



# **Unterlagen zum Hardwarepraktikum “Netzwerk-Technologien”**

**Klaus Heck, Stefan Köhler, Kenji Leibnitz**

**Stand: 17. Januar 2002**



## Vorbemerkung

Ziel des Hardware-Praktikums ist es, sich in Arbeitsgruppen Kenntnisse von Problemstellungen zu erarbeiten, die aus der Hardware resultieren. In den 4 Versuchen des Hardware-Praktikums "Netzwerk-Technologien" werden Probleme behandelt, die bei modernen Rechnernetzen auftreten.

- Versuch 1 behandelt die Bluetooth Technologie zur drahtlosen Übertragung von Daten im Personal Area Network (PAN) und Local Area Network (LAN).
- Im Versuch 2 werden die auf Funkübertragung basierende lokale Netzwerktechnologie Wireless LAN (WLAN, IEEE 802.11) untersucht und Messungen bezüglich ihrer Leistungsfähigkeit durchgeführt.
- Der Versuch 3 beschäftigt sich mit aktueller Routing Technologie. Es werden Routing Algorithmen kennen gelernt und in einem Testnetz konfiguriert und auf ihre Qualität hin untersucht.
- Versuch 4 führt von der Signaldarstellung auf digitalen Übertragungsstrecken über die Kodierung zur Multiplexbildung.

## Organisatorisches

Das Hardware-Praktikum gliedert sich in 4 Versuche, die in Gruppen mit maximal 3 Teilnehmern zu bearbeiten sind. Jeder Versuch besteht aus 3 Teilen: Versuchsvorbereitung, Versuchsdurchführung und Ausarbeitung eines Versuchsberichts.

Durch die Versuchsvorbereitung sollen die zur Versuchsdurchführung notwendigen Kenntnisse erworben werden. Sie beginnt mit der Lektüre der Versuchsbeschreibungen und der dort angegebenen Literatur und umfaßt die Einarbeitung in benötigte Programmpakete. Teilweise können Versuche zuhause oder in den Rechnerräumen des Instituts erprobt werden. Die Versuchsvorbereitung schließt die Abgabe entsprechender Unterlagen im Versuchsbericht mit ein. Alle Versuche müssen so vorbereitet sein, dass eine Abnahme durch den Betreuer innerhalb der vorgegebenen Zeit für die Versuchsdurchführung erfolgen kann.

Die Versuchsdurchführung erfolgt zu der im Praktikumsplan angegebenen Zeit in den angegebenen Räumen. Die Versuchsvorbereitung ist vor der Durchführung dem Betreuer vorzulegen. Die im Praktikumsplan angegebenen Zeiten sind unbedingt einzuhalten. Ohne ausreichende Vorbereitung kann keine Versuchsdurchführung zum Erfolg führen. Einen Ersatztermin wegen nicht ausreichender Vorbereitung gibt es nicht. Erfolgt zum angegebenen Termin keine Abnahme, so wird der Versuch als nicht durchgeführt gewertet. Alle Versuchsphasen sind dem Betreuer vorzuführen, der auch für Fragen zur Verfügung steht und Hilfestellung gibt. Jeder Versuch ist von allen Gruppenmitgliedern vollständig zu bearbeiten.

Die vollständige Durchführung eines Versuchs umfaßt die Abgabe eines Versuchsberichts, der die Versuchsvorbereitung, die Durchführung und die gewonnenen Einsichten auf ca. 2 DIN A4 Seiten dokumentiert. Der Versuchsbericht ist an dem auf die Versuchsdurchführung folgenden Tag abzugeben.

Die Bewertung des Gesamtversuchs erfolgt mit einer einfachen Klassifikation “-, 0, +”. Sollte zum Praktikumsende die Gesamtbilanz einer Gruppe negativ sein, so wird für diese Versuchsteilnehmer eine mündliche Prüfung durchgeführt. Sind ansonsten alle Versuche bearbeitet, wird ein Leistungsschein vergeben.

# 1 Bluetooth

In den vergangenen Jahren hat sich ein starker Trend zu drahtloser Kommunikation entwickelt. Es wurden verschiedene Standards erarbeitet und veröffentlicht, die auf unterschiedliche Anwendungsszenarien abzielen.

Einerseits wird durch die Einführung von GPRS momentan die Entwicklung von verbindungsorientierten zu paketerorientierten Diensten eingeläutet. Dies ist der erste Schritt hin zu UMTS (Universal Mobile Telecommunication System), mit dessen Einführung in den nächsten Jahren zu rechnen ist. Damit wird erreicht, dass die überwiegend für Sprachdienste genutzten Mobilteile eine möglichst flexible und auch kostengünstige Unterstützung von Datendiensten aller Art ermöglichen.

Andererseits wurden Standards entwickelt, wie Wireless LAN (WLAN, IEEE 802.11), Bluetooth, HiperLan/I, die auf eine weniger mobile als viel mehr drahtlose Kommunikation im lokalen Bereich abzielen. Wireless LANs werden dabei hauptsächlich für lokale Netze mit einer räumlichen Ausdehnung bis 100 Metern zum Einsatz kommen und somit eine Verkabelung der Geräte unnötig machen. Der Bluetooth Standard dagegen setzt auf eine möglichst einfache und billige Technologie, um auch Kleinstgeräte mit einem Funkchip ausstatten zu können. Die mit Bluetooth zur Verfügung stehende Bandbreite ist dabei geringer als bei WLAN. Das angestrebte Einsatzgebiet von Bluetooth befindet sich somit in einem etwas kleineren Radius und wird als Personal Area Network (PAN) mit einer Ausdehnung von 10 Metern angesehen.

In diesem Versuch sollen mehrere Rechner mit Hilfe von Bluetooth PCMCIA Karten verbunden und einige Messungen durchgeführt werden. Die gefundenen Ergebnisse sind mit den theoretisch möglichen Werten zu vergleichen und Abweichungen sollen erklärt werden.

## 1.1 Historische Entwicklung

Die Standardisierung von Bluetooth erfolgte in der Form einer technischen Spezifikation, die in der Zusammenarbeit vieler Firmen innerhalb einer speziellen Organisation, der *Bluetooth Special Interest Group* (kurz SIG), entstand. Darin spielen namhafte Firmen eine bedeutende Rolle, unter anderem Ericsson, Intel Corporation, International Business Machines Corporation (IBM), Nokia Corporation und Toshiba Corporation.

Die momentan aktuelle Spezifikation ist die Version 1.0B. Genauere Informationen und Neuigkeiten können auf der Homepage der SIG (siehe [1]) nachgelesen werden. Die meisten heute verfügbaren Geräte entsprechen dieser Spezifikation. Jedoch ist

die Entwicklung der Bluetooth Spezifikation bei weitem noch nicht abgeschlossen. Die angestrebte, endgültige Version 2.0 wird von der SIG für das Jahr 2003 erwartet. Darin sollen zahlreiche Erweiterungen und Mechanismen zur Verdoppelung der heute möglichen Bandbreite enthalten sein.

## 1.2 Netzwerk Topologie

Bluetooth Geräte, die eine Verbindung miteinander herstellen, nehmen unterschiedliche Rollen ein: ein Gerät wird als Master bezeichnet, während das andere die Rolle des Slaves übernimmt. Die Spezifikation erlaubt es jedem Gerät beide Rollen einzunehmen. Außerdem kann ein einzelnes Gerät Master einer Verbindung und gleichzeitig Slave für eine andere Verbindung sein. Die Rolle des Master bestimmt, welches Gerät für die Synchronisation der Übertragung von Daten auf der Verbindung verantwortlich ist.

Damit ergeben sich prinzipiell mehrere mögliche Topologien, um Bluetooth Geräte miteinander zu verbinden. Einerseits können an einen einzelnen Master mehrere Geräte angeschlossen sein, wie in Abb. 1 gezeigt. Eine solche Konstellation nennt man ein *Piconetz*.

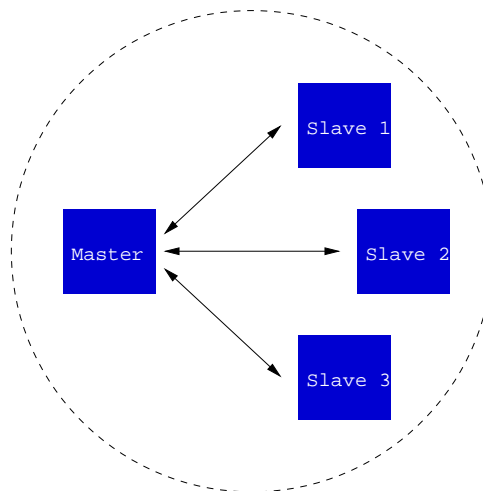


Abbildung 1: Master und Slave Rolle in einem einfachen Piconetz

Es sind aber prinzipiell auch andere Topologien vorstellbar, da ein einzelnes Bluetooth Gerät, wie oben beschrieben, mehrere Verbindungen gleichzeitig unterhalten kann. Dabei spielt es auch keine Rolle, ob ein Gerät dabei einmal Master und einmal Slave ist, oder ob das Gerät in beiden Verbindungen einen Slave darstellt. Solch eine Konstellation, wie sie auch beispielhaft in Abb. 2 dargestellt ist, nennt man ein Scatternetz.

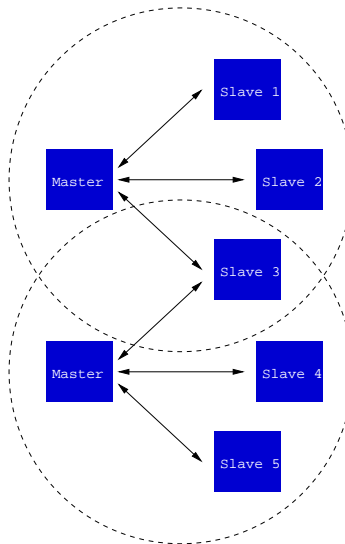


Abbildung 2: Beispiel eines Scatternetzes: ein Gerät ist Slave in zwei Piconetzen

### 1.3 Datenübertragung und Pakettypen

Um eine weltweite Benutzung der Bluetooth Technologie zu ermöglichen, muss ein global zur Verfügung stehendes Frequenzband für die drahtlose Übertragung von Daten verwendet werden. Außerdem sollten keine Lizenzgebühren für seine Nutzung anfallen. Ein Frequenzband, das diesen Anforderungen genügt, ist das sogenannte Industrial-Scientific-Medical (ISM) Band und liegt im Bereich von 2.000 bis 2.483,5 MHz in den USA und Europa (mit Einschränkungen in Spanien und Frankreich) und im Bereich von 2.400 bis 2.500 MHz in Japan. Konsequenterweise wurden, bis auf wenige regionale Ausnahmen, Frequenzen im Bereich von 2.400 bis 2.483,5 MHz für Bluetooth Geräte spezifiziert.

Da das ISM Frequenzband frei zugänglich ist, muss darin auch mit unvorhersehbaren Störungsquellen gerechnet werden, wie z.B. durch Babyphone, Garagenöffner und Mikrowellenherde. Um eine gegen Störungen möglichst robuste Übertragung zu gewährleisten, baut Bluetooth auf Frequency Hopping auf, d.h. für eine Übertragung wird nicht eine feste Frequenz verwendet, sondern es wird innerhalb eines Piconetzes die zur Übertragung verwendete Frequenz ständig verändert. Dazu müssen natürlich alle in einem Piconetz befindlichen Systeme die Reihenfolge der Frequenzen kennen.

Um diesen Mechanismus zu ermöglichen, wird die Zeitachse in Slots der Länge  $625\mu s$  aufgeteilt und jedem Slot eine eigene, mit Hilfe eines Pseudozufallszahlengenerators identifizierte Frequenz zugeteilt. Dies ist in der Abb. 3 angedeutet. Damit ergibt sich eine Hopping Frequenz von 1.600 Hops pro Sekunde.

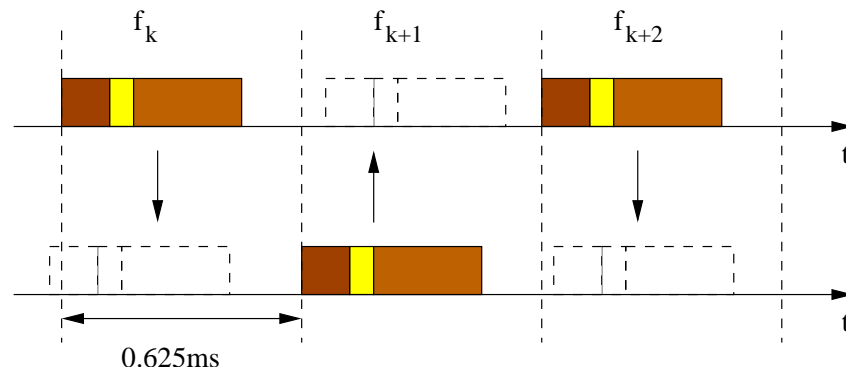


Abbildung 3: Frequency-hop/time-division im Bluetooth Kanal

Da die Bluetooth Technologie für den LAN und PAN Bereich eingesetzt werden soll, muss es möglich sein, beliebige Klein- und Kleinstgeräte mit einem solchen Funkchip auszustatten. Neben den daraus resultierenden Anforderungen an Stromverbrauch und Größe spielen die Komplexität und der Preis eine herausragende Rolle. Bluetooth sollte also so einfach wie möglich sein. Deshalb wurde ein Mechanismus eingeführt, der kollidierende Pakete in einem einzelnen Piconetz verhindert und somit eine komplizierte Kollisionserkennung und -auflösung unnötig macht. Deshalb wurden die unterschiedlichen Rollen Master und Slave definiert. Es liegt in der Verantwortung des Masters, die Hopping Sequenz zu bestimmen und den einzelnen Slaves jeweils Sendeerlaubnis zu erteilen.

Hierzu wird den Zeitslots jeweils eine Nummer zugeteilt. Slots mit gerader Nummer sind Masterslots, d.h. nur der Master darf sie zum Versenden der Pakete verwenden, und ungerade Nummern bezeichnen Slaveslots, d.h. der Slave, der für diesen Zeitslot die Sendeerlaubnis hat, darf ihn zur Übertragung nutzen. Kollisionen innerhalb eines Piconetzes können mit diesem einfachen Mechanismus ausgeschlossen werden.

Der Nachteil dieses Verfahrens liegt jedoch in der Einschränkung der Bandbreite. Angenommen ein Piconetz besteht nur aus einem Master und einem Slave, so kann der Slave im saturierten Fall (Slave hat immer Daten zu senden) nur die Hälfte der theoretisch möglichen Bandbreite von 1 Mbps nutzen. Um diesen Nachteil etwas einzuschränken, wurden verschiedene Pakettypen spezifiziert, nämlich 1-slot, 3-slot und 5-slot Pakete. Zur Verdeutlichung wird die Übertragung eines 3-slot Pakets in Abb. 4 gezeigt. Im Zeitslot  $k$  erteilt der Master einem Slave die Erlaubnis zu senden. Anstatt im darauffolgenden Slot ein einzelnes 1-slot Paket zu verschicken, entscheidet der Slave, ein 3-slot Paket zu verwenden. Dies deutet er im Header des verschickten Pakets an. Damit erkennt der Master sofort, um welche Art von Paket es sich handelt und wieviele Zeitslots der Slave für seine Übertragung in Anspruch nehmen wird.

Durch dieses Verfahren läßt sich die mögliche Bandbreite erhöhen. Die Tabellen 1



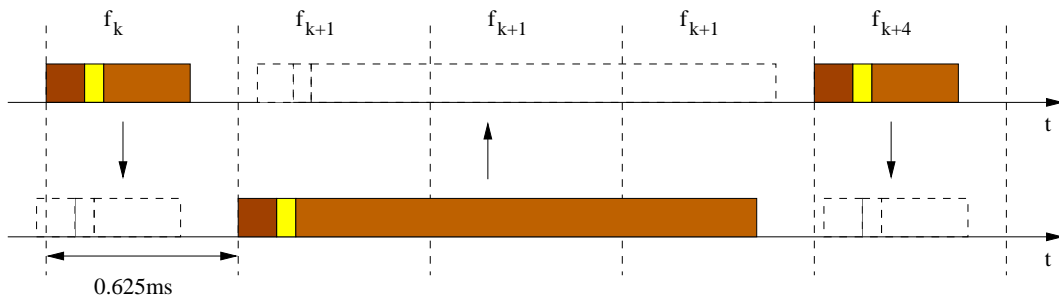


Abbildung 4: Beispiel eines 3-slot Pakets

und 2 zeigen die unterschiedlichen Pakettypen mit ihren jeweils maximal möglichen Durchsatzraten. Dabei unterscheidet man zwischen Synchronous Connection Oriented (SCO) Verbindungen, bei denen jeweils feste Slots für einen Slave reserviert werden (zum Einhalten von Bandbreitengarantien z.B. für Sprachdienste), und Asynchronous ConnectionLess (ACL) Verbindungen.

Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)	Asymmetric Max. Rate (kb/s)	
						Forward	Reverse
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	yes	172.8	172.8	172.8
DM3	2	0-121	2/3	yes	258.1	387.2	54.4
DH3	2	0-183	no	yes	390.4	585.6	86.4
DM5	2	0-224	2/3	yes	286.7	477.8	36.3
DH5	2	0-339	no	yes	433.9	723.2	57.6

Tabelle 1: Bluetooth ACL Paket Typen

Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)
HV1	na	10	1/3	no	64.0
HV2	na	20	2/3	no	64.0
HV3	na	30	no	no	64.0

Tabelle 2: Bluetooth SCO Paket Typen

## 1.4 Bluetooth Profile

Die vorigen Kapitel beschreiben im wesentlichen die unterste Schicht im Bluetooth Protokollstack und legen damit die grundlegenden Übertragungsmechanismen fest. Da die Bluetooth Funkchips in einer Vielzahl von unterschiedlichen Geräten eingesetzt werden sollen, unterscheiden sich auch die Anwendungsszenarien dieser Geräte immens. Um dennoch die reibungslose Interoperabilität zwischen den Geräten unterschiedlicher Hersteller zu gewährleisten, sind weitere Standardisierungen notwendig.

Hierzu wurden von der SIG die Bluetooth Profile mit in die Spezifikation aufgenommen. Ein einzelnes Profil definiert dabei ein gewisses Anwendungsszenario. Zum Beispiel definiert das Headset Profile (HSP) wie die Kommunikation zwischen einem Gateway Device, z.B. Bluetooth fähiges Handy, und dem Headset vonstatten gehen soll. Dabei werden Verbindungsaufbau, verwendete Pakettypen und weitere Festlegungen getroffen. Dadurch wird ermöglicht, dass auch ein Handy von Hersteller A mit einem Headset eines Herstellers B kommunizieren kann, ohne dass die beiden Hersteller sich absprechen müssen.

Die wesentlichen Neuerungen in der Bluetooth Spezifikation, Version 2.0, werden sich deshalb auf die definierten Profile beziehen. Neben dem HSP, welches zur Gruppe der Telephone Profiles gezählt wird, findet man in der Spezifikation 1.0B dann auch die Serial Port Profiles, z.B. für Fax, LAN Access oder Einwählnetze. Zusätzlich wurde noch ein Service Discovery Application Profile definiert, das es einem Bluetooth Gerät ermöglicht, in seiner Umgebung nicht nur nach anderen Bluetooth Geräten zu suchen, sondern auch deren Fähigkeiten bzw. angebotene Dienste zu erfahren.

## 1.5 Aufgaben

Für die in diesem Versuch durchzuführenden Aufgaben stehen Ihnen 3 Laptops mit Bluetooth PCMCIA Karten zur Verfügung. Die nötigen Treiber und die Software sind bereits installiert.

1. Konfigurieren Sie die 3 Laptops unter Zuhilfenahme der folgenden Angaben:

Rechnername	IP Adresse
mozart	10.10.1.1
bach	10.10.1.2
beethoven	10.10.1.3

Die Rechnernamen sind bereits konfiguriert. Außerdem sind auf dem Rechner "mozart" ein FTP Server installiert und die Bluetooth Karte schon korrekt eingestellt. Installieren Sie auf den Rechnern "bach" und "beethoven" die Karten und konfigurieren Sie die IP Adressen in den Netzwerkeinstellungen.

2. Verwenden Sie die Bluetooth Umgebung (ein Icon zum Starten ist auf dem Desktop zu finden), um die Rechner "bach" und "mozart" zu verbinden. Dabei soll "bach" Master und "mozart" Slave sein. Damit ist die Synchronisationsphase abgeschlossen und die Rechner können über ein Profile miteinander verbunden werden. Ziel ist es, einen FTP Client auf "bach" zu verwenden, um Daten von "mozart" zu ziehen. Erklären Sie dem Betreuer, welches Profil dazu nötig ist und verbinden Sie die Rechner miteinander.
3. Starten Sie einen FTP Client auf "bach" und ziehen Sie von "mozart" die Datei "c:\hwp\download.me". Führen Sie diesen Versuch 10mal durch und errechnen Sie die mittlere Durchsatzrate. Erklären Sie die maximal erreichbare Bandbreite bei diesem Profil und die von Ihnen gefundenen Ergebnisse.
4. Verbinden Sie nun zusätzlich den Rechner "beethoven" über die Bluetooth Umgebung als Slave mit dem Rechner "bach". Führen Sie erneut die Downloads durch, diesmal mit Rechner "beethoven" als FTP Client, "mozart" als FTP Server. Erklären Sie die gefundenen mittleren Datenraten im Vergleich zur vorigen Aufgabe.
5. Verwenden Sie nun das Audio Profil, um die Rechner "mozart" und "beethoven" miteinander zu verbinden. Konfigurieren Sie die beiden Rechner so, dass eine Audio Verbindung zwischen Ihnen hergestellt werden kann. Dazu muss die Audioverbindung auf beiden Rechnern als Quelle für die Audioausgabe und als Ziel für die Audioeingabe (Mikrophon) konfiguriert werden. Wie empfinden Sie die Sprachqualität? Kann zusätzlich noch ein Datentransfer stattfinden oder ist keine Bandbreite mehr frei?

## 1.6 Literatur zu Versuch 1

- [1] Homepage der SIG, <http://www.bluetooth.org>
- [2] Artikel zu Bluetooth:  
[http://www.ericsson.com/review/1998\\_03/article14.shtml](http://www.ericsson.com/review/1998_03/article14.shtml)
- [3] Windows Hilfetexte zur Bluetooth Umgebung; steht auf der Homepage des Lehrstuhls (siehe Hardware Praktikum) zum Download bereit

## 2 Wireless LAN

Die Wireless LAN (WLAN) Technologie hat sich in letzter Zeit sehr stark verbreitet. Mittlerweile sind viele öffentliche Plätze wie Hotels oder Flughäfen mit WLAN ausgestattet und jeder, der einen Laptop mit entsprechender Hardware besitzt, kann sich mit diesem lokalen Netz verbinden und ins Internet gehen.

Der Vorteil von WLAN im Gegensatz zu anderen drahtlosen Übertragungsmechanismen ist, dass der Standard im wesentlichen auf dem Ethernet Standard beruht, der sich in vielen Jahren beweisen konnte. Es wurden lediglich kleine Anpassungen vorgenommen, um die spezifischen Eigenschaften der Luftschnittstelle abzudecken. Aus Sicht von Applikationen, z.B. Internet Browsern, ist die neue Technologie vollständig transparent, d.h. es ergibt sich keinerlei Veränderung bei einem Umstieg von Ethernet zu Wireless LAN.

In diesem Versuch sollen Wireless LANs mit unterschiedlichen Topologien aufgebaut und die jeweiligen Vor- und Nachteile dieser Konfigurationen mit Hilfe von Messungen untersucht werden.

### 2.1 Historische Entwicklung

Im Juni 1997 wurde von der IEEE (Institute of Electrical and Electronics Engineers, Inc.) der erste Standard für Wireless LAN abgeschlossen. Er basiert im wesentlichen auf den Ethernet Standard IEEE 802.3 und wurde deshalb mit IEEE 802.11 bezeichnet. Der Standard spezifiziert die Verwendung des 2.4 GHz Frequenzbandes (ISM, siehe 1.3) mit maximalen Datenraten von 1 Mbps und 2 Mbps. Zusätzlich wurden zwei alternative Modulationschemen eingeführt: Frequency Hopping Spread Spectrum (802.11 FHSS) und Direct Sequence Spread Spectrum (802.11 DSSS).

Im Jahr 1999 veröffentlichte die IEEE mit den Standards IEEE 802.11a und 802.11b zwei Erweiterungen des ursprünglichen Ansatzes. Dabei wird durch IEEE 802.11b der 802.11 DSSS Standard erweitert und ermöglicht somit Datenraten im 2.4 GHz Frequenzband von bis zu 11 Mbps. Die meisten heute erhältlichen Wireless LANs richten sich nach diesem Standard.

Der 802.11a Standard dagegen definiert Datenraten von bis zu 54 Mbps, wobei als Modulation das Orthogonal Frequency Division Multiplexing im 5 GHz Frequenzband (ein ebenfalls frei verfügbares Frequenzband, das höhere Datenraten erlaubt) festgelegt wurde. Damit kann eine ganze Palette von unterschiedlichen Bandbreiten unterstützt werden, nämlich 6, 9, 12, 18, 24, 36, 48 und 54 Mbps. Die ersten Produkte, die IEEE 802.11a unterstützen, werden für Ende 2001 erwartet.

## 2.2 Verwendete Modulationsarten

Wie schon im vorigen Kapitel angeklungen, werden bei WLAN prinzipiell drei unterschiedliche Modulationsverfahren eingesetzt, nämlich Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) und Orthogonal Frequency Division Multiplexing (OFDM). Die Funktionsweise der drei Verfahren ist prinzipiell die folgende:

**Frequency Hopping Spread Spectrum:** Bei FHSS wird, wie schon bei Bluetooth kennengelernt, das zur Verfügung stehende Frequenzband in unterschiedliche Frequenzbereiche (Kanäle) unterteilt. Nach einem vorgegebenen Mechanismus wird eine pseudo-zufällige Sequenz von Kanälen ausgewählt. Alle Geräte, die miteinander kommunizieren wollen, müssen dabei dieselbe Sequenz kennen bzw. erzeugen können. Zusätzlich wird eine Hopping Rate festgelegt; sie bestimmt die Rate, mit der zu den durch die Sequenz bestimmten Frequenzbereichen gesprungen wird.

**Direct Sequence Spread Spectrum:** Das DSSS Verfahren verknüpft das zu sendende Datensignal am Sender mit einer Bit Sequenz, die eine höhere Datenrate besitzt. Diese wird häufig als Chipping Code oder Processing Gain bezeichnet. Das resultierende Signal wird anschließend übertragen. Je höher der Processing Gain, desto weniger anfällig wird das übertragene Signal gegenüber Interferenz, also Störungen der Luftschnittstelle.

**Orthogonal Frequency Division Multiplexing:** Bei der OFDM Modulation werden mehrere Kanäle benutzt, um Daten von einem Endgerät zu den anderen zu transportieren. Dabei haben die Kanäle jeweils eine geringere Bandbreite als der Ausgangsdatenstrom. Durch die parallele Verwendung mehrerer derartiger Kanäle erreicht man jedoch die gewünschte Datenrate. Die Orthogonalität der für die einzelnen Verbindungen genutzten Frequenzbereiche sorgt unter anderem für eine bessere Ausnutzung des verwendeten Spektrums und erhöht die Belastbarkeit gegenüber Interferenz.

Die in diesem Versuch verwendeten Geräte (Lucent Orinoco PC Card, Elsa LANCOM Wireless L-11 Access Point) entsprechen dem IEEE 802.11b Standard, d.h. als Modulation wird DSSS verwendet und die maximal erreichbare Bandbreite entspricht 11 Mbps. Weitere niedrigere Bandbreiten werden erreicht, indem ein entsprechend höherer Processing Gain verwendet wird. Damit wird außerdem erreicht, dass die Qualität der Verbindungen sich verbessert, also die Anfälligkeit gegenüber Interferenz gemindert wird. Andererseits ergibt ein höherer Processing Gain einen größeren maximalen Radius, in dem WLAN Geräte noch kommunizieren können.

## 2.3 Datenübertragung und Datenpakete

Die grundlegende Funktionalität von WLAN wurde vom Ethernet Standard IEEE 802.3 übernommen. Der wichtigste Mechanismus dabei, das Zugriffsverfahren CSMA/CD, wurde in der Vorlesung Technische Informatik II ausführlich besprochen. Darin wird festgelegt, wann eine Station Pakete auf das Medium schicken darf, wie mögliche Kollisionen entdeckt und schließlich aufgelöst werden.

Ein ähnliches Verfahren kommt mit CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) bei Wireless LANs zum Einsatz. Die Unterschiede liegen hauptsächlich in den Regeln zur Verwendung des Mediums, also in den Zugriffsrechten. Bei CSMA/CA wird zusätzlich ein Parameter "NAV" (Network Allocation Vector) benutzt, der dazu dient, die Dauer der Übertragung des letzten auf dem Medium gesendeten Datenpakets zu speichern und mit der Zeit herunterzuzählen. Dazu werden alle Pakete auf dem Medium mitgeschnitten und ihre Übertragungsdauer jeweils in "NAV" abgelegt. Nur wenn dieser Parameter auf "0" heruntergezählt ist und das Medium zusätzlich frei ist, erhält eine Station Sendeberechtigung. Dadurch wird die Wahrscheinlichkeit einer Kollision im Gegensatz zu CSMA/CD weiterhin verringert.

Kollisionen sind aber immer noch möglich. Wird eine Kollision erkannt, so greifen die von CSMA/CD bekannten Mechanismen mit dem Binary Back-Off Algorithmus.

2 Octets	2 Octets	6 Octets	6 Octets	6 Octets	2 Octets	6 Octets	0–2312 Octets	4 Octets
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Abbildung 5: Die Struktur von Wireless LAN Datenpaketen

Die Struktur der in WLANs eingesetzten Datenpakete ist in Abb. 5 dargestellt. Die Payload eines Datenpakets kann dabei beliebig im Bereich von 0 bis 2312 Bytes gewählt werden. Um prinzipiell Mechanismen wie Relaying (das Weiterleiten von Paketen durch Zwischenstationen) zu ermöglichen, wurden im Paketformat 4 Adressfelder vorgesehen. Sie werden auch häufig für andere Zwecke verwendet.

## 2.4 Aufgaben

Für die in diesem Versuch durchzuführenden Aufgaben stehen Ihnen 2 Desktop PCs mit PCMCIA Adapterkarten und ORINOCO PCMCIA WLAN Karten sowie ein EL-SA L-11 Access Point zur Verfügung. Der Access Point ist dabei die zentrale Einheit Ihres WLANs und ist mit einem Anschluss an das lokale Netzwerk ausgestattet.

Zur Konfiguration der ORINOCO Karten steht der ORINOCO Client Manager zur Verfügung. Die Software erlaubt Ihnen unter anderem, ein Profil auszuwählen. Für diesen Versuch brauchen Sie das Peer-to-peer Profil, um die beiden Desktop Rechner zu verbinden, und das Access Point Profil, um über den Access Point Zugriff in das lokale Netzwerk zu erhalten.

Zur Konfiguration des Access Point stellt Ihnen das Gerät einen HTTP Server zur Verfügung. Hierzu stellen Sie einen Desktop Rechner auf das Access Point Profil um und, vorausgesetzt die Netzwerkkonfiguration ist korrekt, greifen mit einem Web Browser auf das Gerät zu. Das zur Konfiguration notwendige Passwort ist beim Betreuer zu erfragen.

1. Erklären Sie Ihrem Betreuer den Unterschied zwischen dem Ethernet Protokoll (CSMA/CD) und dem bei WLAN eingesetzten Zugriffsprotokoll (CSMA/CA). Wie funktionieren die beiden Protokolle? Was sind die Unterschiede? Warum wurde das Ethernet Protokoll nicht einfach übernommen?
2. Überprüfen Sie die Konfiguration der beiden Desktop Rechner. Folgende Parameter sollten eingestellt sein:

Rechner	Name	IP Adresse
Desktop	goethe	132.187.106.151
Desktop	schiller	132.187.106.152
Access Point		132.187.106.242

Zeigen Sie dem Betreuer, wie die momentane Netzwerkkonfiguration aussieht und wie sie verändert werden könnte.

3. Starten Sie den ORINOCO Client Manager auf beiden Rechnern und stellen Sie das Peer-to-peer Profil ein. Damit sollten Verbindungen ermöglicht werden. Dies kann mit einem einfachen "ping" überprüft werden. Auf dem Rechner "goethe" ist ein FTP Server eingerichtet. Starten Sie einen FTP Client auf "schiller" und ziehen Sie die Datei "download.me". Wiederholen Sie den Versuch mehrere Male und berechnen Sie die durch FTP mittlere erreichte Bandbreite. Schätzen Sie den erreichten Durchsatz grob ab (ein Overhead von 10% kann angenommen werden). Ermitteln Sie dazu das Verhältnis zwischen theoretisch maximal möglicher und tatsächlich erreichter Datenrate.
4. Ändern Sie das benutzte Profil der beiden Rechner auf "Access Point", um damit Zugriff auf das lokale Netzwerk zu bekommen. Überprüfen Sie mit einem Web Browser die Konfiguration des Access Points, hauptsächlich die Übertragungsbandbreite (TX Rate). Sie sollte für diese Aufgabe 11 Mbps betragen. Verwenden Sie den FTP Client auf "schiller", um nun einen Download von Rechner "cerberus" im festvernetzten LAN auszuführen. Wiederholen Sie den Ver-

such wie in der obigen Aufgabe und geben Sie auch hier die mittlere erreichte Bandbreite an. Schätzen Sie den erreichten Durchsatz ab (siehe oben).

5. Starten Sie zusätzlich einen FTP Client auf Rechner "goethe" und führen Sie nun die Downloads von Rechner "cerberus" gleichzeitig von den beiden Rechnern "goethe" und "schiller" aus. Berechnen Sie die gemeinsam erreichte Bandbreite. Wiederholen Sie auch diesen Versuch 5 mal. Schätzen Sie den erreichten Durchsatz ab.
6. Verändern Sie mit Hilfe des Web Interfaces des Access Points dessen Konfiguration. Stellen Sie die vom Gerät angegebene maximale Sendebandbreite (TX Rate) auf 1 Mbps. Wiederholen Sie Aufgabe 4 mit der neuen Konfiguration.
7. Erklären Sie dem Betreuer die ermittelten Werte für den Durchsatz! Warum wird bei 11 Mbps ein geringerer prozentualer Wert erreicht als bei 1 Mbps?

## 2.5 Literatur zu Versuch 2

- [1] Homepage der IEEE: <http://www.ieee.org>
- [2] Artikel zu WLAN: <http://www.sss-mag.com/wlan.html#info>
- [3] Literatur zu den Orinoco WLAN Karten:  
[ftp://ftp.orinocowireless.com/pub/docs/ORINOCO/BROCHURES/ORiNOCO\\_World%20PC%20Card.pdf](ftp://ftp.orinocowireless.com/pub/docs/ORINOCO/BROCHURES/ORiNOCO_World%20PC%20Card.pdf)  
[ftp://ftp.orinocowireless.com/pub/docs/ORINOCO/MANUALS/ug\\_OM.pdf](ftp://ftp.orinocowireless.com/pub/docs/ORINOCO/MANUALS/ug_OM.pdf)
- [4] Literatur zum ELSA Access Point:  
<ftp://ftp.elsa.de/pub/FILES/DATACOMM/LANCOM/WIRELESS/LCIL11/MANUALS/WL11DOKG.ZIP>



## 3 Routing

Das Praktikum gliedert sich in 3 Teilgebiete:

- Subnetting
- Network Address Translation (NAT)
- Routing

### Ziel

Ziel des Praktikums ist es, die Computer in ein eigenes Subnetz zu bringen, das vom Uni-Netz über mehrere Pfade erreichbar ist. Dabei werden Sie das Routing Information Protocol RIP, das Routing Protocol OSPF und die Konfigurationsweise eines CISCO bzw. Linux Routers kennenlernen. Ein weiteres Ziel ist das Verständnis für Subnetting und der Network Address Translation (NAT), die einen Anschluss an das Netz der Universität Würzburg ermöglicht.

### 3.1 Benötigte Hard-&Software

- Netzwirkkabel
- Program Ethereal
- Program zebra (Routing unter Linux)
- 4 Computer (2x Linux, 2x Windows)
- 2 CISCO Router

### 3.2 Subnetting

Wie Sie in der Einführungsliteratur gelesen haben, ist es ziemlich verschwenderisch, ein ganzes Klasse C Netzwerk mit 254 möglichen Adressen für unseren Praktikumsaufbau zu verwenden. In der realen Welt eines Firmennetzwerkes sind die IP Adressbereiche aus obengenannten Gründen meistens in Subnetze aufgeteilt. Wir möchten nun in dieser ersten Aufgabe diesen Schritt ebenfalls vollziehen. Dazu werden zuerst

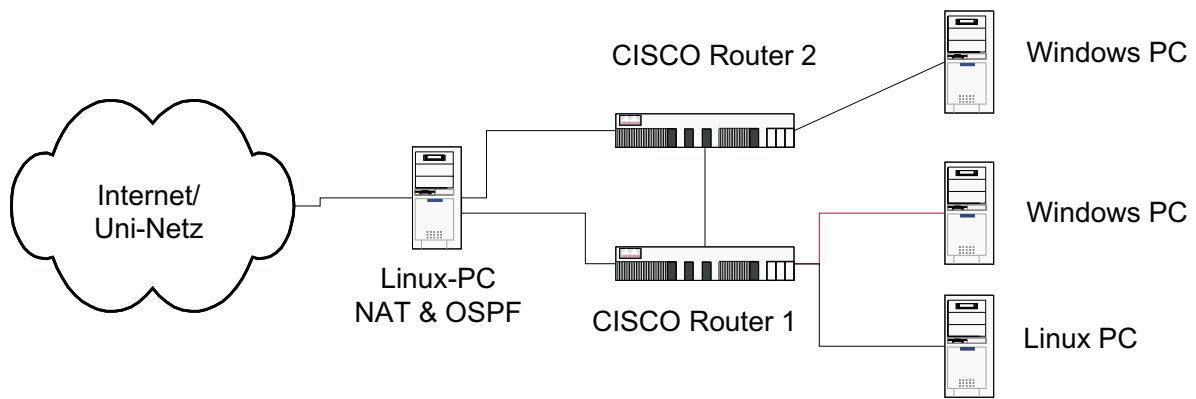


Abbildung 6: Versuchsaufbau

einige theoretische Fragen gestellt. Danach gilt es, den Router entsprechend zu konfigurieren. Für die weitere Bearbeitung des Praktikums ist es unerlässlich, dass die im Anhang angegebene Literatur gelesen wurde.

### **Berechnungen zum Subnet (vor Praktikumsbeginn zu erledigen)**

Der Netzwerkadministrator Ihrer Firma gibt Ihnen folgende Vorgaben: Ihnen steht das 32 IP Adressen umfassende C-Klasse Subnetz 192.168.1.64 zu.

- Geben Sie die Einteilung in Netzwerkadresse und Hostadresse eines normalen C-Klasse Netzwerks an.
- Nun wird Subnetting eingeführt:  
Wieviele Bits der 32 Bit umfassenden IP Adresse werden für Netz, Subnetz und Host verwendet?
- Welche ist die erste IP Adresse, die Sie für ein Gerät in Ihrem Subnetz verwenden können?  
Welche ist die letzte?
- Welche Adresse teilen Sie nun Router, Linux Server und Windows PCs zu?
- Neben einer IP Adresse ist nun auch eine Subnet-Maske nötig. Wie heißt die korrekte Subnetmaske für das Ihnen zugeteilte Netz?
- Führen Sie folgende Berechnung mit den in der Aufgabenstellung genannten Vorgaben durch: In welchem Netz (Nummer) befinden sich die IP Adressen 192.168.1.48 und 192.168.1.244?

### 3.3 Network Address Translation (NAT)

Als nächste Aufgabe werden wir Network Address Translation NAT näher betrachten. Im Praktikum wird NAT eingesetzt, um das Praktikumsnetzwerk vollständig vom Uni Netzwerk abzutrennen. Die Cisco Router sind dafür direkt mit einem Linux PC, welcher als NAT Box dient, verbunden. Um die Funktionsweise von Network Address Translation zu verstehen, werden wir einen TCP Transfer vor und nachdem NAT angewendet wurde aufzeichnen.

#### Aufgabe:

Bauen Sie die in Bild 6 dargestellte Topologie auf und verbinden Sie den Linux-Rechner sowohl mit dem Router als auch mit dem Uni-Netz. Konfigurieren Sie nach der Anleitung im Anhang folgenden NAT bzw. Masquerading auf dem Linux Rechner. Starten Sie nun Ethereal und beginnen Sie mit der Aufzeichnung beider Netzwerkkarten auf dem Linux-Rechner. Wir verwenden eine HTTP Verbindung auf [www.uni-wuerzburg.de](http://www.uni-wuerzburg.de), die wir vor und nach NAT vergleichen. Starten Sie telnet aus der Shell mit dem Befehl `telnet www.uni-wuerzburg 80` und geben Sie, sobald die Verbindung steht, zweimal einen Zeilenumbruch (return Taste) ein. Die telnet Verbindung wird sodann einige Zeilen HTML ausgeben. Das telnet Programm kann nun beendet werden. Stoppen Sie die Aufnahme in Ethereal und suchen Sie in der Detailansicht die korrespondierenden Pakete.

Vergleichen Sie die korrespondierenden Pakete des HTTP request und der dazugehörigen Antwort. Betrachten Sie für die nachfolgenden Fragen alle zu der von Ihnen initiierten Verbindung enthaltenen Pakete, also Verbindungsaufnahme und Datenpakete.

#### Fragen:

- Welche Einträge in den korrespondierenden Paketen haben sich mit NAT verändert?
- Welche Einträge passierten NAT unverändert?
- Die Checksumme auf Stufe TCP hat sich ebenfalls verändert, obwohl die Daten (payload) unverändert geblieben sind. Haben Sie hierfür eine Erklärung?
- Beschreiben Sie nun ausführlich, wie NAT funktioniert. Eine Skizze könnte dabei hilfreich sein!

## 3.4 Routing

Als letzte Thematik möchten wir uns mit Routing befassen. Wie Sie in der theoretischen Vorbereitung gelesen haben, befasst sich Routing - auf deutsch Verkehrs- oder Leitweglenkung - mit der Lenkung von IP Paketen durch das globale Netzwerk.

### Konfiguration des Routers

Der Cisco Router wird über die Kommandozeile konfiguriert. Die Kommandozeile des Routers wird normalerweise über ein Terminal erreicht, das an der seriellen Schnittstelle des Routers (Anschluss Console) angehängt ist. Sind die Netzwerkinterfaces richtig konfiguriert, kann dies auch über das Netz mit telnet geschehen. Das Betriebssystem, das auf den Routern läuft, heisst Cisco IOS - Cisco Internet Operating System. Das IOS kennt drei verschiedene Modi:

- User (unprivileged) Mode: Der User Mode ist jener Modus, in dem man sich nach dem Einloggen befindet. Dies analog zu einem Unix System, bei dem als nichtprivilegiertes User die meisten Konfigurationsfiles lesbar sind, jedoch keine Veränderungen abgespeichert werden können.
- Privileged Mode: Der privilegierte Modus des Cisco IOS entspricht dem Login als SuperUser im UNIX Betriebssystem. Hier können auch sicherheitsrelevante Konfigurationen angeschaut werden. Zusätzlich kann vom privilegierten Modus in den Konfigurationsmodus gewechselt werden.
- Configuration Mode: Der Konfigurationsmodus dient zur Konfiguration des Routers. Hier können alle Parameter verändert werden. Der Konfigurationsmodus wird durch Eingabe von control-z verlassen.

Der wichtigste Befehl des Cisco IOS heisst "?". In jedem Modus zeigt die Eingabe von "?" die möglichen Befehle an. Soll die Wirkung eines Befehls oder dessen Parameter angezeigt werden, geschieht dies durch Eingabe des Befehls gefolgt von "?", bzw. "show?". Wir möchten nun den Router für die neue Netzwerkumgebung konfigurieren.

Jedes Gerät mit Routingfunktionalität hat eine interne Routingtabelle. Im Linux Server haben wir diese Tabelle mit dem `route` Befehl statisch angelegt. Der Befehl

```
route add default gw IP_DES_ROUTERS,
```

den wir bei der Konfiguration eingegeben haben, trägt eine Default Route in die Routingtabelle ein. Das Betriebssystem weiss nun, dass alle Pakete an den Default-Gateway versendet werden, die nicht lokal bekannt sind. Dieser Eintrag ist statisch - d. h. der Eintrag wird nicht automatisch verändert, wenn sich die Netzwerktopologie ändert. Die Cisco Router wurden nicht mit statischem Routing konfiguriert. Unter den Routern wird das Routing Information Protocol RIP eingesetzt (zur Konfiguration siehe Literatur im Anhang). RIP ist ein Distance Vector Routing Protokoll. Es werden also sporadisch Routing Informationen zwischen jedem Knoten ausgetauscht. Ein Router versendet über jedes angeschlossene Interface ca. alle 2 Minuten ein RIP Paket, das alle Destinationen auflistet, die über den Router erreichbar sind.

### **Aufgabe:**

Verwenden Sie Ethereal um die RIP Pakete zu betrachten, die auf Ihr Subnetz versendet werden.

### **Fragen:**

- Welche Information beinhaltet ein RIP Paket?
- Welche Destinationen werden vom Router angepriesen?
- Was bedeuten diese Einträge?

### **Aufgabe:**

Wir möchten uns nun die Routingtabellen auf Router 1 ansehen. Loggen Sie sich wiederum mit telnet in Router 1 ein und wechseln Sie in den privilegierten Modus. Die interne Routingtabelle wird mittels dem Befehl show ip route angezeigt.

### **Fragen:**

- Welche Netzwerke sind direkt mit dem Router verbunden?
- Welche Netzwerke sind dem Router über RIP bekannt gemacht worden?
- Welcher Router ist jeweils der nächste Ansprechpartner für diejenigen Netze? Welchen Gateway nimmt der Router für alle ihm unbekannt Netze? Welches Gerät wird damit angesprochen?

### **Aufgabe:**

Wir betrachten nun die Konfiguration des Routers. Dies geschieht mit dem Befehl `show running-config`.

### **Fragen:**

- Betrachten Sie die Konfiguration des Routers. Welche Einträge sind für das Routing relevant?

Bisher haben wir immer Punkt-zu-Punkt Anwendungen betrachtet. Ping beispielsweise sagt nichts über den Weg aus, den ein Paket genommen hat. Ping besagt nur, dass ein Endpunkt erreicht worden ist. Unter Unix und Windows gibt es ein Tool namens `tracert` bzw. `tracert`, das mittels einem speziellen Verfahren den Weg, den ein Paket über das Netzwerk nimmt, anzeigt.

### **Aufgabe:**

Verwenden Sie `tracert`, um den verwendeten Weg zu `www.mainpost.de` zu bestimmen.

### **Frage:**

- Welche Knoten passiert ein Paket zwischen den Endpunkten? Nennen Sie nicht nur die IP Adresse sondern auch, welches Gerät zu den jeweiligen Adressen gehört. Die DNS Namen der einzelnen Stationen sagen oft etwas über verwendete Technologien oder den geographischen Standort aus.
- Was können Sie aus dem `tracert` zu `www.apple.com` alles herauslesen?

### **Aufgabe:**

Als nächste Aufgabe möchten wir die Arbeitsweise von `tracert` bestimmen. Starten Sie hierfür `Ethereal` und nehmen Sie ein `tracert` auf. Tip: Beachten Sie in der Aufnahme nur die UDP und ICMP Pakete. Die DNS Abfragen dienen der Auflösung

von IP Adressen zu Hostnamen. Dieser Vorgang hat keine Relevanz für das traceroute Protokoll. Betrachten Sie insbesondere die Unterschiede der einzelnen IP Protokoll-Header Einträge der UDP Pakete.

**Fragen:**

- An welche Destination und welche Portnummern werden die einzelnen Pakete geschickt?
- Wie bestimmt das traceroute Programm den eingeschlagenen Weg eines Datenpaketes?
- Wieso schicken die jeweiligen Stationen das Datenpaket zurück?
- Wieso schickt die letzte Station das Datenpaket zurück?

Mit traceroute kann eine weitere Einsatzmöglichkeit von ICMP veranschaulicht werden.

**Aufgabe :**

Nehmen Sie mit Ethereal ein traceroute an eine nicht existierende IP Adresse (z.B. 192.168.0.155) auf.

**Fragen:**

- Wer antwort auf das UDP Paket?
- Was wird dem Versender der UDP Pakete mitgeteilt?
- In der Ausgabe von traceroute erscheint ein Eintrag “!H”. Was wird damit angezeigt?

**Aufgabe:**

Wir betrachten als nächstes das Routing Protocol OSPF. Dazu verändern wir auf den beiden Cisco Routern und dem Linux Rechner (näheres siehe Literatur im Anhang) das Routing Protocol nach OSPF.

## Fragen:

- Welche Pakete können Sie OSPF zuordnen?
- Welchen Aufbau haben diese Pakete?
- Starten Sie traceroute und bestimmen Sie den Weg zum WWW-Server der Universität Würzburg
- Ändern sie mit Hilfe der Befehls `ip ospf cost xxx` die Linkkosten. Können Sie das Paket umlenken?

## 3.5 Literatur zu Versuch 3

- [1] Craig Hunt: TCP/IP Network Administration, O'Reilly & Associates, Inc.
- [2] Radia Perlman: Interconnections (Bridges and Router), Addison-Wesley 1993 (deutsch)
- [3] "Understanding IP Addressing: Everything You Ever Wanted To Know"  
[http://cache.3com.com/www.3com.com/other/pdfs/solutions/en\\_US/50130201a.pdf](http://cache.3com.com/www.3com.com/other/pdfs/solutions/en_US/50130201a.pdf) (Alles was man über IP-Adressierung und Subnetting wissen muss, wird hier beschrieben).
- [4] "Linux IP Masquerade HOWTO",  
<http://www.linuxdoc.org/HOWTO/IP-Masquerade-HOWTO.html>
- [5] "Linux IPCHAINS-HOWTO",  
<http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html>
- [6] Näheres zu Ethereal findet man unter  
<http://www.ethereal.com/>
- [7] Näheres zu zebra findet man unter <http://www.zebra.org>  
oder <http://pointless.net/~jasper/zebra-html/zebra.html>
- [8] Näheres zu CISCO Routern findet man unter  
<http://www.cisco.com>
- [9] Näheres zur OSPF Konfiguration der CISCO Router findet man unter  
<http://www.cisco.com/warp/public/104/1.html>
- [10] Näheres zur OSPF Konfiguration der CISCO Router findet man unter  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/sumadr.htm>
- [11] Wichtige RFCs zu RIP: 1058, 1582, 2453, 1923
- [12] Wichtige RFCs zu OSPF: 2328, 2329, 1850



## 4 Signalübertragung und Multiplexbildung

Ziel dieses Versuchs ist es, den Ablauf einer digitalen Übertragungsstrecke für ein Audiosignal bei einem Mobilfunksystem mit Codemultiplex-Mehrfachzugriff (*Code Division Multiple Access, CDMA*) nachzubilden. Die Durchführung erfolgt mit dem Softwarepaket *Matlab* von Mathworks.

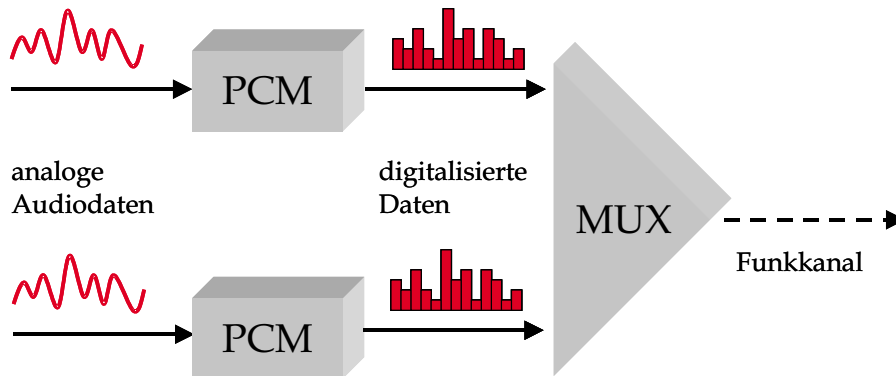


Abbildung 7: CDMA Übertragungsstrecke

Die Abbildung 7 stellt die einzelnen Komponenten des Übertragungssystems dar, die in den folgenden Teilaufgaben implementiert werden sollen. Zunächst wird das Eingangsaudiosignal mit dem *Pulscode-Modulationsverfahren (PCM)* in ein digitales Signal umgewandelt. Im Anschluss daran erfolgt eine Multiplexbildung mit CDMA, und das Signal wird über den Funkkanal übertragen.

### 4.1 Pulscodemodulation von Audiosignalen

#### 4.1.1 Audiosignale und ihre Darstellung

In den gebräuchlichen einfachen Audiodatenformaten, z.B. dem Microsoft WAV Format, werden die Abtastproben des Audiosignals sequenziell abgelegt. Anders als bei den Formaten mit Kompression, z.B. MPEG, speichern WAV Dateien die Samples im Rohformat ab, d.h. sie sind direkt ohne weitere Nachbearbeitung abspielbar.

Eine WAV Datei besteht aus drei Teilen: *RIFF* (12 Bytes) identifiziert die Datei als WAV, *FORMAT* (24 Bytes) gibt die Parameter des Files, z.B. die Samplerate, an und *DATA* beinhaltet die eigentlichen Audiodaten (Samples).

Im Format-Feld sind dabei die folgenden Informationen enthalten:

- Anzahl der Quantisierungs-Bits, z.B. 8 oder 16 *Bit*
- Art der Kompondierung, z.B. A-law,  $\mu$ -law
- Anzahl der Kanäle, z.B. mono oder stereo
- Abtastfrequenz, z.B. 8 *kHz*

Audiodaten für Sprache werden üblicherweise in 8 *kHz*, mono,  $\mu$ -law abgelegt, bei Audio CDs wird hingegen mit 44 *kHz*, stereo gearbeitet. Als Beispiel ist in Abb. 8 ein Ausschnitt der Datei 'ding.wav', die auf den Systemen von Microsoft mitgeliefert wird, dargestellt. Es handelt sich dabei um eine 8-bit, mono, 22050 *kHz* WAV Datei.

```

246E:0100  52 49 46 46 46 2D 00 00-57 41 56 45 66 6D 74 20          RIFF-..WAVEfmt
246E:0110  10 00 00 00 01 00 01 00-22 56 00 00 22 56 00 00          ..... "V.."V..
246E:0120  01 00 08 00 64 61 74 61-22 2D 00 00 80 80 80 80          ....data"-.....
246E:0130  80 80 80 80 80 80 80 80-80 80 80 80 80 80 80 80          .....
246E:0140  80 80 80 80 80 80 80 80-80 80 80 80 80 80 80 80          .....

```

Abbildung 8: Aufbau der WAV-Datei 'ding.wav'

Es gibt zwei prinzipielle Möglichkeiten, Audiosignale graphisch darzustellen: im *Zeitbereich* oder im *Frequenzbereich*. Werden die Amplituden der Abtastproben als Funktion über die Zeit geplottet, ergibt sich eine Darstellung wie in Abbildung 9(a). Das korrespondierende Spektrum ist in Abbildung 9(b) gezeigt. Die Transformation eines Signals vom Zeitbereich in den Frequenzbereich wird durch die Fourier Transformation durchgeführt. Da in dieser Aufgabe das Audiosignal immer als WAV Datei vorliegt und somit zeitdiskret ist, handelt es sich hier um die *Diskrete Fourier Transformation (DFT)*.

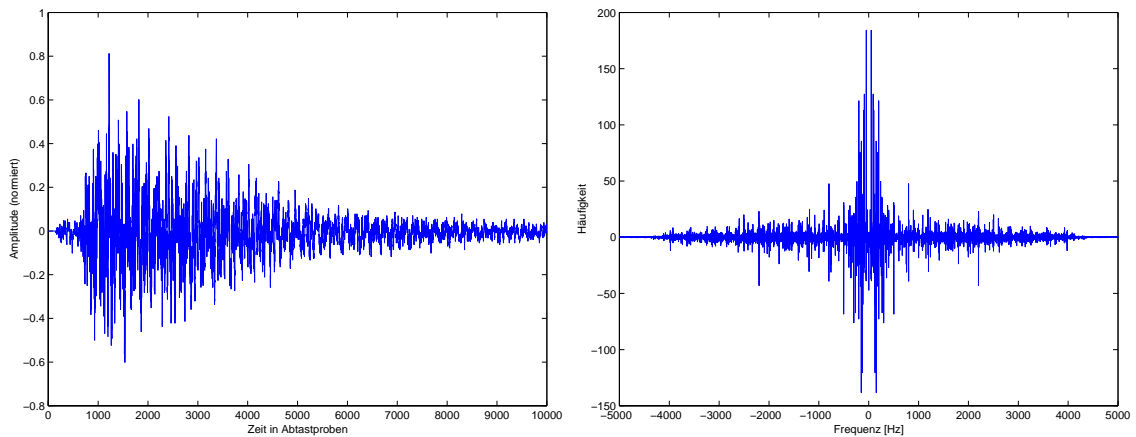
Ein effizienter Algorithmus zur Berechnung der DFT ist die *Fast Fourier Transformation (FFT)* nach folgender Vorschrift. Seien  $x_n, n = 1, \dots, N$  die Abtastproben im Zeitbereich, dann ist deren FFT ebenfalls ein Vektor der Länge  $N$ :

$$X_k = \sum_{n=1}^N x_n \exp \left( -j2\pi(k-1)\frac{n-1}{N} \right) \quad 1 \leq k \leq N.$$

Die Rücktransformation der DFT (inverse DFT) ist gegeben als:

$$x_n = \frac{1}{N} \sum_{k=1}^N X_k \exp \left( -j2\pi(k-1)\frac{n-1}{N} \right) \quad 1 \leq n \leq N.$$

Für eine ausführlichere Beschreibung der Diskreten Fourier Transformation wird auf 1 oder 2 verwiesen.



(a) Darstellung im Zeitbereich

(b) Darstellung im Frequenzbereich

Abbildung 9: Darstellungsarten der Audiodatei 'chord.wav'

#### 4.1.2 Die PCM-Übertragungsstrecke

Analoge Signale werden oft über eine digitale Strecke übertragen. Um die Konvertierung des Signals von analog nach digital durchzuführen, wird ein Verfahren angewendet, das *Pulscodemodulation (PCM)* genannt wird.

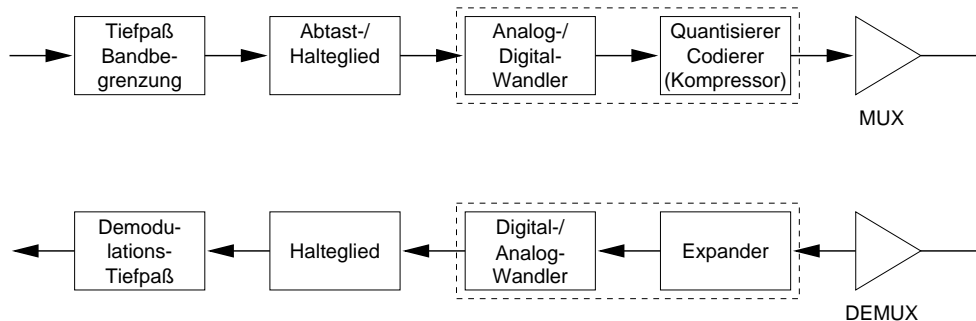


Abbildung 10: Die PCM-Übertragungsstrecke

Die Komponenten der PCM-Übertragungsstrecke sind in Abb. 10 dargestellt und bestehen aus: *Tiefpassfilter, Abtastung, Quantisierung/Kompondierung* und *Multiplexer*.

Im ersten Schritt wird das analoge Signal mit einem Tiefpassfilter bandbegrenzt. Dieser Schritt ist nötig, damit das Signal eine Grenzfrequenz  $f_g$  besitzt und somit das

Signal bei einer Nyquist-Abtastrate von  $2f_g$  ohne Verlust wiedergewonnen werden kann.

Die Abtastung kann dann an den diskreten Abtastzeitpunkten erfolgen, wodurch das wertkontinuierliche Signal von einem zeitkontinuierlichen in ein zeitdiskretes umgewandelt wird. Falls die Nyquist-Abtastrate hier nicht eingehalten wird, kann eine Über- bzw. Unterabtastung erfolgen, je nachdem, ob die Abtastrate kleiner bzw. größer als die Nyquist-Rate ist.

Der letzte Abschnitt bei der PCM-Strecke ist die Quantisierung und Kompondierung. Dieser Schritt wandelt das bisher noch wertkontinuierliche Signal in ein wertdiskretes um. Der einfachste Fall ist hierbei die *lineare Quantisierung* mit  $n$  Bit. Der Bereich der auftretenden Signalwerte wird dabei in  $2^n$  gleiche Stufen eingeteilt und die Zuordnung an die diskreten Werte erfolgt durch Auf- bzw. Abrunden. Das Runden an dieser Stelle verursacht jedoch einen Quantisierungsfehler, siehe Abb. 11.

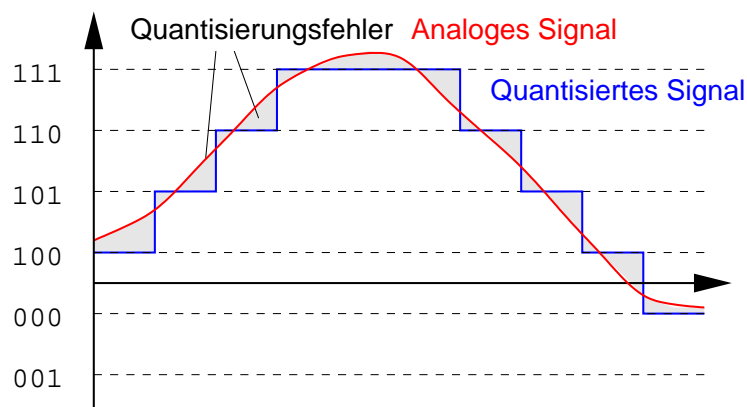


Abbildung 11: Fehler bei linearer Quantisierung

Um ein Maß für den Quantisierungsfehler zu haben, wird das Signal-Quantisierungsgeräusch-Verhältnis, engl. *signal-to-quantization-noise ratio (SQNR)*, definiert. Seien im folgenden  $s_i$  die digitalen Signalproben zu den Abtastzeitpunkten,  $q_i$  das quantisierte Signal an den Stellen und  $N$  die Anzahl der Samples. Dann lässt sich der Wert für SQNR wie folgt berechnen:

$$\text{SQNR} = \frac{1/N \sum_{i=1}^N s_i^2}{1/N \sum_{i=1}^N (q_i - s_i)^2}.$$

Da Signale und Signal-Geräusch-Verhältnisse oftmals um mehrere Größenordnungen

schwanken können, werden sie in der Regel in der logarithmischen Einheit dB (Dezibel) angegeben. Die Umrechnung einer linearen Signalstärke  $X_{\text{lin}}$  nach dB erfolgt gemäß folgender Gleichung:

$$X_{\text{dB}} = 10 \log_{10} (X_{\text{lin}}).$$

Anstelle einer linearen Quantisierung wird in der Praxis eine Kompondierung durchgeführt. Dies wird dadurch begründet, dass das Eingangssignal in der Realität nicht gleichverteilt, sondern um 0 konzentriert ist. Aus informationstheoretischer Sicht ist es daher günstiger, ungleiche Quantisierungsstufen zu nehmen und die Werte um 0 etwas genauer zu kodieren, während die äußeren Werte größere Quantisierungsstufen haben.

## 4.2 Aufgaben

Diese Aufgabe ist mit MATLAB durchzuführen. Dazu sollen Sie sich in einem ersten Schritt mit der Bedienung von MATLAB vertraut machen. MATLAB ist in den CIP Pools des Instituts, sowie in den Labors am Lehrstuhl installiert.

Zur Vorbereitung arbeiten Sie das Tutorial in der Online-Dokumentation durch. Sie erreichen es, indem Sie in der Kommandozeile den Befehl 'intro' eingeben. Lesen Sie auch im HTML Helpdesk den Abschnitt 'Getting Started' durch. Alternativ dazu können Sie die Dokumentation online lesen:

<http://www.mathworks.com/access/helpdesk/help/techdoc/matlab.shtml>

Für die Implementierung der Aufgaben benötigen Sie die folgenden MATLAB-Funktionen: `fft`, `fftshift`, `linspace`, `wavread` und `sound`. Schlagen Sie diese Funktionen in der Online-Hilfe nach.

1. Erzeugen Sie ein mit  $8\text{kHz}$  abgetastetes  $400\text{ Hz}$  Sinus-Signal. Plotten Sie das Spektrum des Signals. Achten Sie dabei auf die richtige Achsenbeschriftung!
2. Laden Sie nun die Sprachdaten aus der Datei 'speech.wav' und zeigen Sie das Spektrum des Signals an. In welchem Frequenzbereich befindet sich die wesentliche Information des Signals?
3. Implementieren Sie die MATLAB-Funktion 'lowpass', die eine Tiefpassfilterung durchführt. Die Funktion erhält den Signalvektor, die Abtastfrequenz des

Signals und die Grenzfrequenz des Filters als Eingabe und gibt das gefilterte Signal zurück.

Variieren Sie die Grenzfrequenz des Tiefpasses und die Abtastrate. Wann erfolgt eine Unter- bzw. Überabtastung? Wie wirkt sich das auf das ausgegebene Audiosignal aus?

4. Implementieren Sie die MATLAB-Funktion `'sample'`, welche eine Neuabtastung durchführt. Die Funktion erhält den Signalvektor und dessen Abtastfrequenz sowie die neue Abtastfrequenz als Eingabe und liefert das neu abgetastete Signal zurück. Da das Eingangssignal schon in Abtastproben vorliegt, kann für die Neuabtastung Interpolation notwendig sein.
5. Implementieren Sie die MATLAB-Funktion `'linquant'`, die eine lineare Quantisierung realisiert. Die Funktion erhält den Signalvektor und die Länge eines quantisierten Wertes in *Bit* als Eingabe und gibt das quantisierte Signal zurück. Wieviele Bit sind bei der Quantisierung minimal notwendig, um ein noch verständliches Ausgangssignal zu erzeugen?  
Ändern Sie die Funktion `'linquant'` so ab, dass anstelle des quantisierten Wertes die Quantisierungsstufe ausgegeben wird.
6. Benutzen Sie die von Ihnen in den Teilaufgaben 3, 4 und 5 implementierten Funktionen dazu, das Sprachsignal mit  $8\text{kHz}$  PCM zu modulieren. Führen Sie die PCM-Modulation mit  $8\text{--}16\text{bit}$  Quantisierung durch und berechnen Sie jeweils die SQNR. Plotten Sie die SQNR über die Anzahl der Quantisierungs-Bits. Um wieviel *dB* verbessert sich die SQNR pro zusätzliches Bit?

## 4.3 Codemultiplex-Schaltung

### 4.3.1 Prinzipien der Codemultiplex Übertragung

Damit mehrere Benutzer gleichzeitig auf die Ressource des Übertragungskanal zugreifen können, ist Multiplexen notwendig. Bei der Übertragung in einem Mobilfunkkanal sind die Verfahren für den Mehrfachzugriff gegeben durch:

**FDMA (Frequenzmultiplex):** Jeder Benutzer erhält eine Frequenz für die Übertragung, die er die ganze Dauer seines Gespräches nutzen kann.

**TDMA (Zeitmultiplex):** Die Zeitachse wird in Zeitslots diskretisiert und jeder Benutzer erhält nach einer gewissen Vorschrift die Zeitslots für sein Gespräch. Diese Methode kann auch mit FDMA kombiniert werden. Dieses kombinierte

F/TDMA Verfahren wird bei dem europäischen GSM (Global System for Mobile Communication) angewendet.

**CDMA (Codemultiplex):** Jeder Benutzer bekommt einen eindeutigen Code (z.B. eine Binärfolge), den er mit der Nachrichtenfolge korreliert.

Das CDMA Zugriffsverfahren fällt unter die Kategorie *Spread Spectrum* Mehrfachzugriff, bei dem eine Bandbreite zur Übertragung verwendet wird, die um mehrere Größenordnungen größer ist als die benötigte Funkbandbreite (Spreizung). Durch Verwendung eines Rauschträgers, d.h. einer Zufallsfolge, wird das schmalbandige Nutzsignal in ein breitbandiges Rauschsignal umgewandelt. Auf diese Weise trägt jeder Teilnehmer zum Hintergrundrauschen bei. Die Kapazität wird somit durch die Interferenz limitiert und ist im Idealfall wesentlich höher als bei herkömmlichen Systemen (Shannon 1948). Es gibt zwei Arten von Spread Spectrum Zugriffsverfahren, *Frequency Hopped* und *Direct Sequence*. Im folgenden wird nur die Direct Sequence Variante betrachtet, die auch als *Code Division Multiple Access* (CDMA) bekannt ist.

Die Entwicklung von CDMA wurde hauptsächlich aufgrund ihrer geringen Störanfälligkeit und hohen Abhörsicherheit vor allem im militärischen Bereich vorangetrieben. Aufgrund der überlegenen Kapazität dieser Systeme werden sie in den letzten Jahren auch verstärkt in der Telekommunikation eingesetzt. Neben dem Einsatz im Satelliten-Bereich wird in den USA und einigen anderen Ländern das *cdmaOne* Mobilfunksystem eingesetzt. In Europa werden ebenfalls die Mobilfunksysteme der nächsten Generation, *Universal Mobile Telecommunication System* (UMTS), mit einem Wideband-CDMA (W-CDMA) als Zugriffsverfahren über die Funkschnittstelle arbeiten.

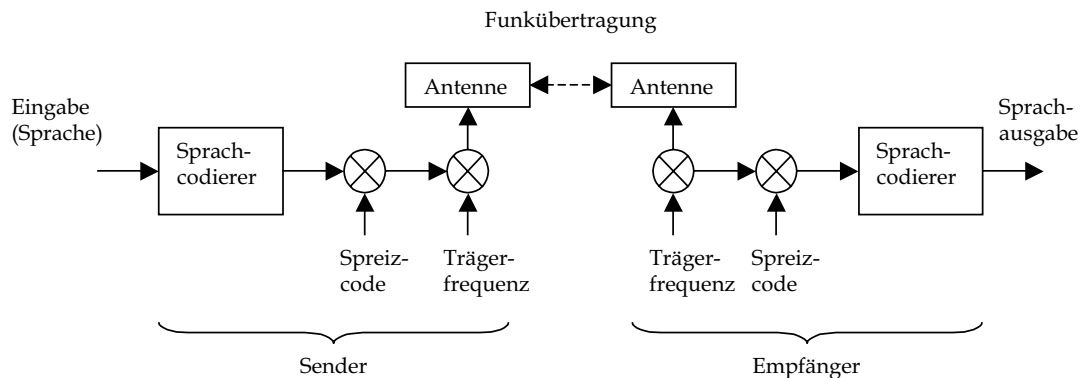


Abbildung 12: Ablauf einer Codemultiplex-Schaltung

Der prinzipielle Ablauf bei CDMA für die Sprachübertragung ist in Abb. 12 dargestellt. Die ankommenden Eingangssignale werden nach der Sprachcodierung mit

einem sogenannten Spreiz-Code (auch bekannt unter Chip-Folge) multipliziert. Diese Codefolge besitzt dabei eine wesentlich höhere Frequenz als das Datensignal, und führt somit nach der Multiplikation zu einer "Spreizung" des Signals. Da alle Teilnehmer auf dem gleichen Frequenzband senden, überlagern sich ihre Signale auf der Funkschnittstelle. Nach der Funkübertragung und der Demodulation wird das empfangene Signal mit dem Code des Empfängers multipliziert (korreliert) und das korrekte Signal zurückgewonnen.

### 4.3.2 Orthogonalität von Codes

Die wichtigste Eigenschaft, die ein Code bei CDMA haben muss, ist die *Orthogonalität*. Je besser diese Eigenschaft gegeben ist, umso besser eignet sich der Code für die Übertragung. Zwei reellwertige kontinuierliche Signale  $x$  und  $y$  sind dann orthogonal, falls ihre *Kreuzkorrelationsfunktion*  $R_{xy}(0)$  über den Zeitraum  $T$  null ist.

$$R_{xy}(0) = \int_0^T x(t) y(t) dt \stackrel{!}{=} 0.$$

Falls die Signale zeitdiskret sind, wird die Orthogonalität über das Kreuzprodukt definiert.

$$R_{xy}(0) = \sum_i x_i y_i \stackrel{!}{=} 0.$$

Neben der Kreuzkorrelation sollte jeder Code innerhalb einer Menge von orthogonalen Codes die gleiche Anzahl an Einträgen "1" und "-1" haben. Diese Eigenschaft gewährleistet eine Pseudo-Zufälligkeit des Codes. Als dritte Eigenschaft muss gelten, dass das Kreuzprodukt des Codes mit sich selbst (skaliert nach der Länge) gleich eins sein soll, d.h. es muss gelten:

$$R_{xx}(0) = \sum_{i=1}^I x_i x_i \stackrel{!}{=} 1.$$

Somit gelten zusammenfassend die folgenden Eigenschaften für eine Menge von orthogonalen Codes:

1. Die Kreuzkorrelation von paarweise unterschiedlichen Codes ist null (oder sehr klein).
2. Jede Sequenz besitzt die gleiche Anzahl von "1" und "-1" (oder unterscheidet sich um maximal 1).



3. Das skalierte Kreuzprodukt jedes Codes mit sich selbst ergibt 1.

Codefolgen können auf unterschiedliche Weise erzeugt werden, z.B. durch *Walsh-Codes* oder *Quasi-Orthogonale Codes*. Walsh-Codes werden nach der folgenden Vorschrift generiert. Für ein System mit  $N$  Codes (d.h. max.  $N$  Teilnehmer) wird rekursiv die Matrix  $H_N$  generiert. Die Zeilen der Matrix ergeben die Codes, die zueinander orthogonal sind.

$$H_1 = -1 \qquad H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

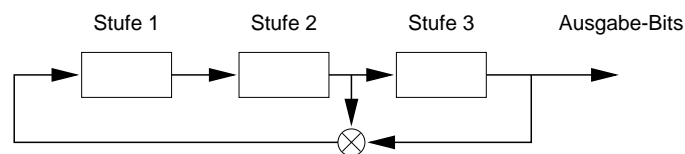


Abbildung 13: Schieberegisterschaltung

Eine weitere Methode für die Generierung einer Codesequenz liegt in der Verwendung einer Schieberegisterschaltung, um Quasi-Orthogonale Codes zu erzeugen. Ein Beispiel für eine Schieberegisterschaltung ist in Abb. 13 gegeben. Die Eingabe-Bits werden binär durch die einzelnen Stufen des Schieberegisters durchgeschoben. Der Ausgang der letzten Stufe und mindestens einer weiteren Stufe werden miteinander verknüpft und als Eingabe für die erste Stufe zurückgeführt. Die Ausgabebits an der letzten Stufe bilden den Code. Ein Code hat dabei die maximale Länge (d.h. er ist *primitiv*), falls bei  $k$  Stufen im Schieberegister er nach  $2^k - 1$  Schritten die gleiche Ausgabe produziert.

#### 4.3.3 Beschreibung der CDMA Übertragungsstrecke

Betrachten Sie nun das in Abb. 14 dargestellte CDMA Übertragungssystem.

Die auftretenden Variablen seien dabei wie folgt bezeichnet.

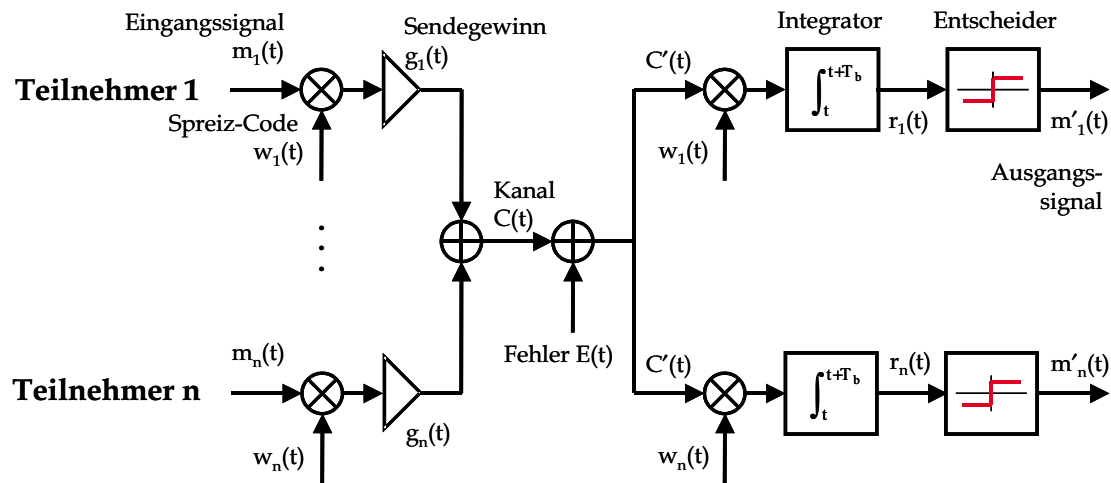


Abbildung 14: Ablauf einer CDMA Übertragung

- $t$  Zeitpunkt des  $t$ -ten Bits
- $T_b$  Dauer der Übertragung eines Bits
- $m_i(t)$  Datenbits, die von Benutzer  $i$  zum Zeitpunkt  $t$  gesendet werden
- $w_i(t)$  Walsh-Code des Benutzers  $i$
- $C(t)$  überlagertes Signal aller Teilnehmer auf dem Funkkanal
- $E(t)$  Fehler auf dem Übertragungskanal zum Zeitpunkt  $t$
- $C'(t)$  Signal am Empfänger, d.h.  $C'(t) = C(t) + E(t)$
- $g_i(t)$  Gewinn des von Teilnehmer  $i$  gesendeten Signals. Falls nicht anders angegeben, sei  $g_i(t) = 1$ .
- $r_i(t)$  Datenbits nach der Integration, d.h. es wird über alle Chips innerhalb von  $t$  und  $t + T_b$  aufsummiert.
- $m'_i(t)$  Ausgabebits nach der Entscheidung: es wird bestimmt, ob das Ausgabe-Bit eine "1" oder "-1" ist, d.h.  $m'_i(t) = \text{sgn}(r_i(t))$ .

## 4.4 Aufgaben

Die Aufgabe ist ebenfalls mit MATLAB zu bearbeiten. Zur Vorbereitung auf diese Aufgabe ist es erforderlich, sich mit der Funktionsweise von CDMA vertraut zu machen. Arbeiten Sie dazu u.a. die Literaturstellen in Ross 4 und Tanenbaum 3 durch.

1. Implementieren Sie eine MATLAB-Funktion 'walsh', die als Eingabe die Anzahl von Codes  $N$  enthält und als Ausgabe die Walsh-Hadamard Matrix  $H_N$  liefert. Beachten Sie, dass nur gerade Zahlen für  $N$  zulässig sind.

2. Betrachten Sie nun das folgende CDMA System mit 3 Teilnehmern und den (Nutz-)Bitfolgen.

$$m_1 = [+1, -1, +1]$$

$$m_2 = [+1, +1, -1]$$

$$m_3 = [-1, +1, +1]$$

Ordnen Sie jedem Teilnehmer einen Walsh-Code als Spreiz-Code zu. Geben Sie das überlagerte und gespreizte Signal  $C(t)$  für obiges Beispiel an. Wie lauten die empfangenen Bitfolgen  $m'_i(t)$ ?

3. Wie verhält sich das System, falls durch Mehrwegeausbreitung der Code des Benutzers 3 um eine Chip-Periode verschoben wird? Sind die Codes noch orthogonal? Wie kann man einen solchen Fall in der Praxis verhindern?
4. Erweitern Sie das in Teilaufgabe 2 erstellte Programm um zufällige Eingabebitfolgen. Um die Robustheit des Systems zu demonstrieren, sollen die Signale  $C(t)$  auf einem fehlerhaften Übertragungskanal verfälscht werden. Verwenden Sie dazu eine Nachrichtenlänge von 10 Bits, die (unabhängigen) Bitfehlerwahrscheinlichkeiten  $p_b = 0.01$  und  $p_b = 0.1$ . Wie ändert sich das Fehlerverhalten, wenn Sie die Codelänge auf 64 vergrößern?
5. Betrachten Sie wieder das Szenario aus Teilaufgabe 2. Verwenden Sie nun als Spreiz-Codes die Pseudo-Zufallsfolgen, die aus der Schieberegisterschaltung in Abb. 13 erzeugt wurde:

$$c_1 = [+1, -1, +1, +1, +1, -1, -1]$$

$$c_2 = [+1, -1, -1, +1, -1, +1, +1]$$

$$c_3 = [-1, +1, +1, +1, -1, -1, +1]$$

Erweitern Sie das Programm um sogenannte Sendegewinn-Komponenten. Wie verhält sich das System, wenn Benutzer 3 einen Gewinn von  $g_1 = 10$  hat, also doppelt so stark sendet wie die anderen beiden Teilnehmer? Kann ein derartiger Effekt in der Realität auftreten? Wenn ja, schlagen Sie vor, wie dies verhindert werden könnte.

## 4.5 Literatur zu Versuch 4

- [1] A.V. Oppenheim and R.W. Schaffer, *Digital Signal Processing*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1974.
- [2] Skript zur Vorlesung *Technische Informatik II*, Lehrstuhl für Informatik III, Universität Würzburg

- [3] **A.S. Tanenbaum**, *Computer Networks*, Prentice-Hall, Inc. Englewood Cliffs, NJ, 1988.
- [4] **A. Ross**, *Principles of CDMA*, [http://www.cdg.org/tech/a\\_ross/index.asp](http://www.cdg.org/tech/a_ross/index.asp)
- [5] **S.C. Yang**, *CDMA RF System Engineering*, Artech House, 1998.
- [6] **A.J. Viterbi**, *Principles of Spread Spectrum Communication*, Addison-Wesley, 1995.