anwendbarkeit eines Modells identifiziert ist, welches in Echtzeit die Energieaufnahme einer Netzwerkschnittstelle abschätzen soll: die verwendeten Eingabedaten müssen messbar sein. In dem gerade erläuterten Beispiel bedeutet dies, dass das momentane Energielevel also entweder durch die Hardware oder deren Treiber in Erfahrung gebracht werden kann oder sich durch den Zeitpunkt des letzten relevanten Transfers abschätzen lässt. Bevor nun der Vorgang der Datenübertragung im Detail betrachtet wird, soll noch kurz auf EL_d eingegangen werden. Bei EL_d besteht keine Netzwerkverbindung. Demnach ist zu erwarten, dass sich die Energieaufnahme mit hoher Zuverlässigkeit linear zu der Zeit verhalten wird. Natürlich ist nicht anzunehmen, dass sich ein Netzwerkadapter nur auf einem einzigen Energielevel befinden kann, wenn er nicht an einem Netzwerk teilnimmt. Möglicherweise gilt es auch hier eine Unterscheidung zwischen verschiedenen Energiesparmodi zu machen, so wie sich der Adapter auch in einem Zwischenzustand zwischen EL_d und EL_c befinden kann. Solche Unterscheidungen können etwa gemacht werden, wenn (1) ein Bluetooth Gerät auf Inquiry und Page Anfragen wartet oder es (2) diese ignoriert. Als weiteres Beispiel mag eine Schnittstelle dienen, die zwar potentiell den Netzwerkverkehr anderer Teilnehmer empfängt und verarbeitet jedoch selbst keine Daten versendet, wie es bei Wlan im Monitor-Modus der Fall ist. Diese Art der feineren Aufspaltung des EL_d sollte jedoch im Allgemeinen gut möglich sein, da die unterschiedlichen Betriebsmodi oft explizit durch den Benutzer festgelegt werden und somit erkennbar bzw. messbar sind.

Im Folgenden soll nun die andere Grenze der Gültigkeit bisher erörterter Energielevels betrachtet werden. Für diese Levels war angenommen, dass für sie legitimierbar eine gemittelte Energieaufnahme der Netzwerkschnistelle angenommen werden kann, da sie sich durch wiederholende Ketten von Konfigurationsübergängen auszeichnen. Diese Vorstellung ist eng mit der Vorhersagbarkeit der Abläufe innerhalb der Hardware verknüpft. Die Vorhersagbarkeit ist meistens nicht mehr gewährleistet, wenn ein Paket von einem anderen Netzteilnehmer empfangen und verarbeitet wird, was natürlich in gleicher Weise für den Versand von Paketen gilt. Zwar sind einige solcher Pakete auch mit hoher Wahrscheinlichkeit zu erwarten, etwa innerhalb eines größeren Dateitransfers, eines kontinuierlichen Streamings oder ähnlichem. Dafür ist jedoch eine Analyse der höheren Protokollschichten nötig, die aufgrund der Vielzahl von Protokollen und deren Konventionen nur für Sonderfälle anzustreben ist. Darüber hinaus gibt es dennoch Paketübermittlungen, die im Allgemeinen nicht zuvor absehbar sind z. B. wenn ein neuer Teilnehmer am Netzwerk partizipiert und alle anderen darüber informiert bzw. nach angebotenen Diensten abfragt. Aus den genanten Gründen scheint es daher nicht angebracht zu sein, eine Vorhersagbarkeit der Abläufe innerhalb eines Netzwerkadapters über die Verarbeitung und den Transfer eines einzelnen Paketes hinaus anzunehmen.

Wenden wir uns nun dem Senden eines einzelnen Pakets zu. Der Adapter befinde sich zunächst in einem sendebereiten Modus, etwa EL_c. Dann lassen sich folgende Vorgänge identifizieren, die für den Transfer eines Pakets notwendig sind:

Vorverarbeitung
- Einbettung der Daten in Protokoll der Sicherungsschicht
- Berechnung einer Prüfsumme
- Vorbereiten von Fragmentierung bzw. Aggregation
- …

Der Zugriff auf das Medium muss koordiniert werden
- Bei Bluetooth: Nutzung des nächsten reservierten Slots oder Multislots
- Bei Wlan: CSMA/CA sowie RTS/CTS oder CTS-to-self oder PCF Fenster

Transfer der Daten
- Eventuell werden diese noch durch einen Verschlüsselungsalgorithmus gesichert

Sicherung des fehlerfreien Empfangs
- Bei Bluetooth: Explizite Anfrage für erneute Übertragung
- Bei Wlan: Erneute Übertragung falls Empfangsbestätigung ausbleibt

Das Senden eines Pakets lässt sich also schon grob in verschiedene Ketten von Konfigurationsübergängen unterteilen. Dabei zeichnen sich einige von ihnen im Gegensatz zu den im Kontext der Energielevel betrachteten Ketten dadurch aus, dass sie deutlich unregelmäßiger sind. Diese Aussage soll anhand der grade aufgezählten Phasen näher erläutert werden. Zunächst einmal sei der Fokus auf den eigentlichen Transfer der Daten gerichtet. Dieser findet statt, sobald das Medium reserviert ist und verläuft im Wesentlichen sehr homogen: die Eingabedaten werden innerhalb des Netzwerkadapters entsprechend des Übertragungsstandards moduliert bzw. kodiert und auf das Medium gebracht. Betrachtete man hierbei sehr feingranular die Konfigurationen und Konfigurationsübergänge der Hardware, so ließe sich wohl der gleiche Ablauf feststellen, wenn zweimal ein bestimmter Zahlenwert kodiert wird. Für einen anderen Wert würden sich die Vorgänge aber wohl (geringfügig) unterscheiden. Da diese Kodierungsvorgänge letztlich von den Eingabedaten bestimmt werden, ist es prinzipiell möglich, diese Konfigurationsketten voneinander zu unterscheiden ohne eine vollständige Simulation der Hardware zu verwenden. Somit ist die Messbarkeit der Eingangsgrößen für das Modell gegeben, um dem Kodieren einer bestimmten Datenmenge eine zuvor gemessene Energieaufnahme zuzuordnen. Allerdings ist eine Analyse bspw. auf Byte-Basis potentiell sehr rechen- und energieintensiv. An dieser Stelle ist jedoch eine Vereinfachung des Modells unter der Annahme möglich, dass die Kodierung zweier verschiedener Zahlenwerte eine vergleichbare Menge an Energie benötigt. Diese Annahme sollte für die meisten Schaltkreise, die in Netzwerkschnittstellen Verwendung finden, zutreffen, sodass sich diese Phase des Sendens von Daten auf folgende Weise darstellen lässt:

Der Transfer von Daten impliziert auf der Senderseite eine Reihe von Konfigurationsübergängen, die ein energetisch jeweils vergleichbares Verhalten des Netzwerkadapters mit sich bringen. Somit ist zu erwarten, dass bei diesem Vorgang ein näherungsweise linearer Verlauf der Energieaufnahme über die Zeit zu beobachten ist.

Dies kann auch die Verschlüsselung der Daten beinhalten, wenn sie verwendet wird und verschiedene Zahlenwerte dabei mit einer ähnlichen elektrischen Leistung kodiert werden. Um der gesamten Transferphase eines Pakets die benötigte Energie zuzuordnen, muss neben einem Linearitätsfaktor die zeitliche Ausdehnung des Vorgangs bekannt sein. Diese wird direkt durch die Menge der Daten, die dabei übertragen wird, sowie dem Durchsatz an Daten pro Zeitintervall bestimmt. Somit ist es möglich, dem Transfer eines Pakets in Abhängigkeit von dessen Größe die benötigte Energie zuzuordnen. Dabei gilt es jedoch noch einige Randbedingungen und Vorraussetzungen zu beachten. Bereits angesprochen war der Durchsatz, der neben der Größe des Pakets die Dauer des Transfers bestimmt. Dieser kann unter Umständen für jedes übertragene Paket variieren, was hier am Beispiel von Wlan kurz erläutert wird. Nehmen wir an, dass sowohl 802.11b als auch 802.11g Geräte an einem gemeinsamen Netz partizipieren. Kommunizieren nun zwei 802.11g Teilnehmer miteinander, so kann unter Verwendung von OFDM ein höherer Durchsatz erreicht werden, als dies bei einem Transfer möglich ist, der DSSS verwendet, da mindestens Quelle oder Senke dem Standard 802.11b gemäß arbeiten. Neben der unterschiedlichen Zeitspanne, die in diesen beiden Szenarien benötigt wird, um eine gegebene Menge von Daten zu übertragen, kann natürlich auch die Art der Modulation zu unterschiedlichen Linearitätsfaktoren führen, die verwendet werden müssen, um den Energiebedarf abzuschätzen. Darüber hinaus kann die Zeit, in welcher der Netzwerkadapter Daten auf das Übertragungsmedium bringt, bspw. auch davon abhängen, ob eine Kollisionserkennung realisiert ist. Ist dies der Fall, so wird der Transfer möglicherweise abgebrochen, bevor das gesamte Paket gesendet wurde und damit die Zeitspanne dieser Phase verkürzt. Bei vielen Funkübertragungsstandards und insbesondere bei den in dieser Arbeit näher betrachteten, ist jedoch keine Kollisionserkennung vorgesehen, sodass jedes Paket vollständig gesendet wird. Ein weiterer Einfluss auf den Linearitätsfaktor, der den Zusammenhang zwischen aufzuwendender Energie und Paketgröße beschreibt, ist speziell bei drahtlosen Übertragungstechniken in der verwendeten Sendeleistung gegeben. Diese kann in Abhängigkeit der Signalqualität des beobachteten Netzwerkverkehrs angepasst werden und somit für den Versand mehrerer Pakete variieren. Da – wie bereits erwähnt – bei den untersuchten Standards Bluetooth und Wlan kein voller Duplexbetrieb verwirklicht ist, kann jedoch angenommen werden, dass sich die Sendeleistung nicht während des Transfers eines einzelnen Pakets verändert, weil sie auf der Grundlage der Signalqualität empfangener Daten angepasst wird.

Wenden wir uns nun den noch nicht näher betrachteten Vorgängen für das Senden eines Pakets zu und beginnen dabei mit der Reservierung des Übertragungsmediums. Soweit es den Poll-Mechanismus bei Bluetooth und die Auswertung von CTS und PCF Paketen bei Wlan betrifft, wurde bereits dargestellt, dass diese Mechanismen aufgrund der Konventionen der jeweiligen Protokolle auch dann stattfinden, wenn der betrachtete Netzwerkadapter keine anstehenden Sendeaufträge hat. Daher wurden diese Vorgänge weiter oben einem Energielevel, insbesondere EL_c zugeordnet. So bleibt also noch auf den Versand

eines RTS bzw. CTS-to-self und den Empfang eines CTS Pakets in 802.11 Netzen einzugehen. Dabei kann argumentiert werden, dass der Transfer dieser Pakete sich grundsätzlich nicht von dem anderer unterscheidet, wenn die entsprechende Modulation berücksichtigt wird. Allerdings werden eventuell geringfügig andere Konfigurationsübergänge innerhalb der Hardware zu beobachten sein, was die Vorverarbeitung dieser Pakete im Vergleich zu den nachfolgenden betrifft, die Daten aus höheren Schichten des ISO-OSI-Schichtenmodells kapseln. Der Begriff der Vorverarbeitung, wie er in diesem Kapitel gebraucht wird, impliziert keine chronologische Einordnung der ihm zugeordneten Vorgänge in Bezug auf den Versand eines Pakets. Vielmehr ist davon auszugehen, dass sich einige Abläufe, die er umfasst, während des Transfers von Daten ereignen bspw. die Berechnung einer Prüfsumme. Allerdings zeichnen sich diese Vorgänge dadurch aus, dass sie sehr ähnliche Ketten von Konfigurationsübergängen pro Versand eines Pakets mit sich bringen. Somit kann für diese eine konstante Menge an benötigter Energie erwartet werden, die für den Versand eines jeden Paketes unabhängig von dessen Größe benötigt wird.

Abschließend wird nun noch auf den Empfang eines Paketes eingegangen, der sich nach den grade ausgeführten Vorüberlegungen ähnlich begreifen lässt wie der Versand. Daher wird hier nur auf die wesentlichen Unterschiede zwischen diesen beiden Vorgängen hingewiesen. Zunächst einmal wird für den Transfer auf der Empfängerseite keine Sendeleistung benötigt. Dennoch ist auch hier durch Demodulation und Dekodierung ein energetischer Energiebedarf anzunehmen, der sich näherungsweise linear zu der zeitlichen Ausdehnung der Transferphase verhält und damit unter anderem auch durch die Größe des empfangenen Pakets bestimmt wird. Darüber hinaus kann auch ein konstanter Aufwand pro empfangenem Paket erwartet werden, etwa durch die Auswertung der Zieladresse des Pakets oder einer Prüfsumme. Soweit es Wlan betrifft, kann die Bestätigung eines fehlerfrei empfangenen Pakets durch ein ACK Paket wiederum als eigenständiger Sendevorgang begriffen werden.

3.2 Strategien für energieeffiziente Nutzung mehrerer Netze

Nun sollen Mechanismen untersucht werden, die eine energieeffiziente Nutzung von paketorientierten Netzwerkverbindungen unterstützen. Dabei wird der Begriff Energieeffizienz – wie auch durchgängig in dieser Arbeit – als die Minimierung der für den Transfer einer bestimmten Menge von Daten benötigten Energie verstanden.

Bei der Betrachtung des energetischen Verhaltens eines Netzwerkadapters ist zu erwarten, dass dieser eine geringere Energieaufnahme hat, wenn er nicht mit einem Netzwerk verbunden ist, als wenn er an einem solchen teilnimmt und zumindest die anfallenden Übermittlungen anderer Teilnehmer auswerten muss. Ist dies der Fall, so ist es sinnvoll, den Adapter vom Netzwerk zu trennen bzw. gar nicht erst mit diesem zu verbinden, wenn kein Datentransfer auf IP Ebene stattfindet. Eine Verbindung sollte genau dann hergestellt werden, wenn Daten über das Netzwerk übertragen werden müssen. Allerdings lässt sich diese Situation nur an der Quelle der Daten feststellen, die Senke hingegen muss darüber wiederum mittels einer Datenverbindung informiert werden, damit auch

sie an dem Funknetzwerk teilnimmt. Ein häufig verwendeter Mechanismus ist dabei, dass ein Netzwerkteilnehmer sich für einen bestimmten Zeitraum beim Netzwerk abmeldet und für ihn anfallende Daten zwischengespeichert werden. Nach Ablauf dieser Zeit meldet er sich entweder selbst zurück, um eventuell anstehende Übertragungen entgegenzunehmen, oder er wird aufgrund eines vereinbarten Zeitfensters automatisch als aktiv angesehen. Eine andere Vorgehensweise besteht darin, dass ein Netzwerkadapter in einen Energiesparmodus wechselt, in dem es nur noch möglich ist bestimmte Nachrichten zu empfangen. Bei Wlan sind dies etwa Pakete die DSSS moduliert sind und ein festgelegtes Format haben, sodass einige Elemente des Adapters in dieser Zeit abgeschaltet werden können. Beim Empfang einer solchen Nachricht wird der Energiesparmodus dann wieder verlassen, um nachfolgende Pakete auf normale Weise empfangen zu können. Letzteres Verfahren erfordert neben der Implementierung im Kommunikationsprotokoll auch eine direkte Unterstützung durch die verwendete Hardware, während ersteres sich transparent auch auf die Kommunikation der Vermittlungsschicht aufwärts übertragen lässt. In einem IP Netz könnte dies wie folgt ablaufen: ein Teilnehmer C, der sich für eine gewisse Zeit vom Netz trennen will, informiert alle anderen Teilnehmer darüber. Diese speichern von nun an alle Pakete, die an C gerichtet sind, und bestätigen dessen Anfrage. Hat Teilnehmer C alle Bestätigungen erhalten, trennt er sich vom Netz und schaltet seinen Netzwerkadapter ab. Nach einer gewissen Zeit stellt er die Verbindung wieder her. Dabei kann er eventuell auf einige Vorgänge verzichten, die normalerweise bei der Anmeldung anfallen würden z.B. eine IP Adresse über DHCP zu beziehen, solange sein Lease noch nicht abgelaufen ist. Nun informiert er alle anderen Teilnehmer darüber, dass er wieder empfangsbereit ist, woraufhin diese ihm ihre zwischengespeicherten Pakete zustellen. Dieses Verfahren weist offensichtlich einige Schwächen auf. Ist z.B. kein Broadcast im Netz möglich, so muss für jeden Teilnehmer der potentiell mit C in Kontakt treten könnte eine eigene Nachricht versandt werden. Es ist dann sehr unwahrscheinlich, dass ein kurzzeitiges Abschalten des Netzwerksadapters die Energie für den zusätzlichen Netzwerkverkehr zumindest kompensiert. Die Trennung vom Netz muss dabei aus zwei Gründen kurzzeitig sein: zum einen kann nicht angenommen werden, dass die Zwischenspeicher der anderen Netzteilnehmer beliebig groß sind. Zum anderen sollen Verbindungsabbrüche durch Timeouts vermieden werden. Doch selbst wenn ein Broadcast möglich ist, muss jeder Teilnehmer diesen Mechanismus unterstützen und das gesamte Netz wird belastet, insbesondere wenn mehrere Teilnehmer sich kurzzeitig vom Netz trennen wollen. In diesem Fall ist es dann auch nicht mehr trivial, die An- und Abmeldung im Netz so zu koordinieren, dass alle Teilnehmer darüber informiert werden. An dieser Stelle soll auf die Untersuchung in [EECAWLAN] hingewiesen werden. Anders stellt sich die Situation dar, wenn der genannte Teilnehmer C über einen ausgezeichneten Zugriffspunkt auf das restliche Netzwerk zugreift, wie etwa bei Wlan im Infrastruktur-Modus. Dann muss nur dieser Nachrichten für Teilnehmer C zwischenspeichern und auch nur dieser muss über dessen Erreichbarkeit informiert werden.

Unter gewissen Vorraussetzungen kann eine kurzzeitige Trennung der Netzwerkverbindung zu einer Minderung der insgesamt aufgenommenen Energie führen.

Das Einsparungspotential hängt dabei von folgenden Größen ab:

- Der Differenz der Energieaufnahme in verbundenem bzw. nicht verbundenem Zustand des Netzwerkadapters
- Der benötigten Energie und Zeit, um die Ab- bzw. Anmeldung am Netz zu gewährleisten
- Der benötigten Energie und Zeit für die Trennung vom bzw. Verbindung zum Netzwerk
- Der Zeitspanne, für die eine Trennung vom Netzwerk andauert

Der grade beschriebene Mechanismus ist natürlich besonders geeignet für Phasen, in denen kein Transfer von Nutzdaten im Netzwerk stattfindet. Es ist jedoch nicht a priori auszuschließen, dass sich hierdurch auch dann ein Einsparungspotential bietet, wenn dies nicht der Fall ist, also Netzwerkverkehr vorliegt. Dann würde die Anwendung dieses Mechanismus zwar zu einer Verminderung des mittleren Durchsatzes und zu einer erhöhten mittleren Verzögerung für einen gegebenen Netzwerkadapter führen, könnte jedoch bei geeigneten Randgrößen zu einem geringeren Energiebedarf pro übertragener Datenmenge führen.

Ein anderer Mechanismus, der bspw. auch in einigen Netzwerkadaptern oder deren Treibern realisiert ist, besteht in der Aggregation von Paketen. Dabei werden möglichst mehrere Pakete der Vermittlungsschicht gesammelt und dann gemeinsam in einem Paket der Sicherungsschicht übertragen. Normalerweise soll mit einem solchen Vorgehen die benötigte Dauer minimiert werden, die das Übertragungsmedium für den Transfer reserviert werden muss, um somit einen höherer Durchsatz des Netzes zu erreichen. Dies wird je nach Implementierung jedoch durch eine geringe Erhöhung der Verzögerung erkauft, in der Daten aus der Vermittlungsschicht gesammelt werden, bevor sie versendet werden. Von diesem Verfahren ist aber auch ein Effekt hinsichtlich einer energieeffizienten Übertragung von Daten zu erwarten. Wenn die Aggregation, also im speziellen die Zwischenspeicherung von Paketen, einen gewissen Bedarf an Energie nicht überschreitet, so wird durch diesen Mechanismus auch ein Teil der Energie eingespart werden können, der sonst für die Vorbereitung und Übertragung mehrerer Pakete (inklusive bspw. mehrerer Paketköpfe und Präambeln) benötigt würde.

Der Fokus dieser Arbeit richtet sich allerdings auf die Wahl eines geeigneten Übertragungsstandards, abhängig vom momentanen Transportaufkommen. Dabei soll zunächst einmal unterstellt werden, dass diese Wahl jederzeit stattfinden kann, nicht nur beim initialen Verbindungsvorgang. Dies ist insbesondere für IP Netze nicht selbstverständlich, geht es etwa darum, bestehende Verbindungen durch das Umschalten auf ein anderes Netz nicht zu unterbrechen. Wie diese Möglichkeit im Kontext dieser Arbeit realisiert wurde, wird später noch in Kapitel 4.2 erläutert.

Die eingangs beschriebene Methode der kurzzeitigen Trennung vom Netzwerk kann natürlich auch parallel zum Umschalten zwischen Netzwerkverbindungen

genutzt werden. Es lässt sich sogar selbst als eine Art von dynamischer Netzwahl auffassen, wenn man die Trennung vom Netz als einen Übergang in ein Netz mit anderen Anforderungen an die benötigte Energie, jedoch einer maximalen Bandbreite von 0, betrachtet. Stehen mehrere „echte“ Netzwerke mit sich unterscheidenden energetischen Verhalten zur Verfügung, so können nach dieser Abstraktion einige der Randbedingungen des Mechanismus der Trennung vom Netzwerk übernommen werden, wenn es um eine energieeffiziente Umschaltung auf ein anderes Netzwerk geht. Tritt also die Situation auf, dass ein anderes als das momentan genutzte Netzwerk plötzlich energieeffizienter ist (weil es z.B. in Reichweite kommt oder sich das Transportaufkommen ändert), so sind vor einer Umschaltung auf dieses ebenfalls die Kosten in Form von benötigter Energie für diesen Vorgang zu beachten. Die Möglichkeit, dass sich die Energieeffizienz zweier Übertragungsstandards dynamisch gegeneinander ändern kann, soll an dieser Stelle durch ein Beispiel motiviert werden. Es seien zwei Netzwerktechnologien verfügbar, die verschiedene Protokolle der Sicherungsschicht verwenden, sich jedoch sonst (z.B. in ihren Energielevels siehe Kapitel 3.1) nicht wesentlich unterscheiden. Technologie A verwende Pakete mit einem kurzen Paketkopf jedoch einer geringen maximalen Menge an Nutzdaten pro Paket, wohingegen Technologie B einen langen Paketkopf mit einer großen maximalen Menge von Nutzdaten verwendet. Beim Versand von Nutzdaten, die A mit einem einzigen Paket übertragen kann, ist A dabei potentiell vorzuziehen, da das Verhältnis von Nutzdaten zu Protokolldaten hier zu seinen Gunsten ausfällt. Dieses Verhältnis kann jedoch wiederum für die Verwendung von Technologie B sprechen, wenn eine große Menge an Nutzdaten transportiert werden soll, für deren Übertragung A mehr Pakete benötigt als B. Auch wenn dieses Beispiel sehr einfach gehalten ist, weist es dennoch auf gemessene Eigenschaften der in dieser Arbeit untersuchten Hardware und Protokolle hin, wie sie in Kapitel 2 präsentiert werden.

Eine Umschaltung, wie sie grade beschrieben wurde, kann also aufgrund des beobachteten Netzwerkverkehrs stattfinden. Da jedoch zunächst davon ausgegangen werden muss, dass die Umschaltung selbst ein gewisses Maß an Energie benötigt (Herstellen bzw. Trennen der Verbindung zum Netzwerk), sollte sie erst erfolgen, wenn sich die Energieeffizienz mehrerer Netze hinreichend lange zugunsten eines anderen als dem grade genutzten verändert hat. Diese Situation kann sich im schlechtesten Fall jedoch unmittelbar nach dem Umschaltvorgang wieder geändert haben, sodass sich diese Umschaltung im Nachhinein als kontraproduktiv für die Energieeffizienz herausstellt. Wie in Kapitel 6.2 noch verdeutlicht wird, ist die Umschaltung zwischen den beiden hier genutzten Netzwerkschnittstellen mit dem Ziel die Energieressourcen des Endgerätes zu schonen, grundsätzlich nur unter der Annahme von zuvor nicht messbaren Randbedingungen möglich. Um diesem Umstand zu begegnen, wird in dieser Arbeit die Vorhersagbarkeit von Netzwerkübertragungen, wie sie in Kapitel 3.1 eingeführt wurde, am Beispiel des Hypertext Transfer Protokolls untersucht.

4 Implementierung dynamischer Netzumschaltung

In Kapitel 3.2 wurde angenommen, dass es möglich ist, transparent für den Nutzer zwischen zwei Netzwerkadaptern umzuschalten. Darüber hinaus soll diese Umschaltung jeder Zeit erfolgen können, nicht nur wenn bspw. grade kein Datenaustausch mit dem verbundenen Netzwerk stattfindet. Es darf bei diesem Vorgang also nicht zu einer Unterbrechung bestehender Verbindungen kommen. Geschähe dies, so bedeutete es nicht nur einen immensen Verlust an Verlässlichkeit der Kommunikationsverbindung sondern könnte sich auch negativ auf die Energieeffizienz derselben auswirken. Das kann anhand eines unterbrochenen Dateitransfers verdeutlicht werden. Im besten Fall kann dieser an der Position wieder aufgenommen und fortgeführt werden, an dem es zum Abbruch kam. Dabei währe jedoch zunächst eine neue Anforderung der Datei beim Dienstgeber nötig, die unter normalen Umständen eventuell nicht nötig gewesen wäre. Ist es jedoch nicht möglich den Transfer fortzusetzen, so war der bisherige Transport zwecklos, hat aber dennoch die Energieressource des Empfängers (und natürlich auch des Senders) belastet.

Verschärft wird dieser Umstand durch folgende Überlegung, die in dieser Arbeit an anderer Stelle noch einmal aufgegriffen wird. Der Nutzer eines mobilen Gerätes möchte dieses verwenden, um eine bestimmte Aufgabe auszuführen. Dafür benötigt er jedoch zusätzliche Daten, die er über das verbundene Netzwerk anfordert. Ist es nicht möglich mit der Abarbeitung zu beginnen, bevor alle benötigten Daten empfangen wurden, so bedeutet dies, dass auch andere Komponenten des verwendeten Gerätes für die Zeit des Transfers Energie aufnehmen, obwohl sie für diesen nicht benötigt werden (z.B. die Anzeigeeinheit). Bezieht man dieses Szenario nun auf den Verbindungsabbruch ohne Möglichkeit der Fortsetzung wie er oben beschrieben wurde, so wird klar, dass nicht nur für den Transport der Daten unnötig viel Energie aufgenommen wurde sondern auch für andere Systemkomponenten, die in dieser Zeit aktiv waren jedoch nicht genutzt werden konnten.

Um transparent zwischen zwei Netzwerkverbindungen umschalten zu können, muss die Vermittlungsschicht Möglichkeiten anbieten, um dies zu gewährleisten. Dabei ist es von großem Vorteil, wenn das Gerät, welches die Verbindung wechselt, vor, während und nach diesem Vorgang derselben Netzwerkadresse zugeordnet ist. Dies hat nämlich zur Folge, dass die Umschaltung für alle anderen Netzwerkteilnehmer transparent geschieht, und sie den Vorgang nicht direkt unterstützen müssen. Ein solcher Mechanismus kann direkt durch die Infrastruktur realisiert werden, über die das Endgerät die Verbindung zum Netzwerk herstellt. Dabei soll Folgendes erreicht werden: die Pakete der Vermittlungsschicht werden zunächst mithilfe der Sicherungsschicht von Netzwerkschnittelle A übertragen. Sobald die Verbindung einer anderen Schnittstelle B hergestellt wurde, werden diese Pakete durch die von B bereitgestellte Übertragungstechnik transportiert. Daraufhin kann die nun nicht mehr benötigte Verbindung der Schnittstelle A getrennt werden. Das folgende Kapitel widmet sich der Implementierung dieses Mechanismus, wie sie im Rahmen der Arbeit erfolgte.

4.1 Schnittstellenumschaltung mithilfe von Netzwerkbrücken

Bluetooth bietet für die Nutzung eines Transports von Netzwerkpaketen das PAN (Personal Area Networking) Profil an. Dieses wiederum benutzt das BNEP (Bluetooth Network Emulation Protocol), welches eingesetzt wird, um Ethernet Pakete in L2CAP zu kapseln und darüber zu transportieren. Wlan ist schon von seinem Aufbau her, was etwa die Adressierung innerhalb der Sicherungsschicht angeht, sehr nah an Ethernet angelehnt. Somit ist es ohne weiteres möglich, eine Netzwerkbrücke zwischen diesen beiden Übertragungsstandards zu betreiben. Der Linux Kern bietet schon seit Version 2.2 eine direkte Unterstützung dafür an. Dabei werden eine einzelne oder auch mehrere Schnittstellen zu einer logischen Schnittstelle zusammengefasst. Außerdem besteht die Möglichkeit, neue Schnittstellen zu dieser Brücke hinzuzufügen oder vorhandene aus dieser zu entfernen. Nehmen wir nun also folgende Situation an: ein Gerät C sei über Wlan mit einem Zugriffspunkt S verbunden. Dieser Zugriffspunkt agiert dabei als Gateway für den Rest des Netzwerks. Sowohl auf der Seite von C als auch auf der Seite von S sind die Netzwerkschnittstellen einer Netzwerkbrücke zugeordnet, die in der Ausgangssituation nur eben diese Wlan Verbindung beinhaltet. Dieser Netzwerkbrücke ist auf beiden Seiten jeweils eine IP Adresse zugeordnet, mit deren Hilfe Daten der Transportschicht aufwärts zugeordnet werden. Nun möchte C seine Wlan Verbindung beenden und stattdessen Bluetooth einsetzen. Zunächst wird eine Verbindung über Bluetooth hergestellt. Ist das geschehen, wird diese neue Schnittstelle auf beiden Seiten der Brücke zugeordnet. Daraufhin wird Wlan aus der Brücke entfernt und C kann diese Verbindung beenden. Während des gesamten Vorgangs war es nicht nötig, die Adresse der Vermittlungsschicht auf einer der beiden Seiten neu zuzuordnen oder auszutauschen. Darüber hinaus bestand zu jedem Zeitpunkt mindestens eine Verbindung der Sicherungsschicht, sodass keine Daten zwischengespeichert werden mussten.

Allerdings hat dieses kanonische Vorgehen noch einige Mängel, die besonders für den Zeitraum zum tragen kommen, in dem sowohl Bluetooth als auch Wlan Teil der Brücke sind. Normalerweise werden Netzwerkbrücken eingesetzt, um verschiedene Netzsegmente miteinander zu verbinden. Das bedeutet insbesondere, dass Pakete von einem in das andere Segment weitergeleitet werden. Sind nun also beide Übertragungstechnologien aktiv und an der Brücke beteiligt, so entsteht dadurch ein geschlossener Ring, in dem ein einmal auftauchendes Paket potentiell endlos weitergeleitet wird. Somit wird nicht nur das Netzwerk unnötig belastet, sondern durch die Verarbeitung der Pakete ist auch ein erhöhter Energiebedarf anzunehmen. Um das zu vermeiden, sieht der Standard 802.1d den Einsatz des Rapid Spanning Tree Protocol (RSTP) vor. Dieses kann sowohl zur Aufdeckung von Zyklen in der Netztopologie eingesetzt werden, als auch um verschiedenen Pfaden eine Priorität zuzuordnen. Allerdings eignet sich der Einsatz dieses Protokolls nicht unbedingt für das hier vorgestellt Szenario. Zum einen benötigt das Aufspannen des Baumes eine gewisse Zeit, in der bereits einige Pakete zyklisch weitergeleitet werden können. Zudem ist hier auch nicht zu erwarten, dass die Situation, in der beide Netzwerkadapter der Brücke zugeordnet sind, von langer Dauer ist, da es ja Ziel ist, einen der beiden zugunsten des anderen nicht weiter zu nutzen. Zum anderen wird das RSTP normalerweise während der Lebenszeit einer Netzwerkbrücke eingesetzt, um Veränderungen in der Topologie ausfindig zu machen. Der permanente Netzwerkverkehr, der dadurch erzeugt

wird, wirkt sich jedoch wiederum negativ auf die benötigte Energie aus. Um Zyklen zu vermeiden ohne RSTP einzusetzen, können geeignete Weiterleitungsregeln für die Brücke definiert werden. Eine Möglichkeit besteht darin, keine Weiterleitung von Paketen innerhalb dieser Brücke zu erlauben. Dies ist in dem hier verwendeten Beispiel auch nicht zwingend erforderlich, wenn der Zugriffspunkt S den Zugang zum Rest des Netzwerks beispielsweise über eine kabelgebundene Verbindung gewährleistet. Allerdings kann es sein, dass es neben C noch ein weiteres Gerät D gibt, das S als Zugangspunkt zum Netzwerk verwendet. In diesem Fall ist es durchaus sinnvoll, die Brücke direkt zu nutzen, um einen Datenaustausch zwischen C und D zu gewährleisten. Das ist besonders dann nützlich, wenn diese beiden Geräte verschiedene Übertragungstechnologien nutzen, also etwa Bluetooth (C) und Wlan (D). Es bietet sich also einerseits an, Weiterleitungsregeln zu verwenden, die einerseits die Kommunikation verschiedener Geräte untereinander gewährleisten, und zwar unabhängig davon, welche ihrer Netzwerkschnittstellen grade benutzt wird. Andererseits soll die Weiterleitung von Paketen von einer Netzwerkschnittstelle zu einer anderen desselben Geräts verhindert werden.

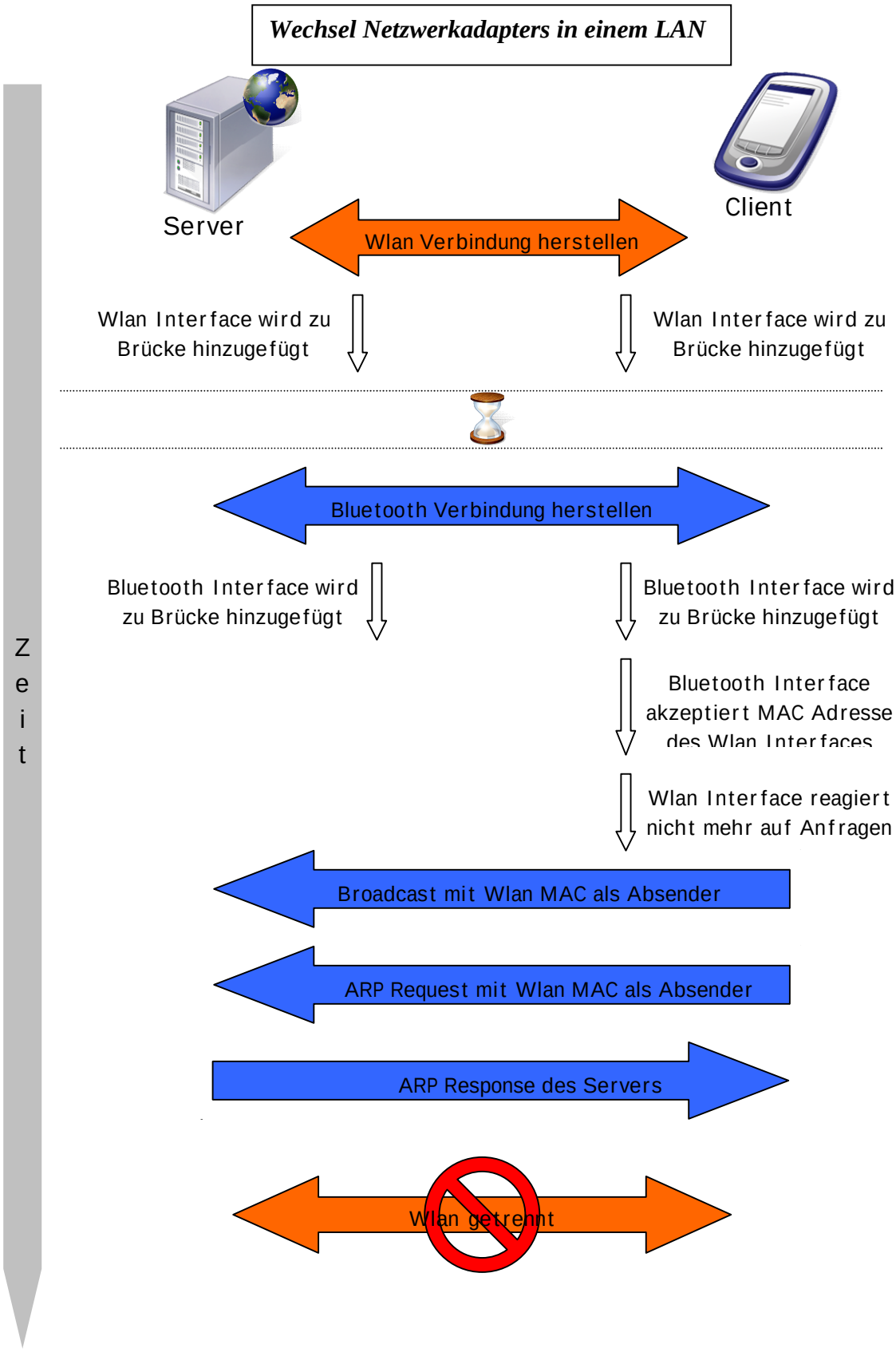
Bevor nun weiter auf diese Regeln eingegangen wird, soll noch ein weiterer Aspekt erwähnt werden, der für den Vorgang der Umschaltung relevant ist. Zu irgendeinem Zeitpunkt muss eine neue Zuordnung der Netzwerkadressen der Sicherungsschicht zu denen der Vermittlungsschicht stattfinden, was in einem Ethernet üblicherweise durch das Address Resulution Protocol (ARP) geschieht. Bezogen auf das am Anfang dieses Kapitels beschriebene Szenario bedeutet dies, dass spätestens nachdem Wlan getrennt wurde, der Eintrag in der ARP Tabelle von C, welcher die Netzwerkadressen von S auflöst, ungültig wird. Natürlich gilt dies spiegelsymmetrisch auch für die Tabelle von S. Die Zuordnung der neuen Sicherungsschichtadresse erfolgt im besten Fall, sobald ein Paket übertragen werden soll und festgestellt wird, dass die Senke nicht mehr unter der bekannten Sicherungsschichtadresse ansprechbar ist. Neben einer deutlichen Verzögerung durch den aussichtslosen Versuch, ein Paket an diese alte Adresse zu übermitteln, kann es jedoch auch zu der Unterbrechung einer Verbindung der höheren Schichten des ISO-OSI-Schichtenmodells kommen, da das Ziel zunächst als nicht erreichbar gilt. Um diesen beiden Umständen vorzubeugen empfiehlt es sich also, das Routing der Pakete explizit anzupassen, sobald die neue Netzwerkschnittstelle der Brücke zugeordnet ist und bevor der zuvor genutzte Kommunikationsweg unterbrochen wird.

Nach diesen Überlegungen soll der Ablauf der Umschaltung von Netzwerkverbindungen mithilfe von Brücken anhand des Diagramms auf Seite 25 detailliert erläutert werden. Die Ausgangssituation ist dabei dieselbe wie in dem bisher verwendeten Beispiel, wobei ein Rechner S den Zugangspunkt für ein Gerät C bildet. Benötigt C einen Zugriff auf das verfügbare Netzwerk, so wird eine der möglichen Übertragungstechniken ausgewählt und über diese eine Verbindung zu S hergestellt. Um später auf eine andere Verbindung wechseln zu können, müssen die entsprechenden Netzwerkschnittstellen auf beiden Seiten einer Brücke zugeordnet werden. Da S neben C eventuell auch anderen Geräten als Zugriffspunkt dient oder die Schnittstelle ohnehin Teil einer Brücke ist, um mehrere Netzwerksegmente miteinander zu verbinden, ist dieser Vorgang hier eventuell nicht mehr nötig. Diese Zuordnung könnte auf beiden Seiten auch aufgeschoben werden, bis C das erste Mal auf eine andere Sicherungsschicht

wechseln möchte. Dann ist jedoch zu beachten, dass sich die Schritte, die für den ersten Wechsel nötig sind, von denen eventuell nachfolgender unterscheiden. Um auf den Einsatz von RSTP in diesem Szenario verzichten zu können (nicht zu müssen), sollte einer möglichen Zyklenbildung soweit wie möglich vorgebeugt werden. Zu diesem Zweck unterbindet C die Weiterleitung von Paketen komplett, da hier angenommen wird, dass C dieser Funktionalität nicht bedarf.

Zu einem bestimmten Zeitpunkt kann C nun die Entscheidung treffen, eine andere Übertragungstechnik zu nutzen. Im Kontext dieser Arbeit tritt dieser Fall ein, wenn sich die Nutzung des Netzwerks durch C derart ändert, dass ein anderer Übertragungsstandard energieeffizienter wird. Zunächst stellt C daher eine neue Verbindung zu S her. Diese wird sowohl von C, als auch von S der jeweiligen Brücke hinzugefügt, falls dies nötig ist. Nun muss die Zuordnung zwischen den Adressen der Sicherungs- und der Vermittlungsschicht für C bei den anderen Teilnehmern im Netz aktualisiert werden, bzw. es muss sichergestellt werden, dass diese gültig bleiben. In letzterem Fall kann C sowohl Pakete akzeptieren, die an die neue wie auch solche, die an die alte Sicherungsschichtadresse gerichtet sind. Dies kann unter Linux beispielsweise mithilfe der arptables realisiert werden und ist im Diagramm auf Seite 25 dargestellt. Eine andere Möglichkeit ist es, dass C für die neue Verbindung dieselbe Sicherungsschichtadresse benutzt wie für die alte. Bei beiden Varianten muss aber dafür gesorgt werden, dass die Brücke von S und andere Switches im Netzwerk von nun an alle Pakete, die an die alte Adresse gerichtet sind, über die neue Verbindung transportieren. Um dies zu erreichen kann C ein Paket im Netzwerk broadcasten, das die alte Adresse als Absender enthält jedoch über die neue Verbindung transportiert wird. Um zu verhindern, dass der Vorgang durch den Versand eines Pakets über die alte Verbindung wieder rückgängig gemacht wird, muss diese zunächst für den Versand von Paketen deaktiviert werden und der Transport von C über die neue Schnittstelle geschehen.

Die andere Möglichkeit, um zu gewährleisten, dass C weiterhin erreichbar ist, besteht darin, dessen Sicherungsschichtadresse bei den anderen Teilnehmern im Netzwerk zu aktualisieren. Das kann folgendermaßen realisiert werden: C sendet (per Broadcast) ein ARP Antwort Paket an alle anderen Teilnehmer im Netz, dass als Absender seine neue Adresse enthält. Beim Empfang dieses Pakets kann jeder Netzteilnehmer das Gerät C mit der neuen Adresse identifizieren und diese für zukünftige Übertragungen nutzen. Allerdings müssen dafür alle Teilnehmer ARP Pakete akzeptieren und auswerten, die sie nicht als Antwort auf ihre eigenen Anfragen erhalten.


Wechsel Netzwerkadapters in einem LAN
Server
Client
Wlan Verbindung herstellen
Wlan Interface wird zu Brücke hinzugefügt
Wlan Interface wird zu Brücke hinzugefügt
Bluetooth Verbindung herstellen
Bluetooth Interface wird zu Brücke hinzugefügt
Bluetooth Interface wird zu Brücke hinzugefügt
Bluetooth Interface akzeptiert MAC Adresse des Wlan Interfaces
Wlan Interface reagiert nicht mehr auf Anfragen
Broadcast mit Wlan MAC als Absender
ARP Request mit Wlan MAC als Absender
ARP Response des Servers
Wlan getrennt
Zeit

4.2 Schnittstellenumschaltung mithilfe von Protokollkapselung

Im Kapitel 4.1 wurde dargelegt, wie sich Vorraussetzungen schaffen lassen, unter denen ein Gerät in einem lokalen Netzwerk von der Nutzung einer Übertragungstechnologie auf eine andere umschalten kann, ohne dass dabei bestehende Verbindungen unterbrochen werden. Um dies zu erreichen wurde besonders von den Routingeigenschaften der Sicherungsschicht gebrauch gemacht. Es ist jedoch wünschenswert, wenn für ein mobiles oder tragbares Gerät auch außerhalb einer daraufhin ausgelegten Infrastruktur die Möglichkeit besteht, zwischen verschiedenen Zugriffsmethoden auf ein Netzwerk wechseln zu können. Es existieren mittlerweile viele Übertragungsstandards, die es einem mobilen Nutzer gestatten auf das Internet zuzugreifen. Daher wird in diesem Kapitel speziell auf IP Verbindungen eingegangen, worauf die Strategien aus Kapitel 4.1 zunächst nicht festgelegt sind. Außerhalb eines für eine bestimmte Gruppe von Nutzern ausgelegten lokalen Netzwerks, findet sich selten eine gleichmäßige Flächenabdeckung aller nutzbaren Netze. Diese Arbeit konzentriert sich jedoch auf Situationen, in denen mehr als ein Netz zur Verfügung steht. Somit ist das Einsparungspotential von Energie durch geeignete Netzwahl dann auch begrenzt. Allerdings gibt es unter diesen Umständen noch einen weiteren Aspekt, der hier bisher noch nicht beschrieben wurde. Ist es möglich, bestehende Netzwerkverbindungen über den Wechsel der Art des Zugriffs auf das Netzwerk hinaus zu erhalten, so kann ein mobiles Gerät einen Datentransfer vor einem Abbruch schützen, indem es auf einen zuverlässigeren Zugang zum Netzwerk wechselt. Als Beispiel sei hier ein PDA genannt, der über einen Wlan-Zugriffspunkt mit dem Internet verbunden ist und eingegangene E-Mail Nachrichten des Benutzers vom Server abruft. Wird die Signalstärke dieser drahtlosen Verbindung so schwach, dass sie abzubrechen droht, könnte eine andere Verbindung z.B. über ein GSM Netz hergestellt und der Transfer über diese fortgesetzt werden. Damit können Wiederholungen von Datenübertragungen aufgrund von Verbindungsabbrüchen vermieden werden.

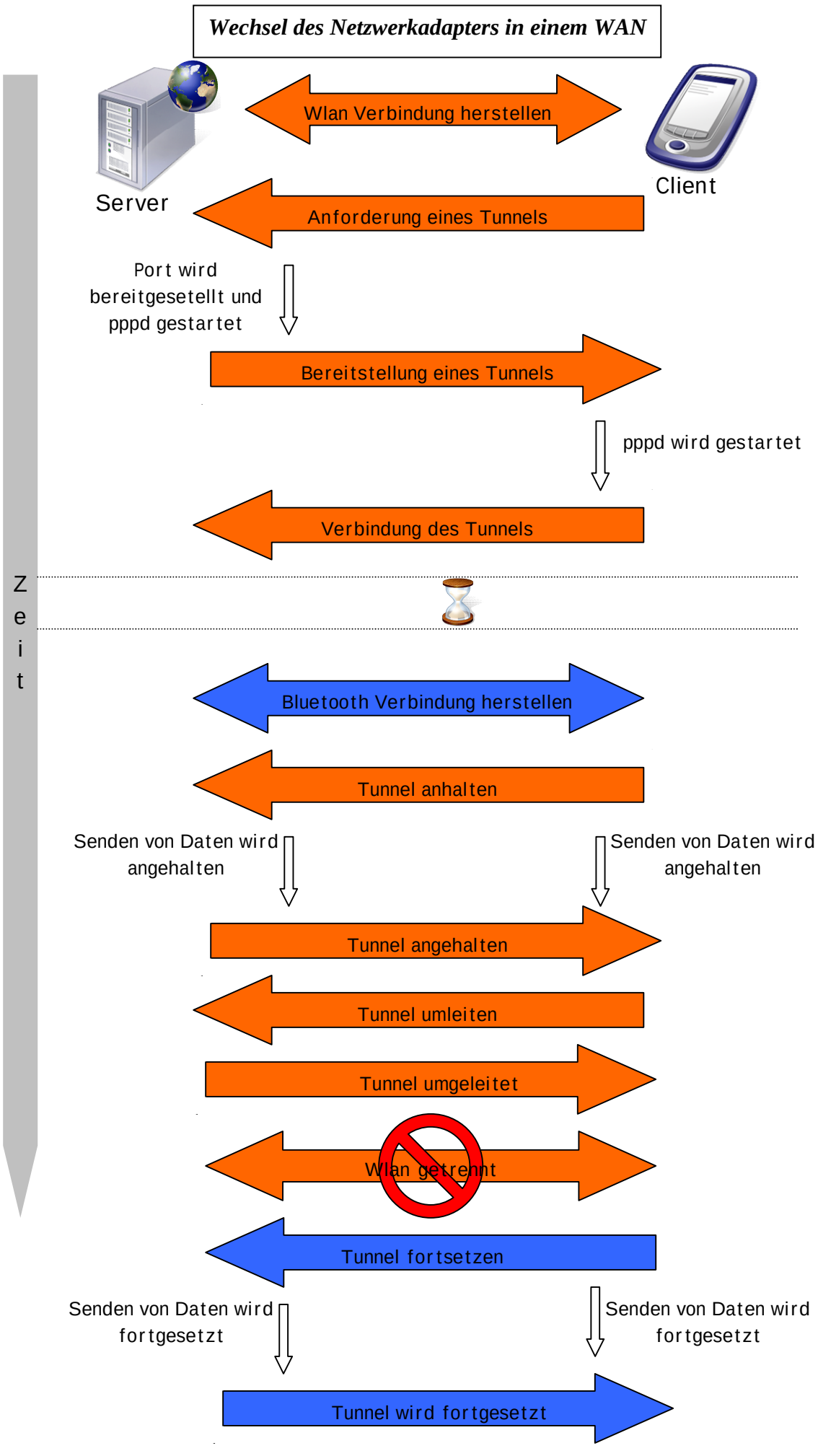
Um IP Verbindungen transparent auf eine andere Schnittstelle umzuleiten ist, ähnlich wie in Kapitel 4.1, die Konsistenz der Zuordnung von IP Adresse und tragbarem / mobilem Gerät notwendig. Allerdings ist das nicht ohne weiteres möglich, wenn über verschiedene Subnetzwerke auf das Internet zugegriffen werden soll. Die IP Adressbereiche, die an verbundene Geräten vergeben werden, können von Netz zu Netz unterschiedlich sein. Darüber hinaus kann auch ein privater Adressbereich verwendet und ein Zugang zum Internet mittels Network Address Translation (NAT) oder IP Masquerading realisiert werden. Für solche Szenarien wurde der IP Mobility Support (IPMS, [RFC3344]) konzipiert. Dabei kommen drei Komponenten zum Einsatz: ein Heim- und ein Fremdagent sowie das mobile Endgerät. Befindet sich das mobile Gerät nicht in seinem Heimnetz, so wird über den Fremdagenten eine Verbindung zum Heimagenten hergestellt. Über diese Verbindung werden Daten vom und zum mobilen Gerät getunnelt, sodass für die Kommunikation des mobilen Geräts über das Internet immer dieselbe IP Adresse aus dem Heimnetz verwendet werden kann. Diese Technik hat zwar den großen Vorteil, dass im Optimalfall keine Voraussetzungen an das mobile Gerät nötig sind (wenn es beispielsweise eindeutig identifiziert werden kann), wurde in dieser Arbeit aber dennoch nicht eingesetzt. Das ist besonders dem Umstand

geschuldet, dass IPMS keine sehr große Verbreitung hat, was konkret bedeutet, dass wenige Netzte einen Fremdagenten anbieten, der genutzt werden kann. Stattdessen wurde hier eine proprietäre Strategie benutzt, um ein ähnliches Ergebnis zu erzielen. Bevor Motivation und Vorteile des verwendeten Ansatzes aufgezeigt werden, soll er zunächst genau beschrieben werden.

Um einem mobilen Gerät C bei einem Wechsel des Zugriffs eine gleichbleibende IP Adresse zuzuordnen, wurde hier – vergleichbar mit IPMS – ein Tunnel zu einem Rechner S verwendet, der über eine stabile Internetverbindung mit fester IP Adresse verfügt. Dieser kann seine eigene Adresse mit einem oder mehreren mobilen Geräten unter der Verwendung von IP Masquerading teilen oder ihnen mittels NAT eigene öffentliche Adressen zuteilen. Da dieser Mechanismus nicht von dem Vorhandensein eines Fremdagenten abhängig sein soll, wird der Tunnel direkt durch C hergestellt. Für den Aufbau und den Transport von Daten durch diesen Tunnel kam dabei das Point-to-Point Protocol (PPP, [RFC1661]) zum Einsatz kommen. Dafür wurde auf Rechner S eine Dienstgeber-Software (in dieser Arbeit als PTOUS bezeichnet) implementiert, die einen offenen Port P bereitstellt. Benötigt das Gerät C die Unterstützung durch den Tunnel, mit dessen Hilfe ein dynamische Netzwahl durchgeführt werden kann, so startet es eine dazu passende Dienstnehmer-Software (PTOUC). Diese Stellt eine Verbindung zu S her und fordert dort den benötigten Tunnel an. Dabei übermittelt G eine eindeutige Identifikation (ID), mit welcher der aufzubauende Tunnel assoziiert wird. In dieser Arbeit wurde die ID dabei zuvor manuell festgelegt. Es ist jedoch auch möglich, diese dynamisch zu wählen oder durch S zuzuteilen. Die Dienstgeberseite (also S) stellt daraufhin einen weiteren offenen Port PX bereit und übermittelt dessen Nummer an C. Dabei wird ein neuer Programmfaden ST von PTOUS erzeugt, der auf eine eingehende Verbindung auf diesem neuen Port wartet. Gleichzeitig wird eine Instanz des pppd gestartet und über eine Pipe mit dem neuen Faden verbunden. Auf der Seite von C wiederholt sich dieser Vorgang auf sehr ähnliche Weise. Sobald C die Nummer des neuen Ports PX von S übermittelt wurde, ist damit automatisch sichergestellt, dass dieser aktiv und für C reserviert ist. Nun startet auch PTOUC einen neuen Programmfaden CT, der ebenfalls eine Instanz des pppd startet, über die er mit einer Pipe verbunden ist. Daraufhin nimmt CT über den auf S für ihn reservierten Port PX Kontakt zu ST auf. Im Folgenden werden über diese Verbindung die Daten zwischen den pppd Instanzen auf S und C transportiert, sodass eine Punkt-zu-Punktverbindung hergestellt wird. Abschließend wird die Routingtabelle von C derart aktualisiert, dass sie neben einem Eintrag für die öffentliche Adresse von S dessen Ende des Tunnels als Standardgateway enthält. Von diesem Zeitpunkt an kann C eine von S bereitgestellt öffentliche IP Adresse nutzen, um mit dem Rest des Netzwerks zu kommunizieren.

Um den Tunnel für eine dynamische Netzwahl nutzbar zu machen, werden von PTOUS und PTOUC Möglichkeiten angeboten, um den Transport von Paketen zwischen den beiden Instanzen von pppd zu steuern. Das Gerät C kann ST über den Port für die Transportsteuerung P veranlassen den Versand von Paketen an CT zu stoppen, mit diesem fortzufahren oder die Pakete zukünftig an eine andere Adresse bzw. einen anderen Port zu senden und eingehende Pakete von dort zu akzeptieren. Dabei wird die ID benutzt, um den Tunnel innerhalb von PTOUS zu identifizieren. Die gleichen Funktionen werden auch von PTOUC zur Verfügung gestellt, sodass es C damit möglich ist, die in Kapitel 3.2 vorgestellten Strategien

zu nutzen. Soll die Netzwerkverbindung kurzzeitig getrennt werden, wird der Transport von Daten zwischen den beiden pppd Instanzen angehalten und zu einem späteren Zeitpunk fortgesetzt. Um den Übertragungsstandart zu wechseln, also etwa von Bluetooth auf Wlan, wird eine neue Verbindung zum Internet hergestellt, die Kommunikation zwischen ST und CT auf diese umgestellt und der zuvor genutzte Internetzugang unterbrochen. Die gerade beschriebenen Abläufe sind auf Seite 29 dargestellt. Zusätzlich wurde in PTOUS und PTOUC die Möglichkeit implementiert, Daten von der jeweiligen pppd Instanz über einen gewissen Zeitraum zu sammeln und erst nach Ablauf dieser Frist, oder sobald eine bestimmte Menge an Daten vorliegen, an die Gegenstelle (CT oder ST) zu übermitteln. Damit ist es möglich, eine Paketaggregation zu nutzen, die für die beiden pppd Instanzen vollkommen transparent abläuft.
Dieser Ansatz bietet gegenüber IPMS einige Vorteile. Wie bereits angesprochen ist kein Fremdagent im Netzwerk nötig, über das ein mobiles Gerät eine Verbindung zum Internet herstellt. Darüber hinaus bietet er eine direkte Unterstützung der in dieser Arbeit verwendeten Strategien für eine energieeffiziente Nutzung verschiedener Übertragungsstandards an. Der Einsatz von PPP birgt dabei noch weitere Vorteile, die weit über die Fähigkeiten hinausgehen. Zunächst einmal ist PPP weit verbreitet und über verschiedene Bibliotheken nutzbar. Damit stehen grundlegende Mechanismen wie etwa Authentifizierung unmittelbar zur Verfügung. Zudem ist es ohne großen Aufwand möglich, die getunnelten Daten zu komprimieren. Wie in [EALDC] gezeigt wurde, kann bei geeigneter Wahl des Kompressionsalgorithmus Energie eingespart werden, die für den Transfer über eine Funkverbindung benötigt wird. IPMS bietet nach [RFC2002] zwar eine Van Jacobsen Kompression der IP Köpfe von getunnelten Paketen an, von der das mobile Gerät jedoch nicht profitieren kann (diese ist nach [RFC3344] auch nicht mehr vorgesehen).
Zusätzlich eröffnet der Einsatz von PPP eine weitere Möglichkeit der energieeffizienten Nutzung von mehreren Netzwerkschnittstellen. Angenommen die Energieaufnahme eines mobilen Gerätes ist im Vergleich zu der seiner Netzwerkschnittstellen sehr hoch. Muss nun beispielsweise ein Dateitransfer abgeschlossen werden, bevor die Arbeit des Geräts auf diesen Daten fortgeführt werden kann, bietet es sich unter Umständen an, mehrere Verbindungen zu nutzen, um den Durchsatz des Transfers zu erhöhen und ihn damit schneller abzuschließen. Dabei lässt sich die Fähigkeit von PPP ausnutzen, die Daten eines Tunnels auf mehrere Verbindungen zu verteilen. Dies ist sogar dynamisch möglich. Es können also zu einem bestehenden Tunnel neue Links hinzugefügt und später auch wieder entfernt werden. PTOUS/C bietet durch eine geeignete Wahl der Identifikation eines mobilen Geräts (die an pppd weitergegeben wird) eine Unterstützung solcher Multilinks an.
Abschließend soll noch kurz auf Sicherheitsaspekte bezüglich des hier vorgestellten Ansatzes eingegangen werden. Eine Authentifizierung für den eigentlichen Tunnel kann – wie bereits erwähnt – durch PPP geleistet werden. Allerdings findet der Transport sämtlicher Daten zwischen Dienstgeber und -nehmer vollkommen ungesichert statt. Dies hat zur Folge, dass bestehende Tunnel über den Steuerungsport von Unbefugten unterbrochen oder sogar übernommen werden können. Daher empfiehlt es sich, die verwendeten Verbindungen durch eine Authentifizierung und Verschlüsselung abzusichern. Da das aber weit über das Thema dieser Arbeit hinausgeht, soll es genügen, beispielhaft auf den Einsatz von IPSec ([RFC4301]) und die energieeffiziente Implementierung verschiedener Public Key Algorithmen in [EIPKA] zu verweisen.


Wechsel des Netzwerkadapters in einem WAN
Server
Client
Wlan Verbindung herstellen
Anforderung eines Tunnels
Port wird bereitgesetellt und pppd gestartet
Bereitstellung eines Tunnels
pppd wird gestartet
Verbindung des Tunnels
Zeit
Bluetooth Verbindung herstellen
Tunnel anhalten
Senden von Daten wird angehalten
Senden von Daten wird angehalten
Tunnel angehalten
Tunnel umleiten
Tunnel umgeleitet
Wlan getrennt
Tunnel fortsetzen
Senden von Daten wird fortgesetzt
Senden von Daten wird fortgesetzt
Tunnel wird fortgesetzt

5 Energiemessungen

5.1 Beschreibung der Hardware und Arbeitsumgebung

In Kapitel 3.1 wurde das dieser Arbeit zugrundeliegende Verständnis eines paketorientierten Netzwerkadapters dargestellt. Dieses unterstellt Annahmen für das Verhalten bezüglich der Energieaufnahme einer solchen Hardware. Um diese zu überprüfen, wurden exemplarisch Netzwerkadapter für die beiden Übertragungsstandards Wlan und Bluetooth untersucht. Für beide Techniken existieren heute sehr viele Lösungen, um sie mit einem Rechner oder einem mobilen Gerät zu verbinden oder in diese zu integrieren. Um die Einflüsse dieser Verbindung auf die Energieaufnahme der Netzwerkadapter möglichst vergleichbar zu halten, wurden Netzwerkadapter gewählt, die über den Universal Serial Bus (USB) mit einem Rechner verbunden werden. Konkret wurden zwei FRITZ!WLAN sowie zwei BlueFRITZ! Adapter für USB der Firma AVM ([AVM]) verwendet. Darüber hinaus standen zwei Testrechner mit Intel Pentium 4 Prozessoren zur Verfügung (Entfernung zueinander etwa 1 Meter), an die jeweils ein Bluetooth und ein Wlan Adapter angeschlossen wurde. Dabei wurden diese an einem der beiden Rechner über ein USB Kabel verbunden. In das Kabel wurde ein elektrischer Widerstand von 50 mΩ eingebracht. Durch eine externe Messvorrichtung konnte der Spannungsabfall an diesem Widerstand mit einer zeitlichen Auflösung von 10 kHz gemessen werden. Über die USB Versorgungsspannung von 5 V wurde somit die Leistung des angeschlossenen Netzwerkadapters in Watt ermittelt. Auf den Testrechnern kam ein Debian 4.0 System mit einem Linux 2.6.21.5 Kernel zum Einsatz.

Sowohl für Wlan als auch für Bluetooth wurde für beide Seiten einer Verbindung jeweils identische Hardware eingesetzt. Das heißt insbesondere, dass Wlan hier im Ad-Hoc Modus verwendet wurde. Die eingesetzten Bluetooth Sticks wurden direkt vom Kernel unterstützt und zeigten sowohl ein stabiles Verhalten als auch die zu erwartenden Übertragungsgeschwindigkeiten. Um eine IP Verbindung zwischen den Testrechnern herzustellen, kam pand aus dem BlueZ Projekt ([BLUEZ]) zum Einsatz. Dieser nutzt das BNEP (Bluetooth Network Emulation Protocol) aus dem PAN Profil von Bluetooth, um ein Netzwerkinterface unter Linux bereitzustellen. Für den Wlan Stick gibt es keine direkte Unterstützung durch den verwendeten Kernel. Der Hersteller bietet jedoch einen eigenen Treiber für Linux an, der aus einer vorkompilierten Bibliothek sowie Quellcode zum Erstellen eines Kernmoduls besteht. Dieser Treiber (Release Candidate 1) wurde zunächst eingesetzt, jedoch zeigte er teilweise fehlerhaftes Verhalten. Insbesondere bei durchgeführten Tests, in denen sehr viele kleine Pakete übertragen werden sollten, kam es reproduzierbar zum völligen Stillstand der Hardware. Das äußerte sich darin, dass weder Daten empfangen noch gesendet werden konnten, bis das Kernmodul neu geladen und die Verbindung erneut hergestellt wurde. Um auszuschließen, dass die eingesetzte Software, welche die Pakete produzierte, zu dieser Situation beitrug, wurden ähnlich Tests beispielsweise mit hping3 wiederholt, jedoch mit dem gleichen Ergebnis. Der Fehler ließ sich im Quellcode des Treibers bis zum Aufruf einer Funktion der binären Bibliothek zurückverfolgen, sodass ein Patchen wenig erfolgversprechend schien. Daher wurden die Treiber für Windows XP mit Hilfe des NDIS wrappers

([NDISW]) für diese Tests wie auch im gesamten Verlauf der Arbeit eingesetzt, welche diese Anomalie nicht aufwiesen.

5.2 Abbildung des energetischen Verhaltens der untersuchten Hardware

Um die aufgenommene Energie der Netzwerkschnittstellen abschätzen zu können, wurde das Energiemodell nach den Vorüberlegungen aus Kapitel 3.1 rechnerisch umgeformt. Die dort identifizierten Energielevels zeichneten sich dadurch aus, dass sie gültig sind, bis sich die Vorgänge innerhalb der Hardware nicht mehr zyklisch wiederholen. Für EL_c trifft dies beispielsweise zu, wenn mit dem Senden oder dem Empfangen eines Paketes begonnen wird. Gültig wird EL_c dann wieder, sobald der entsprechende Vorgang beendet ist. Um also aus diesem Modell die aufgenommene Energie eines Netzwerkadapters abschätzen zu können, muss die zeitliche Ausdehnung der Phasen, in denen dieses Energielevel gilt, erfasst werden und diesen dann eine Energieaufnahme zugeordnet werden. Hinzu käme eine ähnliche Betrachtung für die Zeiträume der Übermittlung von Paketen, die sich wiederum in Phasen unterschiedlicher Energielevels aufteilen lassen, wie etwa Vorverarbeitung, Reservierung des Mediums und dem eigentlichen Transfer. Für diese einzelnen Phasen muss dann jeweils die benötigte Zeit ermittelt werden und ähnlich wie bei EL_c zur Energieabschätzung beigesteuert werden. Dieses Vorgehen wird jedoch folgendermaßen abgeändert: die elektrische Leistung eines Gerätes, die während EL_c beobachtbar ist, wird von den elektrischen Leistungen subtrahiert, die mit den Energielevels während der Übertragungsphasen assoziiert sind. Damit wird hier eine elektrische Grundleistung EB_c eingeführt, die während der gesamten Zeit gültig ist, in welcher der Netzwerkadapter mit dem Netzwerk verbunden ist. Zudem wurde die Darstellung der Phasen von Paketübertragungen vereinfacht dargestellt. Für die Übertragungen eines Pakets wurde ein linearer Zusammenhang zwischen der zeitlichen Ausdehnung der Transferphase und der Größe eines Pakets angenommen. Dies ist nach den Überlegungen aus Kapitel 2.1 durch den Umstand begründet, dass kein Mischbetrieb von Geräten untersucht wurde, die unterschiedlichen Wlan- oder Bluetoothstandards entsprechen. Daher ist insbesondere für Wlan nicht anzunehmen, dass sich die Modulationsfolge verschiedener Pakete unterscheidet. Dieses Konzept wurde dahingehend erweitert, dass jeweils dem Senden oder dem Empfangen eines Paketes eine bestimmte Energieaufnahme des Netwerkadapters in Abhängigkeit von der Größe des Pakets zugeordnet wurde. Dies impliziert die Annahme, dass die anderen Phasen der Übertragung (neben dem Transfer) für verschiedene Pakete nicht nur einen jeweils gleichbleibenden Energielevel aufweisen sondern auch in ihrer zeitlichen Ausdehnung kaum variieren. Somit werden im weiteren Verlauf dieser Arbeit die folgenden Größen verwendet, um die Energieaufnahme der untersuchten Netzwerkadapter darzustellen:

EB_c: elektrische Leistung eines Netzwerkadapters, während dieser mit einem Netzwerk verbunden ist

EB_d: elektrische Leistung eines Netzwerkadapters, während dieser nicht mit einem Netzwerk verbunden ist

$EQ_s(x)$: elektrische Energie, die benötigt wird, um ein Paket der Größe x zu versenden

$EQ_r(x)$: elektrische Energie, die benötigt wird, um ein Paket der Größe x zu empfangen

$EQ_{d \to c}$: elektrische Energie, die benötigt wird, um die Verbindung mit einem Netzwerk herzustellen

$EQ_{c \to d}$: elektrische Energie, die benötigt wird, um die Verbindung mit einem Netzwerk zu trennen

Wenn im Speziellen zwischen Wlan und Bluetooth unterschieden werden soll, ist der Abkürzung ein *W* bzw. *B* vorangestellt (z.B. WEC_c).

5.3 Durchführung der Energiemessungen

Die Messungen der für die in Kapitel 5.2 eingeführten Größen wurden folgendermaßen durchgeführt. Für die Bestimmung von EB_d wurde die elektrische Leistung der Netzwerkadapter einige lang Sekunden gemessen und ein Mittelwert der so erhobenen Daten errechnet. Bei der Bestimmung von EB_c wurde genauso verfahren, nachdem eine Netzwerkverbindung hergestellt wurde, über die jedoch keine Daten der Vermittlungsschicht transportiert wurden. Die Messungen wurden dabei auf dem Rechner durchgeführt, der das mobile Gerät repräsentiert, also bei Bluetooth auf der Seite des Personal Area Network Users (PANU) und nicht der des Network Access Points (NAP). Bei diesen Messungen wurde auch der Transport von Paketen der Vermittlungsschicht und deren Auswirkungen auf die Energieaufnahme des jeweiligen Adapters erfasst. Im Fall von Bluetooth waren das die Pakete des zentralen Poll-Mechanismus, während es bei Wlan die Beacons waren, die durch die Benutzung des Ad-Hoc Modus hervorgerufen wurden. Da diese beiden Vorgänge jedoch zyklischen Charakter haben, wurde es als sinnvoll angesehen, sie in einen gemittelten Wert für EB_c mit einfließen zu lassen.

Für die Ermittlung von $EQ_s(x)$ bzw. $EQ_r(x)$ wurden jeweils mehrere Messungen durchgeführt. Dabei wurden UDP Pakete fester Größe über das Netzwerk transportiert, wobei keine Bestätigung oder erneute Übertragung durch die Transportschicht erfolgte. Während dieser Phase des Sendens / Empfangens wurde die elektrische Leistung des Netzwerkadapters gemessen und gemittelt.

Von diesem Wert wurde zunächst EB_c subtrahiert. Die so entstandene Differenz wurde auf die benötigte Energie pro übertragenem Paket umgerechnet. Dies war realisierbar, da während der Übermittlung der Pakete auch der vom Netzwerk erreichte Durchsatz festgehalten wurde. Somit war es möglich, die durchschnittlich aufgenommene Energie pro Sekunde des Netzwerkadapters auf den Energieaufwand für die Übermittlung eines einzelnen Paketes umzuschlagen. In den folgenden Kapiteln werden die Ergebnisse dieser Messungen präsentiert.

5.4 Messergebnisse Wlan

Im Folgenden werden die Messungen der Energieaufnahme des Wlan Adapters und deren Ergebnisse aufgezeigt und näher erläutert. Diese Ergebnisse werden in Kapitel 6 als Grundlage benutzt, um das Einsparungspotential durch die in dieser Arbeit untersuchten Strategien zur Energieeffizienz abzuschätzen. Bei der Ermittlung der Werte für WEB_c und WEB_d zeigte der Wlan Adapter ein sehr gleichbleibendes Verhalten. Damit ist gemeint, dass die durch die entsprechende Messreihe ermittelten Werte jeweils nur sehr wenig voneinander abweichen. Die einzige Ausnahme bildete hierbei der Versand von Beacons im mit dem Netz verbundenen Zustand des Adapters. Diese brachten einen deutlichen Anstieg der Energieaufnahme mit sich, waren jedoch von sehr geringer Dauer (typischerweise 0,004 Sekunden). Im Durchschnitt ergaben sich für diese beiden Messreihen:

WEB_c : 0,9726 W
WEB_d : 0,4283 W

Weitere durchgeführte Messreihen sollten den Zusammenhang zwischen aufgenommener Energie und dem Senden bzw. Empfangen von Paketen der Vermittlungsschicht in Abhängigkeit von deren Größe ermitteln. Dabei wurden also die Reservierung des Mediums (CTS) und die Bestätigung eines Paketes (ACK) der Sicherungsschicht auf diese Pakete umgelegt. Wie in Kapitel 5.3 beschrieben, wurde parallel der Durchsatz des Mediums gemessen. Dabei ergaben sich Größen von maximal etwa 6 MBit/s. Dies ist ein Wert, der für ein 802.11b Netz zu erwarten ist, bei einem 802.11g Netz aber um den Faktor 2 übertroffen werden sollte. Tatsächlich zeigte sich, dass der verwendete Wlan Adapter einen solchen Wert erreichen kann. Dies gelang jedoch nur, wenn ein Ad-Hoc Netz mit einer Gegenstelle betrieben wurde, die einen anderen Netzwerkadapter verwendet (in diesem Fall ein WG511T von Netgear). Da unterstellt wird, dass die Ergebnisse dieser Arbeit für andere Hardware übertragbar sind, dabei jedoch die hier gemessenen Größen angepasst werden müssen, wurden die Messungen mit den identischen Netzwerkadaptern als Quelle und Senke durchgeführt.

Bei der Ermittlung von $EQ_r(x)$, also dem Empfang von Paketen zeigte sich, dass bei der zur Verfügung stehenden Abtastrate von 10 kHz mit signifikanten Messungenauigkeiten zu rechnen ist. Dies äußerte sich besonders dadurch, dass die Bestätigung für ein empfangenes Paket typischerweise nur durch einen einzigen Ausschlag in den Messdaten erfasst wurde. Abbildung 1 zeigt den Verlauf einer solchen Messreihe über einen Zeitraum von drei Sekunden. Darin ist

deutlich zu erkennen, wie sich die gemessenen Werte über die Zeit als eine Überlagerung von sinusförmigen Kurven entwickelt. Im weiteren Verlauf einer solchen Messreihe wiederholt sich die abgebildete Struktur zyklisch. Es ist also davon auszugehen, dass durch die Messungen jeweils nur ein bestimmter, sich mit der Zeit verschiebender Ausschnitt der Bestätigungspakete erfasst wurde. Diese Bestätigungspakete werden normalerweise mit maximaler Sendeleistung übermittelt. Es währe also möglich, ihren Energiebedarf durch Messungen für das Senden großer Pakete sowie ihrer per Spezifikation definierten zeitlichen Ausdehnung abzuschätzen. Dabei ließe sich jedoch noch keine endgültige Aussage über die nötige Energie machen, welche die Hardware bspw. zur Auswertung empfangener Pakete benötigt, bevor eine Bestätigung versendet wird. Allerdings zeigte sich, dass die Energie für den Empfang eines Pakets im Vergleich zu anderen gemessenen Größen sehr gering war. Daher werden in dieser Arbeit die gemittelten Werte aus den Energiemessungen verwendet.

Bei den Messungen für den Versand von Paketen war zu erwarten, dass sich solche Messfehler weniger bemerkbar machen, da die zeitliche Ausdehnung des Versands eines Pakets mit dessen Größe zunimmt. Allerdings zeigte die Hardware auch bei der Erhebung der Daten für das Senden eine Auffälligkeit in ihrer Leistungsaufnahme. Wie in Abbildung 2 zu erkennen ist, konnten deutliche Stufen in der Energieaufnahme des Adapters gemessen werden. Nach den Vorüberlegungen aus Kapitel 2.1 sind solche insbesondere für Wlan dann zu erwarten, wenn die Sendeleistung zur Übermittlung von Paketen angepasst wird, um Energie einzusparen. Damit währe es möglich gewesen, den Versand von Paketen unter Berücksichtigung dieser Leistung einem Energiebedarf zuzuordnen. Die mithilfe des NDIS Wrappers verwendeten Treiber für Windows XP lieferten jedoch keine Informationen über diese Größe. Daher wurde auf diesen Bezug zur Sendeleistung verzichtet, weil sie für eine in Echtzeit eingesetzte Energieabschätzung eine messbare Größe sein müsste.

In Abbildung 4 ist der gemessene Durchsatz von Paketen in Abhängigkeit von deren Größe dargestellt. Dabei trat bei Paketen der Vermittlungsschicht, die eine Größe von 886 Bytes überschritten, eine Fragmentierung innerhalb der Sicherungsschicht auf. In der Abbildung sind auch die linearen Trends sowie deren Bestimmungskoeffizienten für fragmentierte bzw. unfragmentierte Pakete angegeben. Die obere Grenze der untersuchten Paketgrößen wurde entsprechend der Maximum Transmission Unit (MTU) des unter Linux bereitgestellten Netzwerkinterfaces gewählt. Abbildung 3 zeigt Ergebnisse der Energiemessungen für den Transfer von Paketen, nachdem sie jeweils auf ein einzelnes Paket umgerechnet wurden. Auch diese Abbildung enthält Trendlinien, welche $WEQ_s(x)$ und $WEQ_r(x)$ darstellen:

$$WEQ_s(x) := 0{,}2309 \cdot x + 216{,}01$$
$$WEQ_r(x) := 0{,}0565 \cdot x + 3{,}392$$

Hier wurde für $WEQ_r(x)$ ein linearer Trend über alle Messpunkte angesetzt, da diese Größe neben dem Versand von Bestätigungen auch die Verarbeitung empfangener Daten berücksichtigt. Beim Empfang von fragmentierten Paketen könnte alternativ dazu auch ein zweiter Trend verwendet werden, wie es bei der Darstellung des Durchsatzes geschehen ist. Allerdings zeigten wiederholte

Messungen sowie auch der Messpunkt nahe 1500 Bytes in dieser Abbildung, dass nicht zwangsläufig von einem erhöhten Aufwand durch Defragmentierung ausgegangen werden kann (eine erhöhte Anzahl von Paketbestätigungen wurde in dieser Darstellung jedoch berücksichtigt).

Abschließend soll nun noch kurz auf $WEQ_{d \to c}$ und $WEQ_{c \to d}$ eingegangen werden.

In dem hier verwendeten Szenario, in dem Kanal und Bezeichnung (Cell ID) des Ad-Hoc Netzwerks bekannt sind, wird kein besonderer Anmeldevorgang beim Verbinden mit dem Netzwerk benötigt. Vielmehr kann der Netzwerkadapter mithilfe dieser Parameter fast instantan an diesem Netzwerk teilnehmen oder sich von ihm trennen. Eine Berücksichtigung des Anmeldevorgangs am Netzwerk (bspw. durch den Einsatz von DHCP) folgt allerdings in Kapitel 6.2.

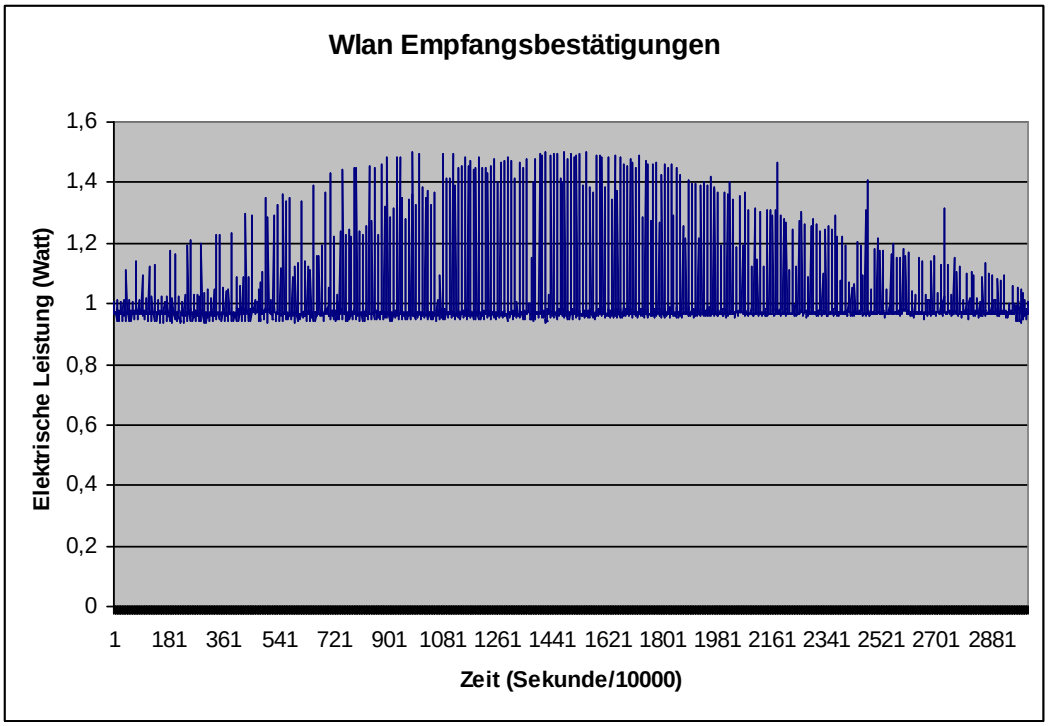


Abbildung 1: Messung von Empfangsbestätigungen Wlan

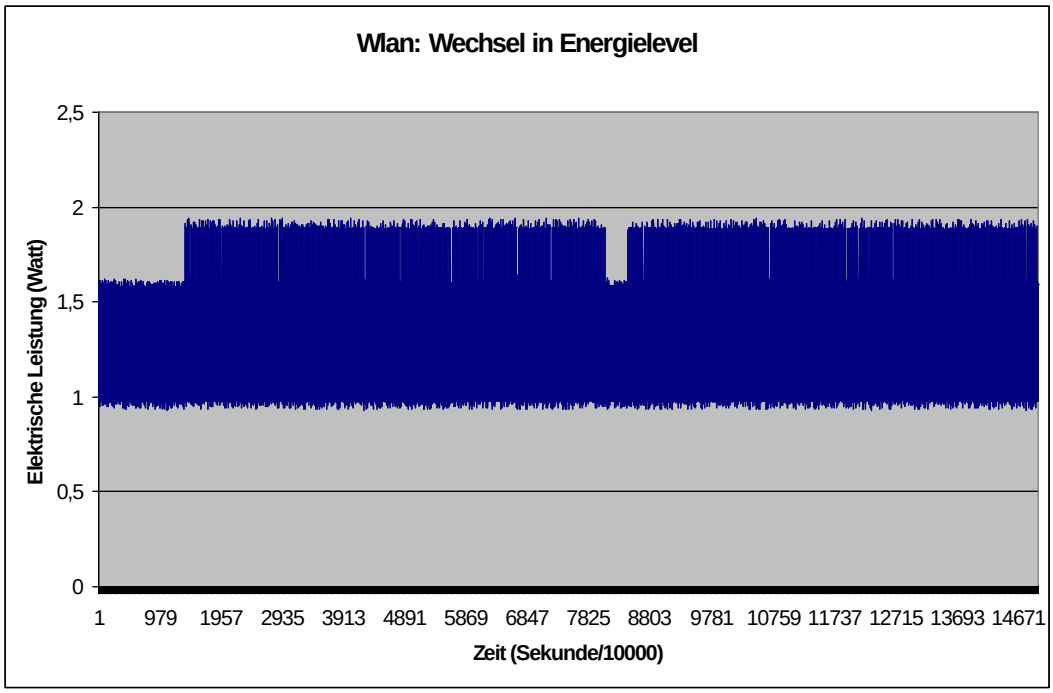


Abbildung 2: Wechsel der Sendeleistung Wlan

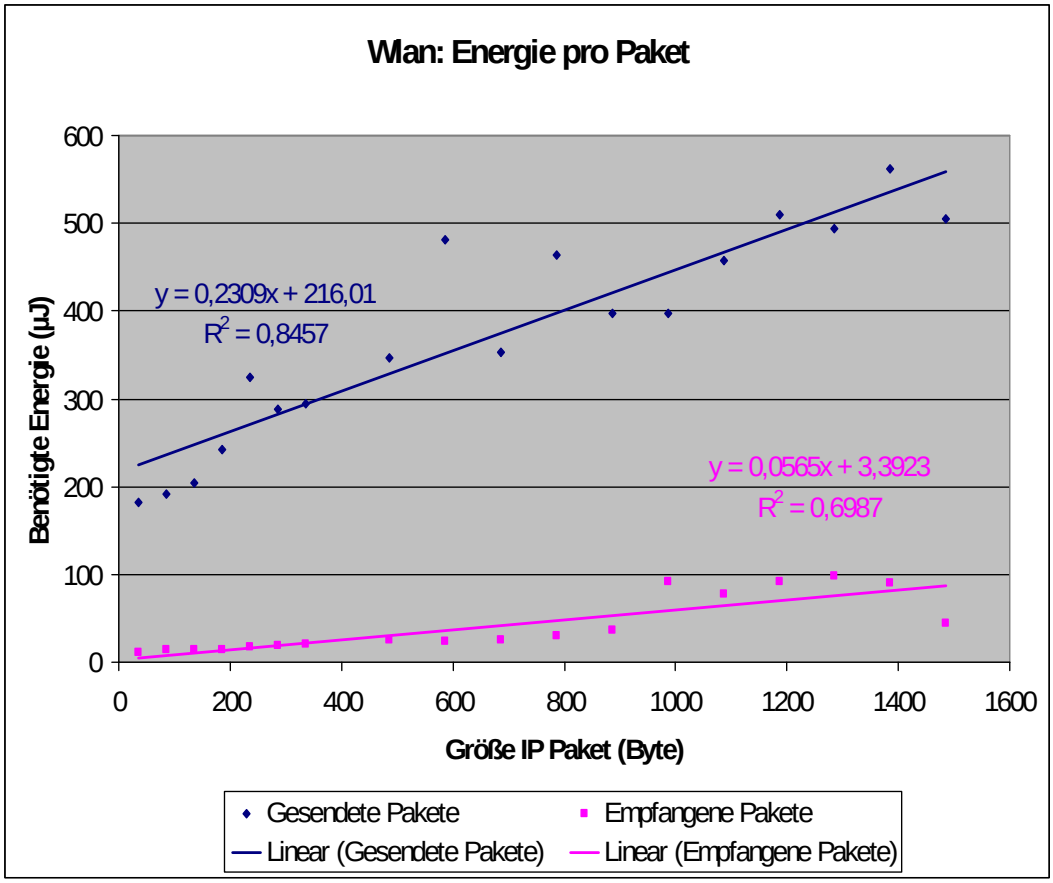


Abbildung 3: Relation zwischen aufgenommener Energie und Netzwerktransfer Wlan

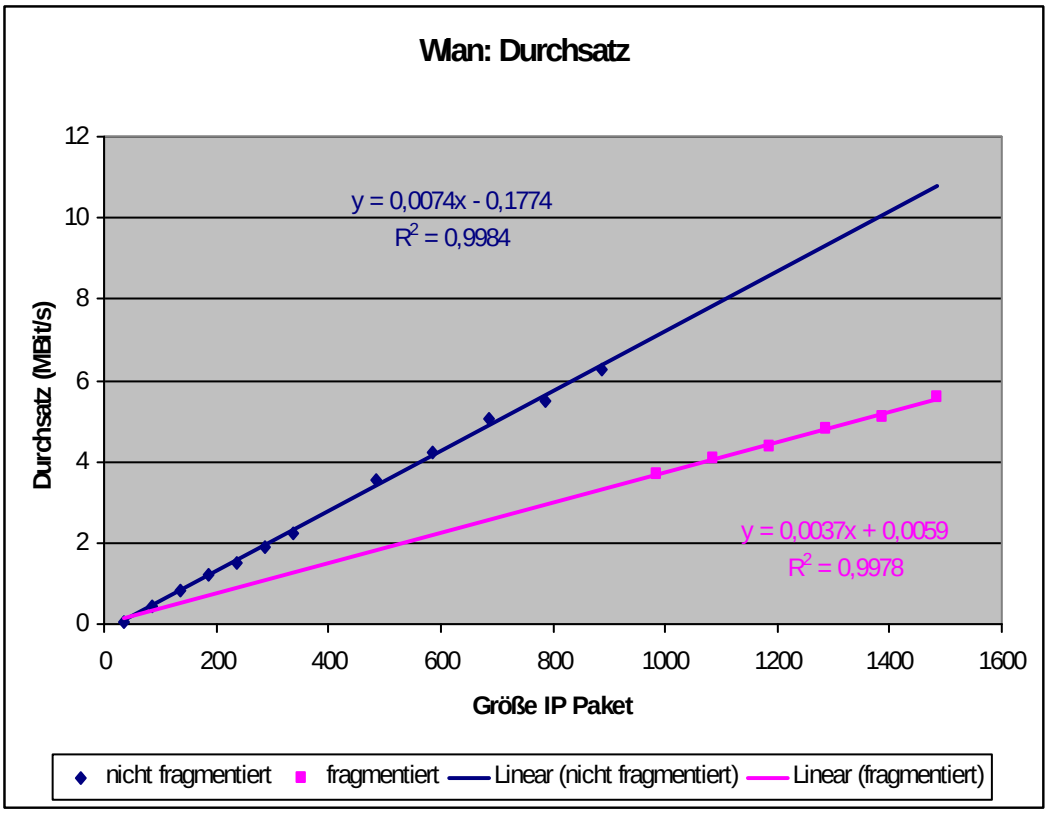


Abbildung 4: Erreichter Durchsatz Wlan

5.5 Messergebnisse Bluetooth

Die hier vorgestellten Messergebnisse wurden in folgendem Szenario ermittelt: der PANU verbindet sich mit dem NAP, um über diesen einen Verbindung zum Netzwerk herzustellen. Dabei wurden die Energiemessungen auf der Seite des PANU durchgeführt. Das bedeutet, dass der PANU in dem hergestellten Piconetz als Master auftritt, der NAP hingegen als Slave, da bei Bluetooth üblicherweise das Gerät zu Master wird, welches eine Verbindung initiiert. Zwar ist es möglich, diese Rollenverteilung dynamisch zu ändern, wobei hier aber kein Gebrauch davon gemacht wurde. Dass bedeutet insbesondere, dass der PANU für den Poll-Mechanismus im Piconetz zuständig ist. Somit ist zu erwarten, dass die Energieaufnahme des NAP insgesamt etwas geringer ausfällt als beim PANU. Da diese Arbeit aber nicht auf die möglichst energieeffiziente Nutzung einzelner Übertragungstechniken abzielt, wurde dieses potentielle Defizit für ein mobiles oder tragbares Gerät in Kauf genommen.

Bei der Messung der Energieaufnahme des verwendeten Bluetoothadapters traten keine Hinweise auf signifikante Messungenauigkeiten auf. Das ist auch in Abbildung 5 zu sehen, die den festgestellten Zusammenhang zwischen benötigter Energie und verwendeter Paketgröße darstellt. Die durch den Poll-Mechanismus auftretenden Pakete sind in die Ermittlung von BEB_c eingeflossen. Im Gegensatz zu Wlan bedarf es bei Bluetooth einer aktiven Kommunikation zwischen NAP und PANU, bis die BNEP Verbindung hergestellt ist. Gleiches gilt für auch für das Trennen dieser Verbindung. Insgesamt wurden folgende Werte ermittelt:

BEB_c : 0,1861 W

BEB_d : 0,109 W

$BEQ_s(x) := 2{,}4751 \cdot x + 128{,}3$

$BEQ_r(x) := 2{,}6529 \cdot x + 140{,}7$

$BEQ_{d \to c}$: 0,1466 Joule

$BEQ_{c \to d}$: 0,0901 Joule

Abbildung 6 zeigt die für die Berechnung von $BEQ_s(x)$ und $BEQ_r(x)$ verwendeten Werte für den jeweils gemessenen Durchsatz. Dieser verhält sich offensichtlich nicht linear zu den verwendeten Paketgrößen. Dies kann eingesehen werden, wenn die Funktionsweise von Bluetooth (wie in Kapitel 2.2 beschrieben) hinzugenommen wird. Pro Slot können 2871 Bits (inklusive Präambel und Paketkopf) übertragen werden. In dem hier untersuchten Szenario werden Pakete der Vermittlungsschicht durch das BNEP Protokoll um einen verkürzten Ethernet Paketkopf (11 Byte) ergänzt, sodass in einem Slot ein IP Paket mit einer Größe von 332 Bytes übertragen werden kann. Aus Abbildung 6 kann bis zu diesem Punkt ein linearer Anstieg des Durchsatzes festgestellt werden. Für größere Pakete werden drei oder fünf Slots belegt. Das bedeutet, dass bspw. für ein IP Paket mit einer Größe von 333 Byte gleich drei Slots belegt werden, wobei zwei von ihnen fasst vollkommen ungenutzt bleiben. Somit lässt sich die deutliche Abflachung der Messpunkte jenseits von 332 Bytes erklären. Der dargestellte logarithmische Trend, der für die Ergebnisse des Kapitels 6 verwendet wird, trägt diesem Wissen zwar keine Rechnung, wird aber als hinreichend genaue Abstraktion des soeben dargelegten Sachverhalts verstanden.

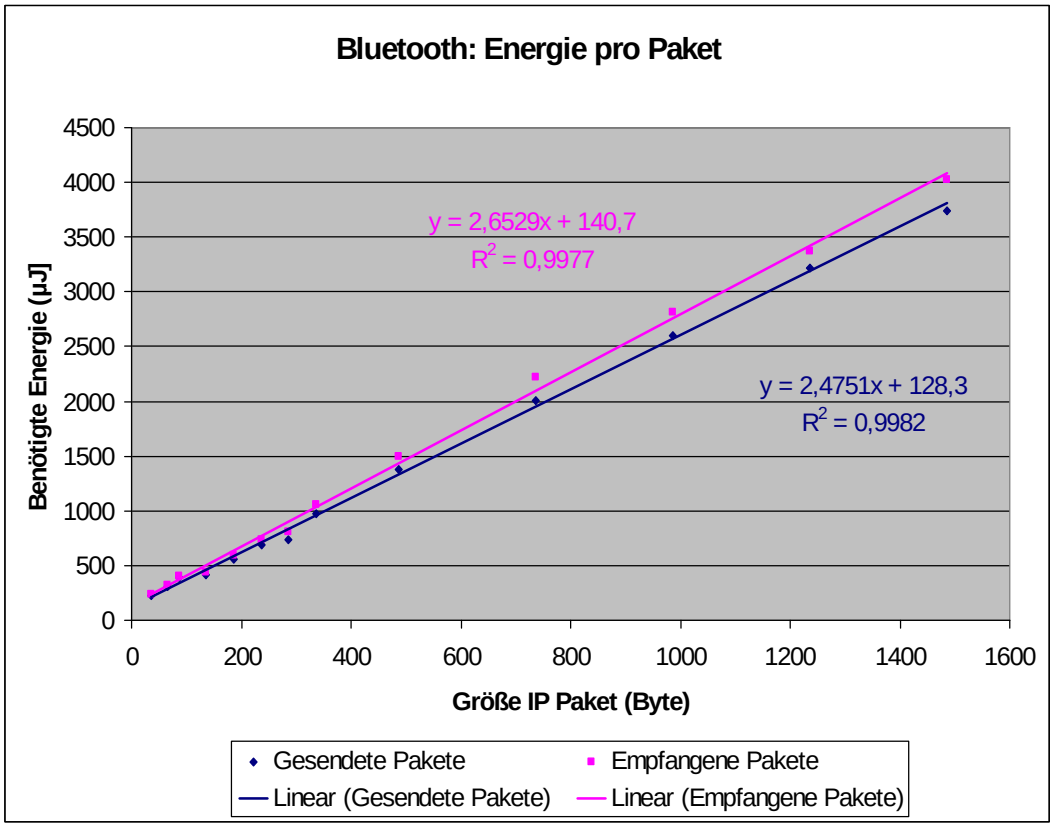


Abbildung 5: Relation zwischen aufgenommener Energie und Netzwerktransfer Bluetooth

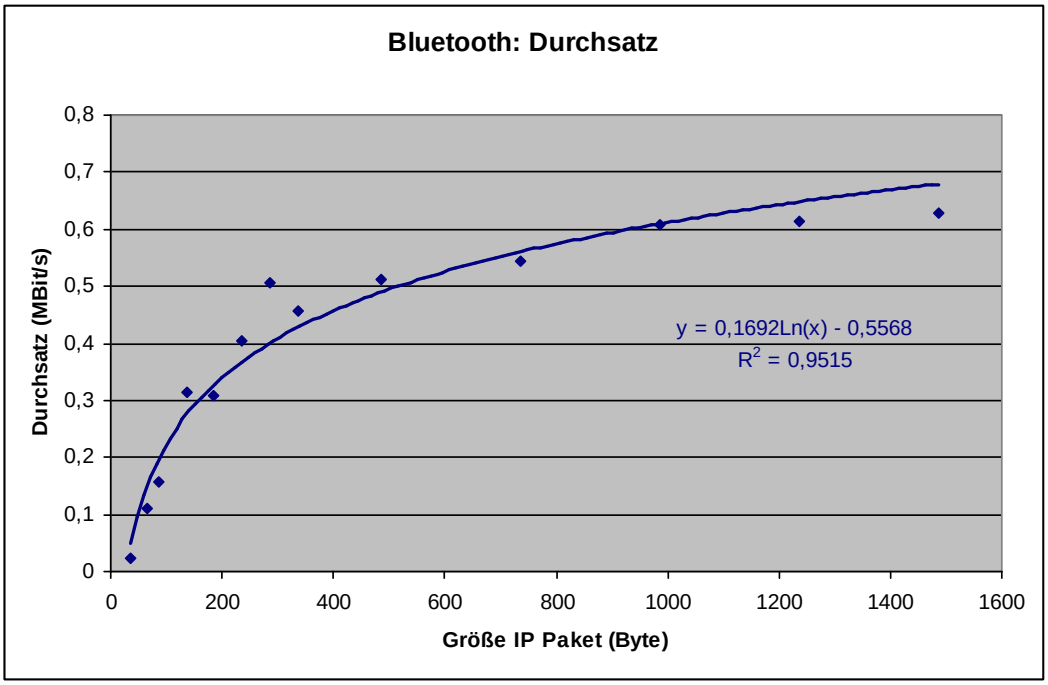


Abbildung 6: Erreichter Durchsatz Bluetooth

6 Strategien für energieeffiziente Netzwahl

6.1 Konsequenzen aus Energiemodell und Messungen

In diesem Kapitel werden die bisherigen Erkenntnisse benutzt, um eine Entscheidungsgrundlage dafür zu schaffen, wann von einer größeren Energieeffizienz eines untersuchten Netzwerkadapters im Vergleich zum anderen gesprochen werden kann. Aus den Messdaten, die in Kapitel 5 präsentiert wurden, wird deutlich, dass der verwendete Bluetooth Adapter selbst bei maximaler Auslastung eine Leistungsaufnahme aufweist, die geringer ist als WEB_c, also der aufgenommenen Energie des Wlan Adapters ohne Netzwerkverkehr. Allerdings können Daten über Wlan potentiell schneller übertragen werden als über Bluetooth, sodass die Wlan Schnittstelle eventuell früher in einen sparsameren Modus geschaltet werden kann. Offensichtlich hängt das direkt davon ab, mit welcher Bandbreite die zu übertragenden Daten zur Verfügung stehen. Ist diese beispielsweise unterhalb von 600 kbit/s, sodass Bluetooth sie in Echtzeit transferieren kann, ist klar, dass diese Funkverbindung energetisch effizienter ist als Wlan. Es ist jedoch möglich, dass es eine Bandbreite gibt, die einerseits von Wlan erreicht werden kann, und bei der andererseits bei gegebener zu übertragener Datenmenge die von Bluetooth zusätzlich benötigte Zeit für den Transfer die aufgenommene Energie beider Netzwerkadapter ausgleicht. Bei dieser Überlegung soll nun zunächst überprüft werden, ob es nötig ist, die Datenmenge tatsächlich konkret zu benennen. Dabei – wie auch bei folgenden Untersuchungen – wird nun das in Kapitel 5.2 vorgestellt Energiemodell mit den Daten verwendet, wie sie für die genutzten Netzwerkadapter gemessen wurden. Nehmen wir an, es sollen x MByte Daten übertragen werden. Für den Transfer der doppelten Menge von Daten bei gleicher Bandbreite wird dann von beiden Technologien die doppelte Zeit zum Transfer benötigt, was aufgrund der linearen Komponenten des Modells auch zu einem doppelt so hohen Bedarf an Energie beider Netzwerkadapter führt. Hier wurde bewusst die Einheit MByte gewählt um eine „hinlänglich große Datenmenge“ zu suggerieren, da ein gewisser Fehler in dieser Aussage unterschlagen wurde. Im Modell wird jedem einzelnen Paket ein Mindestbedarf an Energie beigemessen (was durch die Messergebnisse bestätigt wurde), der Vorverarbeitung, Präambel oder Paketkopf zugeschrieben wird. Es ist also möglich, dass bei der Übertragung von x MByte n Pakete benutzt werden, von denen eines (das letzte) nur maximal zur Hälfte gefüllt ist, sodass bei dem Transfer von 2x MByte nur 2n-1 Pakete übertragen werden müssen. Da beide Funkstandards mit unterschiedlichen Paketgrößen arbeiten, kann es also sein, dass diese Nicht-Verdopplung der Anzahl der Pakete auch zu einer geringeren Energieaufnahme bei zumindest einem der Adapter führt, als dies gerade behauptet wurde. Diese Feststellung zeigt jedoch auf, dass es nicht nur von der Bandbreite abhängt, ob Wlan und Bluetooth energetisch gleichziehen sondern auch von den verwendeten Paketgrößen, die natürlich wiederum Einfluss auf die Bandbreite haben können (siehe Kapitel 5).

Aus den erhobenen Messwerten und dem zugrundeliegenden Energiemodell wird nun eine Energieabschätzung für die beiden verwendeten Netzwerkadapter hergeleitet, die es erlaubt, sie hinsichtlich der aufgenommenen Energie zu

vergleichen. Es soll die Energie abgeschätzt werden, die für den Transfer einer bestimmten Datenmenge benötigt wird. Da grade festgestellt wurde, dass die Schlussfolgerungen auf die Energieeffizienz einer Netzwerkschnittstelle ab einem gewissen Grenzwert nicht mehr wesentlich von der konkreten Wahl der Menge der Daten abhängt, wird im Folgenden untersucht, welche Menge an Energie nötig ist, um ein MByte an Daten zu senden oder zu empfangen. Diese Abschätzung berücksichtigt folgende Größen: die Menge der zu übertragenden Daten, die Bandbreite mit welcher der Transfer stattfindet, und die Paketgrößen der Vermittlungsschicht. Für die beiden zuletzt genannten Größen kann dabei nicht a priori ein bestimmter Wert angenommen werden. Dies soll an einem einfachen Beispiel erläutert werden. Für den Transfer einer Datei von einem Megabyte kommen möglichst große Pakete zum Einsatz, die mit einem Durchsatz übertragen werden können, der die möglichen Bandbreiten von Bluetooth und Wlan voll ausnutzen kann. Dem entgegengestellt sei hier der Einsatz von Voice over IP (VoIP). Es ist wahrscheinlich, dass eine einzelne VoIP Verbindung eine deutlich geringere Bandbreite erfordert, als sie von beiden Übertragungsstandards zur Verfügung gestellt werden kann. Darüber hinaus können die Daten hierbei auf sehr kleine Pakete aufgeteilt sein, da dass Ausfüllen eines großen Pakets eine erhöhte Verzögerung zur Folge hätte. Das Inter Asterisk Exchange Protocol (IAX) etwa verwendet IP Pakete mit einer Größe von etwa 80 Byte. Daher werden die Größen Bandbreite und Paketgrößen bei einem energetischen Vergleich als variabel betrachtet.

Sind diese beiden Werte neben der zu übertragenden Datenmenge jedoch gegeben, kann auf die nun beschriebene Weise abgeschätzt werden. Zunächst einmal muss der Durchsatz ermittelt werden, der bei diesem Transfer zu beobachten sein wird. Dieser ist das Minimum der Rate, in der die Daten zur Verfügung stehen, und dem Durchsatz, der durch die verwendete Übertragungstechnik bei gegebener Paketgröße erreicht werden kann. Dafür werden hier die in Kapitel 5 herausgestellten Trendlinien benutzt, die in Abbildung 4 und Abbildung 6 dargestellt sind. Allerdings wird für sehr kleine Pakete kein negativer Durchsatz zugelassen, sondern dann der kleinste gemessene Wert als untere Grenze benutzt. Für Wlan wird dabei eine der beiden Trendlinien ausgewählt, je nachdem, ob die verwendeten Pakete größer als 886 Bytes sind oder nicht. Aus diesem Durchsatz kann die Zeit errechnet werden, die für den Transfer der gesamten Datenmenge benötigt wird. Nun kann EB_c verwendet werden, um die Energie des Adapters für diese Zeitspanne abzuschätzen, die unabhängig von der Übermittlung von Paketen aufgenommen wird. Hinzu kommt der Anteil an benötigter Energie pro Paket. Dieser hängt zum einen von der Anzahl der Pakete ab, die bei gegebener Datenmenge und Paketgröße festgelegt ist, zum anderen von deren Größe ab.

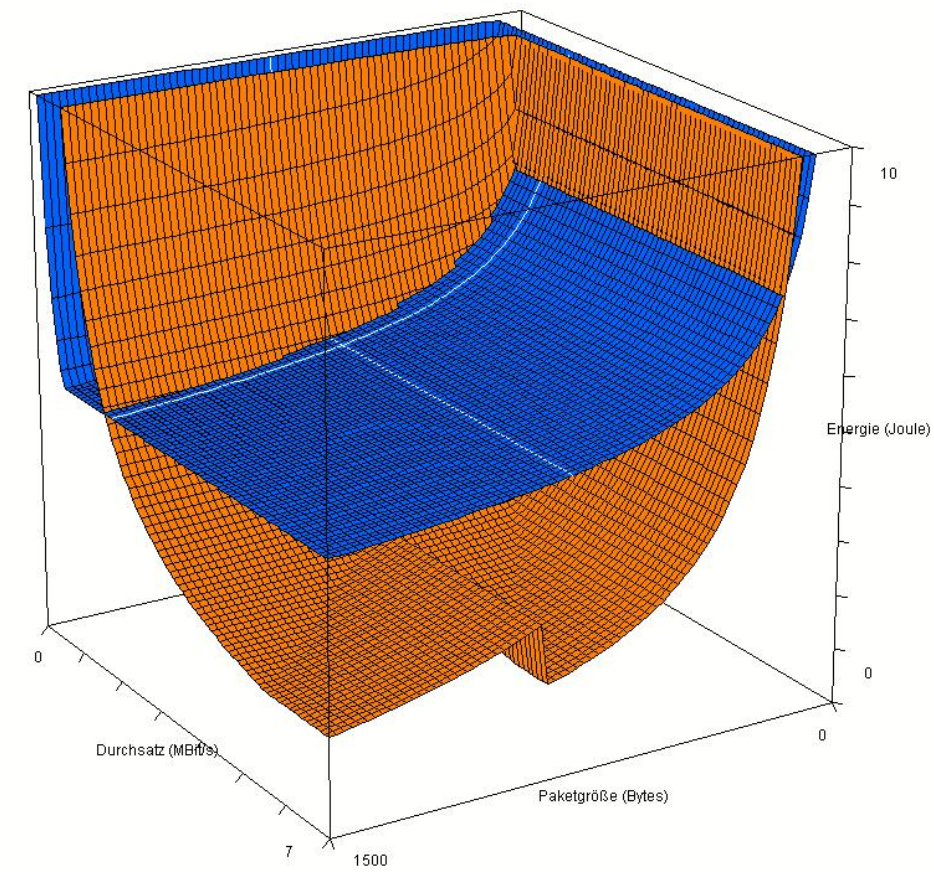


Abbildung 7: Versand von einem Megabyte durch Wlan (orange) und Bluetooth (blau)

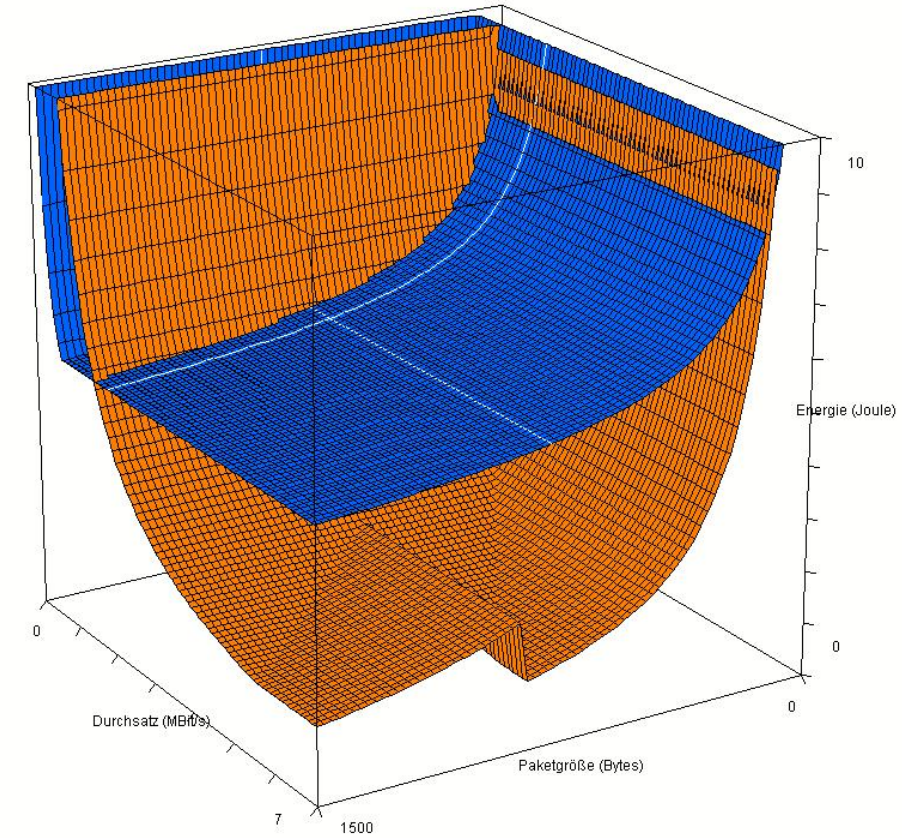


Abbildung 8: Empfang von einem Megabyte durch Wlan (orange) und Bluetooth (blau)

Bevor nun die Ergebnisse der gerade skizzierten Auswertung des energetischen Verhaltens der untersuchten Netzwerkadapter präsentiert werden, sollen an dieser Stelle noch zwei Hinweise eingeschoben werden. Zunächst einmal unterschlägt dieses Vorgehen noch einen weiteren Einfluss auf den Energiebedarf des untersuchten Systems. Während nämlich einer der beiden Adapter mit dem Netzwerk verbunden ist, nimmt auch der andere noch elektrische Energie auf. Daher währe es sinnvoll auf EB_c noch EB_d des jeweils anderen Adapters aufzuschlagen. Dies würde sich jedoch in einer deutlichen „Bestrafung“ der Energieeffizienz des Bluetooth Adapters auswirken, wie aus den gemessenen Größen aus Kapitel 5 leicht ersichtlich ist. Für ein mobiles oder tragbares Gerät soll daher angenommen werden, dass es möglich ist einen nicht verwendeten Netzwerkadapter effektiv abzuschalten.

Die zweite Anmerkung an dieser Stelle betrifft die Anwendbarkeit der Energieabschätzung in Echtzeit. Da sich die Zeit, die Anzahl der übertragenen Pakete und die Menge der übertragenen Daten leicht feststellen lässt, ist ein wichtiges Kriterium aus Kapitel 3.1 erfüllt, nämlich die Messbarkeit der Eingangsgrößen des Modells. Dabei ist es hier sogar möglich, diese Daten mit beliebiger Granularität zu erfassen ohne einen anderen Wert für die Energieabschätzung zu erhalten. Diese Eigenschaft hängt jedoch direkt von der Linearität von $EQ_s(x)$ und $EQ_r(x)$ ab.

Nach diesen Überlegungen folgt nun die grafische Auswertung des Energiebedarfs der beiden Netzwerkadapter, um einen MByte an Daten der Vermittlungsschicht zu senden (Abbildung 7) bzw. zu empfangen (Abbildung 8). Dabei zeigt die blau dargestellte Fläche den Energiebedarf des Bluetooth Adapters, während die orange Fläche den Wlan Adapter repräsentiert. Diese Diagramme zeigen deutlich auf, dass es Bereiche gibt, in denen jeweils einer der beiden Netzwerkadapter energieeffizienter ist als der andere. Die Bereiche werden durch die Schnittlinien der beiden Flächen voneinander abgegrenzt. Es ist zu erkennen, dass es sehr eindeutig vom auftretenden Durchsatz der Daten abhängt, wann die eine oder andere Übertragungstechnik vorzuziehen ist. Diese Größe scheint also eine gute Entscheidungsgrundlage zu sein, um in Echtzeit eine Entscheidung für die eine oder andere Netzwerkschnittstelle zu treffen. Allerdings muss zuvor noch geklährt werden, inwieweit dabei die Paketgröße berücksichtigt werden soll. Abbildung 7 suggeriert zunächst, dass der Bluetooth Adapter bei sehr kleinen Paketgrößen immer etwas energieeffizienter ist als der Wlan Adapter. Allerdings zeigt eine genauere Auswertung der Daten, dass Wlan bei solch kleinen Paketgrößen in den Tests ohnehin niemals den Durchsatz erreichte, der nötig wäre, um den energetischen Vergleich für sich entscheiden zu können.

Damit ist der Durchsatz nun tatsächlich als relevante Größe für eine Entscheidung zwischen den beiden Netzwerkschnittstellen ausgemacht. Nach der Anmerkung über die Linearität von $EQ_s(x)$ und $EQ_r(x)$ ist es zudem möglich den mittlerem Durchsatz über einen beliebigen Zeitraum zu nutzen. Allerdings verläuft die Schnittlinie zwischen den in Abbildung 7 und Abbildung 8 abgebildeten Flächen nicht parallel zu der Achse, welche die Paketgröße repräsentiert. Hingegen kann auch die Verwendung einer gemittelten Paketgröße auf ähnliche Weise legitimiert werden wie dies beim Durchsatz geschah: beim Abschätzen der Energieaufnahme mithilfe des hier verwendeten Modells beeinflusst die Paketgröße zwar den

messbaren Durchsatz jedoch nicht das Ergebnis der Abschätzung. Daher wurden die Schnittlinien der Flächen aus Abbildung 7 und Abbildung 8 numerisch ermittelt und mit einer logarithmischen Funktion beschrieben. Damit hat die hier präsentierte Auswertung des energetischen Verhaltens der Netzwerkadapter folgendes Ergebnis:

Der untersuchte Wlan Adapter ist energieeffizienter als der untersuchte Bluetooth Adapter, wenn mindestens eine der beiden folgenden Bedingungen erfüllt ist:

- Der mittlere Durchsatz gesendeter Daten ist größer als $0{,}2807 \cdot Ln(x) - 0{,}2827$ MBit/s, wobei x der mittleren Größe gesendeter Pakete in Bytes entspricht
- Der mittlere Durchsatz empfangener Daten ist größer als $0{,}2987 \cdot Ln(x) - 0{,}5708$ MBit/s, wobei x der mittleren Größe empfangener Pakete in Bytes entspricht

6.2 Abschätzung des Potentials vorgestellter Strategien

Es wurde aufgezeigt, wie sich das zugrundeliegende Energiemodell für paketorientierte Netzwerkadapter auf gegebene Hardware übertragen lässt. Darüber hinaus wurde aus ihm eine Entscheidungsgrundlage abgeleitet, die es erlaubt, die hier verwendeten Netzwerkadapter hinsichtlich ihrer Energieeffizienz zu bewerten. Nun soll für die in Kapitel 3.2 eingeführten Strategien abgeschätzt werden, welches Potential sie für die Vermeidung einer unnötigen Belastung der Energiequelle bereitstellen. Über diese Strategien soll nun noch einmal ein kurzer Überblick erfolgen, bevor sie im Einzelnen betrachtet werden:

1. Die Wahl des Netzwerkadapters beim initialen Verbinden mit dem Netzwerk
2. Das kurzzeitige Unterbrechen von Netzwerkverbindungen
3. Der dynamische Wechsel des verwendeten Netzwerkadapters
4. Die Aggregation von Paketen der Vermittlungsschicht

Dabei wird besonders die Situation betrachtet, in der das in Kapitel 4.2 vorgestellte Tunneln von Verbindungen benutzt wird. Für die Punkte 2. und 4. wird angenommen, dass diese sehr effektiv vom jeweiligen Übertragungsstandard der Sicherungsschicht realisiert werden können.

Bei der initialen Wahl des Netzwerkadapters kann eine energieeffiziente Wahl nur aufgrund der zukünftigen Nutzung des Netzwerks geschehen. Diese lässt sich zwar nicht immer mit Sicherheit bestimmen, jedoch können Rückschlüsse aus der in der Vergangenheit beobachten Nutzung gezogen werden. Nach den Ergebnissen aus Kapitel 6.1 können also bspw. der mittlere Durchsatz und die mittlere Paketgröße über einen längeren Zeitraum ermittelt werden und somit die Entscheidungsgrundlage bilden, welcher Netzwerkadapter bei der initialen Netzwahl bevorzugt werden sollte. Bei einem Nutzer, der verschiedene Dienste

über das Netzwerk nutzt, können sich diese etwa deutlich in ihrem Durchsatz voneinander unterscheiden. Daher kann eine Erhebung der durchschnittlichen Nutzung also etwas differenzierter vom jeweils verwendeten Dienst abhängig gemacht werden. Eine solche Zuordnung kann beispielsweise aufgrund der verwendeten Protokolle oberhalb der Sicherungsschicht oder für unterschiedliche Benutzerprogramme erfolgen. Entsteht die Verbindung zum Netz dann durch die Anforderung eines bestimmten Dienstes – also transparent für den Nutzer – kann die Wahl der Verbindung dezidierter durchgeführt werden.

Besteht eine Verbindung zum Netzwerk, die jedoch momentan nicht genutzt wird, kann diese vorübergehend unterbrochen werden. Damit sich dieses Vorgehen jedoch positiv auf die Energieeffizienz auswirkt, muss der Energieaufwand für $EQ_{c\to d} + EQ_{d\to c}$ geringer sein als $(EB_c - EB_d)\cdot t$, wobei t den Zeitraum der Trennung vom Netzwerk darstellt. Anhand eines Beispiels soll hier abgeschätzt werden, wie groß t mindestens sein muss, um für die hier untersuchten Netzwerkadapter eine vorübergehende Trennung zu rechtfertigen. Dabei soll folgendes Szenario zugrunde liegen: das mobile Gerät muss sich beim Herstellen der Verbindung beim Netzwerk authentifizieren. Der Vorgang bedarf den Transport nur weniger Pakete, benötigt jedoch eine Zeitdauer von einer Sekunde. Auch der Abmeldevorgang erfolgt durch wenige Pakete und braucht ebenfalls eine Sekunde. Dass bedeutet, dass die benötigte Energie pro übertragenem Paket hier vernachlässigt werden kann und $EQ_{c\to d}$ und $EQ_{d\to c}$ maßgeblich durch EB_c dominiert werden (was im Übrigen auch für die in Kapitel 5.5 gemessenen Werte für $BEQ_{c\to d}$ und $BEQ_{d\to c}$ zutrifft). Daraus ergibt sich, dass diese Trennung mindestens 3,57 Sekunden für Wlan bzw. 4,83 Sekunden für Bluetooth andauern muss, um die Energie für das Trennen und Wiederherstellen der Verbindung aufzuwiegen.

Eine ähnliche Abschätzung ist nötig, um zu entscheiden, wann die dynamische Umschaltung von Netzwerkadaptern effizient ist. Bei der in Kapitel 4.2 vorgestellten Strategie gibt es eine Zeitspanne, in der beide Netzwerkadapter mit dem Netz verbunden sind. Da dort auch nur verhältnismäßig wenige Pakete für die Kommunikation zwischen PTOUC und PTOUS benötigt werden, sollen sie auch bei der nun durchgeführten Abschätzung unterschlagen werden. Für die Anmeldung und Abmeldung am Netz werden dieselben Zeitenspannen angenommen wie im letzten Beispiel. Zunächst sei eine Bluetooth Verbindung hergestellt. Nun werden Daten über das Netzwerk angefordert, die mit einem Durchsatz von 100 MBit/s von der Quelle zur Verfügung gestellt werden können, also beide zur Verfügung stehenden Übertragungstechniken voll ausreizen. Somit ist es sinnvoll, auf die Verwendung von Wlan zu wechseln. Für diesen Wechsel ist zunächst ein zusätzlicher Energieaufwand von 1,1587 Jule nötig. Damit dieser von Wlan durch dessen höhere Bandbreite aufgefangen wird, muss der Transfer über die Wlan Verbindung mindestens 0,5 Sekunden andauern, wobei 0,376 MBytes an Daten übertragen werden.

Da der kritische Durchsatz, anhand dessen die Energieeffizienz der beiden hier verwendeten Netzwerkadapter verglichen wird, oberhalb der Bandbreite von Bluetooth liegt, kann jedoch im Vorfeld nicht endgültig entschieden, ob das Umschalten wirklich zu einer Einsparung der Energie führen wird. Diesem Problem kann auf zweierlei Arten begegnet werden. Zum einen können aufgrund

des verwendeten Protokolls Rückschlüsse gezogen werden. Zu anderen kann beispielsweise PTOUS, über den die Daten transportiert werden, zumindest für den Empfang von Daten auf der Seite von PTOUC Informationen darüber geben, ob diese potentiell mit einem höheren Durchsatz geliefert werden können, als sie momentan an PTOUC weitergeleitet werden. Die andere kritische Größe für die Effizienz des Umschaltens ist die Dauer, für die ein erhöhter Durchsatz zu erwarten ist. Diese kann anhand der zu übertragenden Datenmenge abgeschätzt werden. Im Kontext dieser Arbeit wurde hierfür der Zugriff auf den TCP Port 80 überwacht. Aus den so beobachtet HTTP Köpfen konnte die Menge der ausstehenden Daten aufsummiert werden, die der Nutzer angefordert hat.

Der Einsatz eines Tunnels zwischen dem mobilen Gerät und einer Gegenstelle bedeutet zunächst einmal eine Kapselung von Daten und damit mehr Informationen, die übertragen werden müssen. Dass dies durch eine sinnvoll eingesetzte Kompression zu keinem energetischen Mehraufwand führen muss ([EALDC]) soll hier nicht vertieft werden. Allerdings soll nun abschließend noch abgeschätzt werden, unter welchen Voraussetzungen die Aggregation von Paketen durch den Tunnel diese zusätzlichen Informationen energetisch abfedern können. Beim Einsatz der hier verwendeten Methode der Tunnelung (siehe Kapitel 4.2) kam es zu einem Overhead von 32 Byte pro Paket der Vermittlungsschicht. Durch Aggregation kann der damit verbundene Energiebedarf also eingespart werden, wenn im Mittel genügend Pakete für die Sicherungsschicht zusammengefasst werden, damit der konstante Anteil an benötigter Energie pro übertragenem Paket dem linearen Anteil für den Transfer dieses Overheads entspricht. Bei der untersuchten Hardware bedeutet dies, dass bei Wlan mindestens eins von 29 Paketen beim Senden bzw. eins von 1,87 Paketen beim Empfangen und bei Bluetooth eins von 1,62 Paketen beim Senden bzw. eins von 1,66 Paketen beim Empfangen durch Aggregation eingespart werden muss. Allerdings kann der Overhead auch dazu führen, dass die Anzahl der Pakete, die insgesamt übertragen werden müssen, ansteigt. Da jedoch nur für seltene Fälle angenommen werden kann, dass sich die Menge der zu übertragenden Informationen ausschließlich an der MTU eines bestimmten Standards orientiert, kann dieser Effekt wohl ignoriert werden.

7 Zusammenfassung und Fazit

In dieser Arbeit wurde ein Energiemodell für paketorientierte Netzwerkadapter eingeführt. Dieses Modell wurde benutzt, um einen Wlan- und einen Bluetoothadapter hinsichtlich ihrer Energieaufnahme exemplarisch zu beschreiben. Dabei stellte sich einerseits heraus, dass keiner der beiden generell energieeffizienter arbeitet als der jeweils andere. Andererseits wurde gezeigt, dass aufgrund des durchschnittlichen Netzwerkverkehrs entschieden werden kann, welcher Adapter in einer gegebenen Situation energieeffizienter arbeitet. Damit ein mobiles oder tragbares Gerät auf eine Veränderung des Netzwerkverkehrs hinsichtlich der Wahl des Netzwerkadapters möglichst flexibel reagieren kann, wurden Strategien vorgestellt, die es unter anderem erlauben, zwischen diesen umzuschalten, ohne dass laufende Datenübertragungen unterbrochen werden. Hier wurde zwischen Szenarien für ein LAN bzw. für ein WAN unterschieden, wobei in letzterem Fall der Einsatz eines Tunnels nötig ist. Die Bewertung der vorgestellten Strategien zeigte auf, dass diese, besonders wenn sie kombiniert eingesetzt werden, ein beachtliches Potential hinsichtlich der Einsparungsmöglichkeit von Energie und damit einer Erhöhung der Betriebsdauer für mobile und tragbare Geräte bieten.

8 Ausblick

Eine Annahme für diese Arbeit bestand darin, dass verschiedene verfügbare Netze bekannt sind und nicht nach ihnen gesucht werden muss. Dies ist jedoch besonders für tragbare Geräte wichtig, für die sich die Verfügbarkeit einzelner Netze ständig ändern kann. Um dieses Auffinden möglichst energieeffizient zu gestalten, können etwa Informationen über den momentanen Aufenthaltsort ausgenutzt werden. Dieser kann beispielsweise über das Global Positioning System (GPS) oder die Signalstärke eines verbundenen Netzes ermittelt werden.
Zudem wurden in dieser Arbeit Methoden vorgeschlagen, die über die zu erwartende zukünftige Nutzung des Netzwerks Auskunft geben können. Allerdings wurden hier keine Messungen durchgeführt, was den Energiebedarf solcher Methoden, wie etwa einer Protokollanalyse, betrifft.
Diese beiden genannten Punkte sind jedoch auf jeden Fall zu beachten, wenn die hier vorgestellten Strategien möglichst energieeffizient eingesetzt werden sollen.

A Anhang

A.1 Verzeichnis verwendeter Abkürzungen

ACK	Acknowledgment
ACL	Asynchronous Connectionless Link
ARP	Address Resulution Protocol
BNEP	Bluetooth Network Emulation Protocol
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTS	Clear To Send
CVSD	Continuously Variable Slope Delta
DHCP	Dynamic Host Configuration Protocol
DIFS	Distributed coordination Function inter Frame Spacing
DSSS	Direct Sequence Spread Spectrum
EIRP	Equivalent Isotropic Radiated Power
GPS	Global Positioning System
GSM	Global System for Mobile communications
HTTP	Hypertext Transfer Protocol
IAX	Inter Asterisk Exchange protocol
IP	Internet Protocol
IPMS	Internet Protocol Mobility Support
ISM	Industrial, Scientific and Medical
L2CAP	Logical Link Control and Adaption layer Protocol
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAP	Network Access Point
NAT	Network Address Translation
NDIS	Network Driver Interface Specification
OFDM	Orthogonal Frequency Division Multiplex
PAN	Personal Area Networking
PANU	Personal Area Network User
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PIFS	Point coordination Function inter Frame Spacing
PPP	Point to Point Protocol
RTS	Ready To Send
RTSP	Rapid Spanning Tree Protocol
SCO	Synchronous conection-oriented
USB	Universal Serial Bus
VoIP	Voice over IP
WAN	Wide Area Network

A.2 Literatur- und Referenzverzeichnis

[RFC3626] Thomas Heide Clausen, Philippe Jacquet: Optimized Link State Routing Protocol, http://www.ietf.org/rfc/rfc3626.txt, Oktober 2003

[IEEE] Institute of Electrical and Electronics Engineers, http://www.ieee.org

[BTSIG] Bluetooth Special Interest Group, http://www.bluetooth.org

[EECAWLAN] Jean-Pierre Ebert, Energy-efficient Communication in Ad Hoc Wireless Local Area Networks, http://edocs.tu-berlin.de/diss/2004/ebert_jeanpierre.pdf, April 2004

[RFC2002] Charles Perkins: IP Mobility Support, http://www.ietf.org/rfc/rfc2002.txt, Oktober 1996

[RFC3344] Basavaraj Patil, Phil Roberts: IP Mobility Support for IPv4, http://www.apps.ietf.org/rfc/rfc3344.html, 2002

[RFC1661] William Allen Simpson: The Point-to-Point Protocol, http://tools.ietf.org/html/rfc1661, Juli 1994

[EALDC] Kenneth Barr, Krste Asanovic: Energy Aware Lossless Data Compression, http://www.sigmobile.org/awards/mobisys2003.pdf, Mai 2003

[RFC4301] Stephen Kent, Karen Seo: Security Architecture for the Internet Protocol, http://tools.ietf.org/html/rfc4301, Dezember 2005

[EIPKA] Erik-Oliver Blaß, Holger Junker, Martina Zitterbart: Effiziente Implementierung von Public-Key-Algorithmen für Sensornetze, http://doc.tm.uka.de/2005/blass-sensornetz-key-algo-2005.pdf, September 2005

[AVM] AVM Computersysteme Vertriebs GmbH, http://www.avm.de

[BLUEZ] Official Linux Bluetooth protocol stack, http://www.bluez.org

[NDISW] Network Driver Interface Specification Wrapper, http://ndiswrapper.sourceforge.net/

A.3 Abbildungsverzeichnis

A.4 Erklärung zur Diplomarbeit

Ich versichere, dass ich die vorliegende Diplomarbeit – einschließlich darin enthaltener Grafiken und Darstellungen – selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Stellen der Arbeit, die dem Wortlaut oder dem Sinne nach anderen Werken entnommen sind, habe ich in jedem Fall unter Angabe der Quelle deutlich als Entlehnung kenntlich gemacht.

Karlsruhe, den 7.1.2008

Dominik Winkelmeyer
Georg-Friedrichstr. 19, WG 24
76131 Karlsruhe