

Masterarbeit

„Netzwerkmonitor für die Ortung in GSM-Netzen“

Konrad Meier
KonradMeier@gmx.de



Lehrstuhl für Kommunikationssysteme
Prof. Dr. Gerhard Schneider
Betreuer: Dr. Dirk von Suchodoletz

*Diese Arbeit wurde eingereicht als Teilleistung zur Erlangung
des Master-Grades an der Technischen Fakultät,
Albert-Ludwig-Universität Freiburg, 2010*

Erklärung

Hiermit erkläre ich, dass ich diese Abschlussarbeit selbständig verfasst habe, keine anderen als die angegebenen Quellen/Hilfsmittel verwendet habe und alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten Schriften entnommen wurden, als solche kenntlich gemacht habe. Darüber hinaus erkläre ich, dass diese Abschlussarbeit nicht, auch nicht auszugsweise, bereits für eine andere Prüfung angefertigt wurde.

Freiburg, 4. Mai 2010

Danksagung

An dieser Stelle möchte ich mich bei allen Personen bedanken, die mich während meiner Masterarbeit unterstützt haben. Dabei gilt ein besonderer Dank meinem Betreuer Dirk von Suchodoletz, der mich mit Ideen und Anregungen für meine Ausarbeitung unterstützte. Ebenso möchte ich mich bei Klaus Rechert und Dennis Wehrle bedanken, die mir bei Programmierproblemen mit Hinweisen weiterhelfen konnten. Außerdem möchte ich mich auch bei allen Korrekturleser/-innen bedanken.

Abstract

Die Analyse von Mobilfunknetzen war lange Zeit für jeden außer für Mobilfunk-Anbieter und Hersteller extrem aufwändig. Der Grund hierfür war ein Mangel an entsprechender Hard- und Software. Dieses Hindernis kann heute dank der gestiegenen Rechenleistung von Computern umgangen werden, indem Teile der Signalverarbeitung in Software abgebildet werden. In dieser Arbeit wird ein Software Defined Radio verwendet, um Daten aus dem GSM-Netz zu empfangen und auf einem angeschlossenen Computer zu visualisieren. Der Schwerpunkt der Arbeit liegt dabei auf dem Empfangen und Verarbeiten von solchen Informationen, die den aktuellen Aufenthaltsort des Empfängers charakterisieren. Im Hinblick auf Location Based Services ist eine genaue Bestimmung des Ortes sowie eine schnelle Aktualisierungsrate erstrebenswert. Hierfür wurden unterschiedliche Methoden entwickelt und hinsichtlich ihrer Effizienz verglichen. Um den Empfang von GSM-Signalen zu verbessern, wurden verschiedene Hardware-Optimierungen vorgenommen. Zur Beurteilung der Qualität der gewonnenen Daten werden diese mit den Informationen verglichen, die einem Mobilfunktelefon zugänglich sind. Die empfangenen Daten werden anschließend für Lokalisierungs-Experimente verwendet.

Inhaltsverzeichnis

1. Einleitung	1
1.1. Motivation	1
1.2. Zielsetzung	2
1.3. Aufbau der Arbeit	2
2. GSM	3
2.1. Frequenzen	3
2.2. Anbieter in Deutschland	4
2.3. Systemarchitektur	4
2.3.1. Schnittstellen	7
2.3.2. Mobilstation	7
2.3.3. BSS	8
2.3.4. NSS	9
2.4. Luftschnittstelle	10
2.4.1. Frequency Division Multiple Access, FDMA	10
2.4.2. Time Division Multiple Access, TDMA	11
2.4.3. Burst	11
2.4.4. Logische Kanäle	13
2.5. GSM-Ortung	18
2.5.1. Netzseitige Ortung	18
2.5.2. Ortung durch das Mobilfunktelefon	19
3. Hardware	20
3.1. Universal Software Radio Peripheral	20
3.1.1. Daughterboards	21
3.2. Antennen	22
3.3. Externe Taktgeber	25
3.4. Nokia 3310	27
3.4.1. Aktivierung des Netmonitors	27
3.4.2. Informationen im Netmonitor	27
4. Software	29
4.1. GNU Radio	29
4.2. Airprobe	32
4.2.1. Decodieren der Daten mit gsm-receiver	32
4.2.2. Interpretieren der Daten mit gsmdecode	33
5. GSM-Scanner	35
5.1. Aufbau des GSM-Scanners	35
5.2. Probleme mit dem gsm-receiver	36
5.3. Erste Implementierung	36
5.4. Verbesserung der Scan-Geschwindigkeit	38
5.4.1. Filterbank	38

5.4.2. Kanäle mit guter Signalstärke	40
5.5. Zweite Implementierung	42
5.5.1. Programmablauf	43
5.5.2. Benutzeroberfläche	43
5.5.3. Die empfangenen Daten	44
5.5.4. Analyse des SNR-Schwellwertes	44
5.6. Vergleich der empfangenen Daten mit dem Nokia 3310	47
6. Lokalisierung mittels GSM	51
6.1. Software	52
6.2. Erster Versuchsaufbau	54
6.3. Ergebnisse	54
6.3.1. Schlussfolgerung	57
6.4. Zweiter Versuchsaufbau	58
6.4.1. Auswertung	58
6.4.2. Ergebnisse	59
6.5. Fazit	62
7. Fazit und Ausblick	63
Literaturverzeichnis	65
Abkürzungsverzeichnis	67
Abbildungsverzeichnis	69
A. Software Installation	71
A.1. GNU Radio	71
A.2. Airprobe	72
A.3. Bluetooth GPS als serieller Port	73
A.4. gpsd	73
A.5. GSM-Scanner Installation	74
B. Ergebnisse der Lokalisierung	75
C. Beispiel-Snapshot des GSM-Scanners	76
D. Modifikationen am DBSRX-Daughterboard	77
E. EGSM900 BTS Kanäle und Frequenzen	78
F. GSM1800 BTS Kanäle und Frequenzen	79
G. CD-Inhalt	81

1. Einleitung

Im zweiten Quartal 2009 waren weltweit 4,3 Milliarden Mobilfunkanschlüsse registriert. Davon entfielen 3,45 Milliarden Anschlüsse auf den “Global System for Mobile Communications” Standard [1]. Somit ist er der am meisten verbreitete Mobilfunkstandard und bildet das größte Funknetzwerk weltweit. Das enorme Wachstum der Mobilfunknetze wird durch die zunehmende Vernetzung von Endgeräten gefördert. Geräte wie Laptops, PDAs, Navigationsgeräte und E-Book-Reader senden und empfangen Daten über Mobilfunknetze. Ursprünglich wurde das GSM-Netz für Telefonie entwickelt, erst später sind Dienste wie leitungsvermittelte sowie paketvermittelte Datendienste und Kurzmitteilungen hinzugekommen.

1.1. Motivation

Vorlesungen über Netzwerke bieten typischerweise auch praktische Demonstrationen. Dies stellt für Internet-Protokolle kaum ein Problem dar, für GSM-Netze sind solche Demonstrationen jedoch erheblich schwieriger. In der Arbeit von Bertsch [2] wurden verschiedene Methoden vorgestellt, wie GSM-Signale empfangen werden können. Dabei wird unter anderem der Netmonitor des Nokia 3310 thematisiert. Er wurde während der Entwicklung des Mobilfunktelefons verwendet, um die korrekte Funktionsweise zu verifizieren. Bei der Auslieferung der Mobilfunktelefone an die Kunden ist der Netmonitor deaktiviert, jedoch wurde er nicht entfernt und kann daher wieder aktiviert werden. Mit Hilfe des Netmonitors können Informationen über die aktuell verwendete Funkzelle ausgelesen werden. Auch die vom Mobilfunktelefon ermittelten Nachbarzellen können angezeigt werden. Die größte Einschränkung des Netmonitors ist seine Beschränkung auf lediglich einen Anbieter, der mittels der verwendeten SIM-Karte festgelegt wird.

Obwohl GSM-Netze in Deutschland schon seit 1992 in Betrieb sind, war lange Zeit die Analyse von Mobilfunknetzen aufgrund eines Mangels an entsprechender Hardware schwierig. Mobilfunktelefone wie das Nokia 3310 waren mit entsprechender Software die einzige preiswerte Möglichkeit GSM-Signale zu analysieren. Nach der Entwicklung eines universellen Software Defined Radios der Firma Ettus Research¹ und durch Open Source Projekte zur digitalen Signalverarbeitung und Analyse hat sich dies grundlegend geändert. Mit Hilfe dieser Hardware steht ein preiswertes Werkzeug zur Verfügung, das es ermöglicht, beliebige Frequenzen zu empfangen und die Signalverarbeitung in Software abzubilden. Es wird hiermit möglich, auch GSM-Signale zu empfangen und zu verarbeiten. Beispielsweise können so, anders als mit dem Nokia 3310, Informationen, die eine Zelle eindeutig identifizieren, unabhängig vom Netzanbieter empfangen werden.

Von jeder GSM-Basisstation werden Informationen gesendet, die eine eindeutige Identifizierung der Basisstation zulassen. Diese Informationen sind von Interesse, da sie einen Rückchluss auf die aktuelle Position des Mobilfunktelefons ermöglichen. Dieser Zusammenhang

¹ Ettus Research LLC, <http://www.ettus.com> [Online; letzter Aufruf 29.04.2010]

1. Einleitung

ist vor allem im Hinblick auf Location Based Services (kurz LBS) interessant. LBS sind Dienstleistungen, die in Abhängigkeit vom Aufenthaltsort eines mobilen Endgerätes bereitgestellt werden [3]. Sie haben in den vergangenen Jahren durch die wachsende Verbreitung von Smartphones stark an Bedeutung gewonnen, daher sind sie für Mobilfunkanbieter ein attraktiver Markt. Den Kunden können verschiedene Informationen zu ihren jeweils aktuellen Standorten angeboten werden [4]. Hierfür ist die aktuelle geographische Position notwendig, die meist über einen GPS-Empfänger bereitgestellt wird.

1.2. Zielsetzung

Im Rahmen dieser Arbeit soll eine Software entwickelt werden, die es ermöglicht Signale von GSM-Basisstationen in der Umgebung zu empfangen und Informationen, die die Basisstation eindeutig identifizieren, übersichtlich darzustellen. Dabei sollen die gewonnenen Informationen grafisch so aufbereitet werden, dass sie in der Lehre an der Universität verwendet werden können.

Sowohl Basisstationen im GSM900 als auch im GSM1800 Frequenzband sollen empfangen und analysiert werden. Der Fokus der Arbeit liegt darauf, den Empfang beider Frequenzbänder möglichst effizient zu gestalten.

Im Rahmen der Arbeit sollen auch Möglichkeiten evaluiert werden, wie der Empfang von GSM-Signalen durch Hardware-Verbesserungen optimiert werden kann.

Im zweiten Teil der Arbeit soll überprüft werden, ob es möglich ist, die empfangenen Informationen für eine geographische Lokalisierung zu verwenden. Dies ist von besonderem Interesse, da Mobilfunktelefone die sie umgebenden Nachbarzellen beobachten und somit einen Datensatz besitzen, der eine grobe Lokalisierung ermöglicht.

1.3. Aufbau der Arbeit

Zunächst werden in Kapitel 2 die GSM Grundlagen zum Verständnis der Arbeit präsentiert. Es werden die verschiedenen GSM-Netzwerk-Komponenten und ihre jeweiligen Funktionen erläutert. Zudem werden verschiedene GSM-Lokalisierungsverfahren vorgestellt.

Im folgenden Kapitel 3 wird die Hardware beschrieben, die für den Empfang von GSM-Signalen notwendig ist. Weiter werden in diesem Kapitel verschiedene Methoden vorgestellt, wie der Empfang von GSM-Signalen verbessert werden kann.

Anschließend werden in Kapitel 4 die Softwarekomponenten, die zur Verarbeitung der empfangenen GSM-Signale benötigt werden, beschrieben.

In Kapitel 5 wird die im Rahmen dieser Masterarbeit erstellte Anwendung zum Empfangen von GSM-Broadcast-Informationen vorgestellt. Der Schwerpunkt dieses Kapitels liegt auf der Optimierung der Zeit zum Empfangen aller GSM-Kanäle. Die Qualität und Vollständigkeit der empfangenen Informationen wird anschließend mit Hilfe des Mobilfunktelefons Nokia 3310 bewertet.

Die mit Hilfe der entwickelten Software empfangenen Informationen werden in Kapitel 6 im Hinblick auf ihre Verwendbarkeit für eine geographische Lokalisierung betrachtet. Dazu wird ein praktischer Versuchsaufbau geplant und in einem Feldexperiment umgesetzt. Die gewonnenen Erkenntnisse werden anschließend diskutiert.

Kapitel 7 fasst die Arbeit zusammen und bietet einen Ausblick über weitere interessante Aufgabenbereiche, die im Rahmen dieser Arbeit nicht betrachtet werden konnten.

2. GSM

Ende der 1950er Jahre entstanden in Europa die ersten analogen Mobilfunknetze. Die Kapazität dieser Netze war stark beschränkt und ein Roaming zwischen den Netzen verschiedener Länder wurde erst 1971, mit der Einführung des B-Netzes bedingt möglich [5]. Auch die Bedienung der ersten analogen Mobilfunknetze war nicht benutzerfreundlich. Diese Probleme sollten mit der Einführung des digitalen Mobilfunkstandards GSM beseitigt werden. In Deutschland wurden die ersten GSM-Netze 1992 in Betrieb genommen und bildeten die sogenannten D-Netze. 1994 kam das E-Netz hinzu.

GSM (“Groupe Spécial Mobile”; heute: “Global System for Mobile Communications”) ist ein Mobilfunkstandard zum Übertragen von Sprache und Daten. Er ist der am weitesten verbreitete Standard für mobile Kommunikation weltweit [1]. Im Unterschied zu den analogen Vorgängernetzen werden bei GSM Sprache und Signalisierungsdaten digital übertragen. GSM ist somit das erste rein digitale Mobilfunknetz.

Laut der GSM-Association deckt GSM 80% der Weltbevölkerung ab und kann aufgrund von Roaming-Abkommen zwischen den Anbietern in über 218 Ländern weltweit nahtlos verwendet werden [6].

2.1. Frequenzen

In Tabelle 2.1 sind die für Deutschland relevanten GSM-Frequenzbänder aufgelistet. Es gibt weitere Frequenzbänder, die für GSM im Ausland verwendet werden. Eine vollständige Übersicht aller verwendeten Frequenzen kann der GSM-Spezifikation entnommen werden [7].

Frequenzband	Uplink (MHz)	Downlink (MHz)	Kanalnummer
GSM900	890,0 – 915,0	935,0 – 960,0	1 – 124
EGSM900	880,0 – 915,0	925,0 – 960,0	0, 1 – 124, 975 – 1023
GSM1800	1710,0 – 1785,0	1805,0 – 1880,0	512 – 885

Tabelle 2.1.: Verwendete Frequenzbänder in Deutschland

Die Kommunikation zwischen Mobilfunktelefon und Mobilfunknetz erfolgt auf getrennten Frequenzen. Eine Frequenz dient der Kommunikation von Mobilfunktelefon zum Mobilfunknetz (Uplink) und eine der Rückrichtung (Downlink). Durch die getrennten Kanäle wird ein Duplexbetrieb ermöglicht.

Im EGSM900 Band beträgt die Wellenlänge 33,3 cm und im GSM1800 Band 16,7 cm. Eine hohe Wellenlänge und damit niedrige Frequenz ist für den Mobilfunkanbieter von Interesse, da die Dämpfung der Funksignale durch Hindernisse mit höherer Frequenz steigt. Limitiert durch die Laufzeit der Signale sind Zellen mit einem Durchmesser von 35 km möglich. Im GSM1800 Frequenzband ist die Zellgröße durch die geringeren Sendeleistungen von Mobilfunktelefon und Mobilfunkzelle jedoch beschränkt. In Tabelle 2.2 sind die maximalen Sendeleistungen im EGSM900 und GSM1800 Frequenzband aufgelistet. Die maximale Sendeleistung der Mobilfunktelefone, die am Körper getragen werden, ist bei EGSM900 beschränkt auf 2 W [8].

Gerade im städtischen Bereich sind die Zellen jedoch oftmals wesentlich kleiner als theoretisch möglich. Dies ist notwendig, da eine Funkzelle nur mit einer begrenzten Anzahl von

2. GSM

Teilnehmern gleichzeitig kommunizieren kann und die Anzahl der Teilnehmer in einer Stadt wesentlich höher ist als in ländlichen Gebieten.

Frequenzband	Sendeleistung Mobilfunktelefon	Sendeleistung Mobilfunkzelle
GSM900	max. 2 W (8 W)	max. 640 W
GSM1800	max. 1 W	max. 40 W

Tabelle 2.2.: Maximale Sendeleistungen (Quelle: [9])

Zur Erhöhung der Kapazität sind die Frequenzbänder in 200 kHz breite Kanäle unterteilt. Jeder Kanal hat eine eindeutige Kanalnummer, die “Absolute Radio Frequency Channel Number”, kurz ARFCN. Die entsprechenden Kanalnummern können der Tabelle 2.1 entnommen werden. Das Frequenzband GSM900 war das erste verwendete Frequenzband in Deutschland und wird von Vodafone (ehemals D2 Mannesmann Mobilfunk) und T-Mobile (ehemals D1 Deutsche Telekom Mobilfunk) verwendet. Im GSM1800 Frequenzband startete 1994 das Mobilfunkangebot von E-Plus. 1998 ist das Mobilfunknetz von O₂ im GSM1800 Band hinzugekommen. Das Frequenzband GSM900 wurde im Jahr 2005 um 10 MHz erweitert und wird als EGSM900 bezeichnet. Die neuen Frequenzen wurden an E-Plus und O₂ vergeben, da diesen Anbietern bisher nur Frequenzen im GSM1800 Band zur Verfügung standen. Die Kanalnummern von GSM900 sind in EGSM900 enthalten, da das EGSM900 Band eine Erweiterung des GSM900 Bandes ist.

Die Vergabe der Frequenzen wird in Deutschland durch die Bundesnetzagentur¹ reguliert.

2.2. Anbieter in Deutschland

In Deutschland gibt es insgesamt vier Netzbetreiber. Diese sind in Tabelle 2.3 zusammen mit den zugewiesenen Kanälen aufgelistet.

Betreiber	Kanalzuweisung EGSM900	Kanalzuweisung GSM1800
T-Mobile	13-49, 81-102, 122-124 (62 Kanäle)	587-611 (25 Kanäle)
Vodafone	1-12, 50-80, 103-121 (62 Kanäle)	725-751 (27 Kanäle)
E-Plus	975-999 (25 Kanäle)	777-863 (87 Kanäle)
O ₂	0, 1000-1023 (25 Kanäle)	637-723 (87 Kanäle)

Tabelle 2.3.: Mobilfunkanbieter in Deutschland mit den ihnen zugewiesenen Kanälen

Den Netzanbietern T-Mobile und Vodafone sind jeweils 62 Kanäle im GSM900 Band zugewiesen. Im GSM1800 Band hat T-Mobile 25 und Vodafone 27 Kanäle. Bei E-Plus und O₂ ist es invers. Ihnen stehen im EGSM900 Band 25 Kanäle und dafür im GSM1800 Band jeweils 87 Kanäle zur Verfügung.

2.3. Systemarchitektur

Der Aufbau eines Mobilfunknetzwerkes besteht aus einer vielzahl an Komponenten. Das Mobilfunknetzwerk und das Mobilfunktelefon als Endgerät sind die für den Teilnehmer sichtbaren Bestandteile. Das Mobilfunknetzwerk wird von den Mobilfunkanbietern betrieben und unterteilt sich, wie in Abbildung 2.1 dargestellt, in zwei Bereiche, das Basestation Subsystem (BSS)

¹ Bundesnetzagentur, <http://www.bundesnetzagentur.de> [Online; letzter Aufruf 10.03.2010]

und das Network Subsystem (NSS).

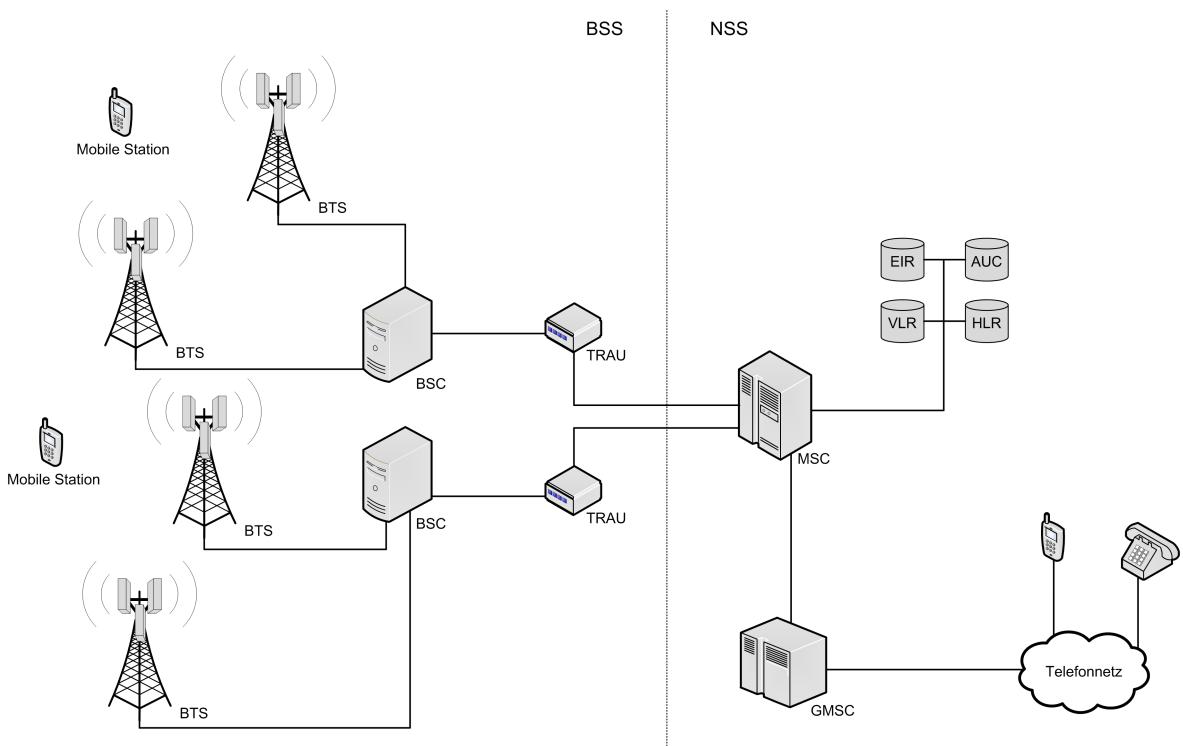


Abbildung 2.1.: Überblick über die Systemkomponenten

Das BSS besteht aus den folgenden Komponenten:

- BTS – Base Transceiver Station
- BSC – Base Station Controller
- TRAU – Transcoder Rate Adaptation Unit

Das NSS besteht aus den folgenden Komponenten:

- MSC – Mobile Switching Center
- GMSC – Gateway Mobile Switching Center
- Datenbanken
 - HLR – Home Location Register
 - VLR – Visitor Location Register
 - AUC – Authentication Center
 - EIR – Equipment Identity Register

Die Komponenten des BSS werden in Kapitel 2.3.3 genauer beschrieben. Auf die Komponenten des NSS wird in Kapitel 2.3.4 eingegangen.

Geographisch ist das GSM-Mobilfunknetz in Zellen aufgeteilt. Jede Funkzelle übernimmt die Versorgung einer bestimmten Region. Als Funkzelle wird der räumliche Versorgungsbereich

2. GSM

einer BTS bezeichnet. Um Interferenzen mit Nachbarzellen zu vermeiden, werden in benachbarten Funkzellen unterschiedliche Frequenzen verwendet.

Die Komponenten des Mobilfunknetzwerkes sind hierarchisch gegliedert. Am unteren Ende steht das Mobilfunktelefon, das über eine Funkverbindung mit der nächstgelegenen BTS in Verbindung steht. Die BTS werden gebietsweise zusammengefasst und dem BSC unterstellt. Mehrere BSC sind schließlich mit dem MSC verbunden.

Die hierarchische Gliederung des Mobilfunknetzes spiegelt sich auch in den Parametern wieder, die eine Funkzelle eindeutig identifizieren:

- MCC – Mobile Country Code:

Der MCC ist ein Ländercode, der ein Mobilfunknetz einem Land eindeutig zuordnet.

Die erste Ziffer gibt eine grobe geographische Zuordnung:

- 2** – Europa
- 3** – Nordamerika und Karibik
- 4** – Asien, Indien, naher Osten
- 5** – Australien und Ozeanien
- 6** – Afrika
- 7** – Südamerika
- 9** – Welt

Die beiden folgenden Zahlen identifizieren das Land eindeutig. Deutschland hat den MCC 262.

- MNC – Mobile Network Code:

Der MNC ist eine eindeutige Kennung für den Anbieter des Mobilfunknetzwerkes. Die Kennung wird in Deutschland von der Bundesnetzagentur zugewiesen. Folgende Kennungen sind im Rahmen dieser Arbeit von Bedeutung:

- 01** – T-Mobile
- 02** – Vodafone
- 03** – E-Plus
- 07** – O₂

- LAC – Location Area Code:

Eine Location Area (LA) besteht aus einer flexiblen Anzahl von BTS, die vom gleichen BSC gesteuert werden. Solange sich ein Mobilfunktelefon im Standby-Modus befindet, ist die Location Area die einzige Information über den Aufenthaltsort des Mobilfunktelefons, die dem Netzwerk bekannt ist. Bewegt sich ein Mobilfunkteilnehmer in eine andere LA, muss das Mobilfunktelefon dies dem Mobilfunknetzwerk über ein "Location Update" mitteilen. Das ist notwendig, da sonst das Mobilfunknetzwerk nicht in der Lage ist, das Mobilfunktelefon bei einem eingehenden Gespräch zu finden. (GSM Spezifikation 03.22 Kapitel 2 [10])

- Cell-ID – Cell Identifier:

Die Cell-ID ist eine eindeutige Kennung für eine BTS.

Beispiel für die Verwendung der hierarchischen Kennungen:

MCC: 262 = Deutschland
MNC: 03 = E-Plus
LAC: 588 = Freiburg im Breisgau
Cell-ID: 55238

(BTS wurde in der Stefan-Meier-Straße 10; 79104 Freiburg empfangen)

Theoretisch versorgt genau eine Funkzelle einen bestimmten geographischen Raum. Dieser ist durch die Sendeleistung der Funkzelle beschränkt und wird als Versorgungsgebiet der Funkzelle bezeichnet. In der Theorie wird der zu versorgende Raum in Hexagone aufgeteilt. Praktisch hängt jedoch die Reichweite und somit das Versorgungsgebiet einer Funkzelle von unterschiedlichen Faktoren ab. Vor allem die Dämpfung der Funksignale durch Hindernisse wie Gebäude, Bäume und Berge reduziert das Versorgungsgebiet deutlich. Die Zellgröße ist auch von der Anzahl zu versorgender Teilnehmer in einer Region abhängig. Dies führt dazu, dass besonders in Städten mehrere Funkzellen ein Versorgungsgebiet abdecken.

2.3.1. Schnittstellen

Die Schnittstellen der Systemkomponenten sind in Tabelle 2.4 aufgelistet. Für diese Arbeit ist die U_m Schnittstelle zwischen MS und BTS von Bedeutung, da auf dieser die BTS die Informationen MCC, MNC, LAC und Cell-ID sendet. Die U_m Schnittstelle wird in Kapitel 2.4 genauer betrachtet.

Zwischen		Schnittstelle
MS	BTS	U_m
BTS	BSC	A_{bis}
BSC	TRAU	A_{ter}
TRAU	MSC	A
GMSC	Telefonnetz	N
MSC	MSC	E
MSC	EIR	F
MSC	HLR	C
MSC	VLR	B

Tabelle 2.4.: Schnittstellen zwischen den Systemkomponenten

2.3.2. Mobilstation

Die Mobilstation (kurz MS) stellt die Schnittstelle zwischen dem Teilnehmer und dem Mobilfunknetz dar und besteht aus einem Mobilfunktelefon und einer SIM-Karte (Abbildung 2.2).

Das Mobilfunktelefon ist für die korrekte Kommunikation mit dem Mobilfunknetz verantwortlich. Die SIM-Karte dient zur Authentifizierung des Mobilfunkteilnehmers gegenüber dem Mobilfunknetz. Das Mobilfunktelefon hat eine beschränkte Sendeleistung von maximal 2 W im GSM900 Band und 1 W im GSM1800 Band. Da es in Deutschland zwei Frequenzbereiche gibt, unterstützen die in Deutschland verkäuflichen Mobilfunktelefone mindestens die Frequenzbänder EGSM900 und GSM1800. Diese Mobilfunktelefone werden als Dualband-Geräte



Abbildung 2.2.: Mobilstation aus Nokia 3310 und T-Mobile SIM-Karte

bezeichnet. Es gibt auch Triband- und Quadband-Geräte, die darüber hinaus die Frequenzbänder GSM850 und GSM1900 unterstützen. Eine Unterstützung dieser Frequenzen ist dann von Vorteil, wenn der Teilnehmer Deutschland verlässt.

Das Mobilfunktelefon ist mit einer eindeutigen 15-stelligen Seriennummer, der IMEI versehen. Theoretisch kann die IMEI verwendet werden, um das Gerät im Falle eines Diebstahls zu sperren. Praktisch wird dies nicht von allen Netzbetreibern unterstützt [11], da die IMEI bei vielen Geräten mit entsprechender Software geändert werden kann [12].

Zur eindeutigen Identifizierung des Teilnehmers wird vom Mobilfunkanbieter eine sogenannte IMSI generiert und auf der SIM-Karte gespeichert. Die ersten drei Ziffern der IMSI sind der MCC und geben somit das Land an, in dem die SIM-Karte herausgegeben wurde. Die folgenden zwei bzw. drei Ziffern stehen für den Anbieter und werden von 9-10 Ziffern gefolgt, die eine eindeutige Kennung des Teilnehmers darstellen. Die IMSI kann somit maximal 15 Ziffern lang sein.

2.3.3. BSS

Das BSS beinhaltet alle Komponenten, die für die Steuerung der Funkmasten notwendig sind. Dieser Teil übernimmt auf der U_m Schnittstelle die Kommunikation mit der Mobilstation.

Base Transceiver Station – BTS

Eine Base Transceiver Station, stellt die Luftschnittstelle zur MS bereit und ist mit einem Transceiver zum Senden und Empfangen ausgestattet. Eine BTS besteht aus mindestens einer Funkzelle. Es gibt jedoch auch BTS, die 3, 4 oder 6 Funkzellen bereitstellen. Diese werden mit Sektorantennen realisiert, die einen Abstrahlwinkel von 120° , 90° oder 60° besitzen. Eine Zelle kann mit mehr als einer Frequenz arbeiten, um die Kapazität der Zelle zu erhöhen. Aufgaben einer BTS sind:

- Modulation und Demodulation der Signale
- Aufbau des Broadcast Control Channels (BCCH) (siehe Kapitel 2.4.4)
- Frequenzhopping zwischen den Frequenzen der Zelle
- Verschlüsseln und Entschlüsseln von übertragenen Daten
- Bestimmung der Signalstärke und Qualität von MS Signalen
- Bestimmung und Übertragung des Timing Advanced Parameter
- Bereitstellung des Frequency Correction Bursts im FCCH (siehe Kapitel 2.4.4)

- Signalanpassung an die PCM-Schnittstelle²

Base Station Controller – BSC

Ein Base Station Controller ist über eine TRAU an das NSS angebunden. Die TRAU (Transcoder and Rate Adaptation Unit) ist für die Sprachkompression zuständig.

Aufgaben eines BSC:

- Steuerung mehrerer BTS
- Verwaltung der freien Zeitschlüsse der angeschlossenen BTS
- Aufrechterhaltung der Verbindungen
- Kontrolle des Handovers

Die Verwaltung der Ressourcen einer BTS übernimmt der BSC. Dafür muss er wissen, welche Zeitschlüsse aktuell frei sind und welche durch aktive Übertragungen belegt sind. Aufgrund dieser Informationen kann der BSC entscheiden, welche Kanäle beim Rufaufbau zur Verfügung stehen und wie diese zugeteilt werden. Deshalb kann auch nur der BSC entscheiden, ob ein Handover sinnvoll und möglich ist.

2.3.4. NSS

Das Network Subsystem ist die Vermittlungszentrale des GSM Netzwerkes. Es übernimmt die Aufgabe, Gespräche und Daten zwischen verschiedenen Netzwerken zu vermitteln. Gleichzeitig wird mit dem NSS die Authentifizierung der Teilnehmer ermöglicht. Das Network Subsystem besteht aus den folgenden Komponenten:

Mobile Switching Center – MSC

Das Mobile Switching Center ist eine Vermittlungszentrale des Mobilfunknetzwerkes. Die Aufgabe besteht in der Vermittlung von Verbindungen zwischen geographisch beweglichen Teilnehmern. Ein MSC ist über mehrere TRAUs an die BSCs angeschlossen. Die Verbindung in andere Netzwerkabschnitte erfolgt über andere MSCs oder über das GMSC in die Netze anderer Anbieter. Für die Verwaltung der Teilnehmer sind die MSCs mit den Datenbanksystemen EIR, AUC, VLR und HLR verbunden.

Gateway MSC – GMSC

Das GMSC übernimmt die Funktion einer MSC. Zusätzlich vermittelt es zwischen dem eigenen Mobilfunknetzwerk und den Telefonnetzwerken anderer Anbieter.

Datenbanken

- Equipment Identity Register – EIR

Die EIR ist eine optionale Datenbank. Beim Anmelden eines Mobilfunktelefones an das Netzwerk wird diese Datenbank verwendet, um zu überprüfen, ob das Mobilfunktelefon als gestohlen gemeldet wurde.

²PCM = Puls-Code-Modulation beschreibt ein Pulsmodulationsverfahren, das ein zeit- und wertkontinuierliches analoges Signal in ein zeit- und wertdiskretes digitales Signal umwandelt.

- Authentication Center – AUC

Das AUC ist für die Authentifizierung des Teilnehmers zuständig. Des Weiteren werden durch das AUC die benötigten Schlüssel für die Verschlüsselung der Verkehrsdaten auf der Luftschnittstelle bereitgestellt.

- Visitor Location Register – VLR

Das VLR speichert temporär Daten der Teilnehmer und bildet mit einer MSC eine Einheit. In dem VLR werden die Daten der Teilnehmer zwischengespeichert, die sich im Verantwortungsbereich der MSC befinden und entlasten somit das HLR. Die Daten werden u.a. für die Mobilitätsverwaltung und für Sicherheitsfunktionen benötigt.

- Home Location Register – HLR

Das HLR speichert die Daten aller Teilnehmer eines Mobilfunkanbieters. Im HLR werden die folgenden Daten gespeichert:

- eindeutige Kennung der SIM-Karte (IMSI)
- Teilnehmerrufnummer (MSISDN)
- momentaner Aufenthaltsort durch den Location Area Code
- Abrechnungsdaten

2.4. Luftschnittstelle

Die Luftschnittstelle bezeichnet die Schnittstelle zwischen MS und BTS und wird auch als U_m bezeichnet. Sie ermöglicht die Kommunikation der MS mit dem Mobilfunknetzwerk und wird von der BTS bereitgestellt. Für die Übertragung von Daten wird eine Kombination aus Frequenz- und Zeitmultiplexing verwendet. Die Kombination beider Verfahren ermöglicht es, eine große Anzahl von Teilnehmern gleichzeitig zu versorgen.

2.4.1. Frequency Division Multiple Access, FDMA

Das Ziel dieses Verfahren ist es, parallele Übertragungen zu ermöglichen. Um dieses Ziel zu erreichen, wird das zur Verfügung stehende Frequenzspektrum in 200 kHz breite Kanäle aufgeteilt. Für das 25 MHz breite GSM900 Frequenzband ergeben sich 124 Kanäle³. Jeder Kanal erhält eine eindeutige Kanalnummer, die ARFCN. In Abbildung 2.3 ist das Frequenzmultiplexing anhand des GSM900 Bandes dargestellt. Um den Duplexbetrieb zu ermöglichen, werden für den Up- und Downlink zwei getrennte Frequenzen verwendet. Im EGSM900 Frequenzband beträgt der Abstand zwischen Uplink- und Downlink-Kanal 45 MHz und im GSM1800-Frequenzband 95 MHz.

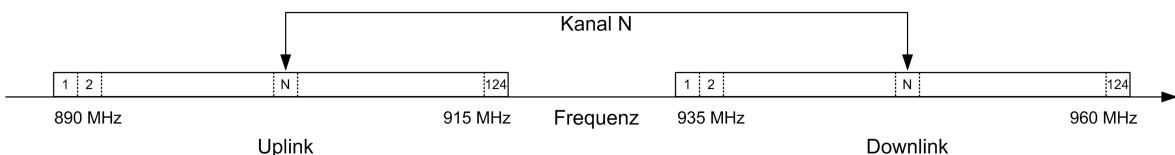


Abbildung 2.3.: Frequenzmultiplexing im GSM900 Band

Nur durch das FDMA könnten im GSM900 Band insgesamt 124 Übertragungen gleichzeitig stattfinden. Dies ist für den Regelbetrieb zu wenig. Aus diesem Grund wird das FDMA mit Zeitmultiplexing kombiniert.

³ $25 \text{ MHz} / 0,2 \text{ MHz} = 125$ Kanäle; Kanal 0 wird bei GSM900 jedoch nicht verwendet.

2.4.2. Time Division Multiple Access, TDMA

Um die Kapazität einer Mobilfunkzelle zu erhöhen, wird jeder Kanal in acht Zeitschlitzte unterteilt. Jeder Zeitschlitz ist $576,6 \mu\text{s}$ lang. Alle acht Zeitschlitzte zusammen bilden einen TDMA-Rahmen der Länge 4,615 ms. Jeder Teilnehmer sendet innerhalb genau eines Zeitschlitzes und stört daher die Kommunikation der anderen Teilnehmer nicht. Die Kapazität der Mobilfunkzelle erhöht sich somit theoretisch um den Faktor 8. In der Praxis wird mindestens ein Zeitschlitz für Signalisierungsdaten verwendet und kann nicht als Datenkanal genutzt werden.

Um dem Mobilfunktelefon das Senden und Empfangen mit einer Antenne zu ermöglichen, sind die Zeitschlitzte im Downlink und Uplink um drei Zeitschlitzte verschoben. In Abbildung 2.4 sind die Zeitschlitzte im Downlink und Uplink mit der erforderlichen Verzögerung (Delay) graphisch dargestellt.

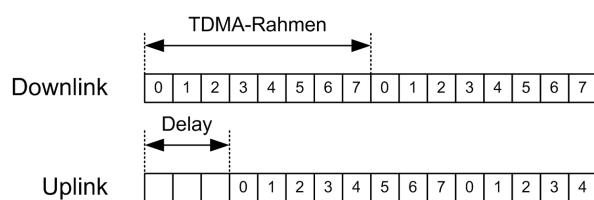


Abbildung 2.4.: Kommunikation in Zeitschlitzten

Die Grafik 2.5 zeigt die Kombination von FDMA und TDMA am Beispiel GSM900. Auf der X-Achse ist FDMA und auf der Y-Achse TDMA aufgetragen.

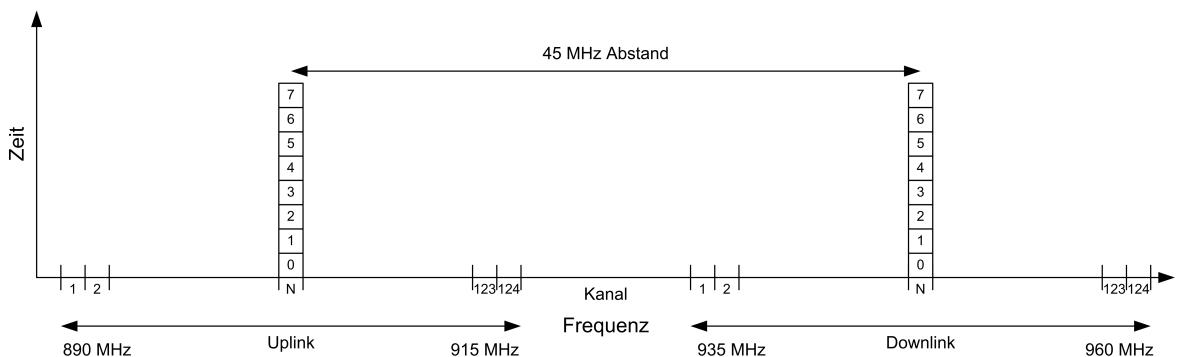


Abbildung 2.5.: Frequenzmultiplexing und Zeitmultiplexing im GSM900 Band

2.4.3. Burst

Für die Übertragung von Daten werden Bursts verwendet. Jeder Zeitschlitz enthält einen Burst mit einer Dauer von $576,6 \mu\text{s}$. In Abbildung 2.6 ist die Struktur der verschiedenen Bursts dargestellt. Es gibt insgesamt fünf unterschiedliche Bursts. Jeder Burst besitzt eine Schutzzeit die bei leichten Überschneidungen der Bursts verhindert, dass die Daten eines Bursts unbrauchbar werden. Leichte Überschneidungen können durch Timingprobleme auftreten.

Im Downlink (BTS zu MS) werden die folgenden Bursts verwendet: Normal Burst, Frequency Correction Burst, Synchronization Burst, Dummy Burst. Im Uplink (MS zu BTS): Normal Burst und Access Burst.

- Normal Burst

Der Normal Burst wird zum Übertragen von Nutzdaten wie Sprache oder Paketdaten,

2. GSM

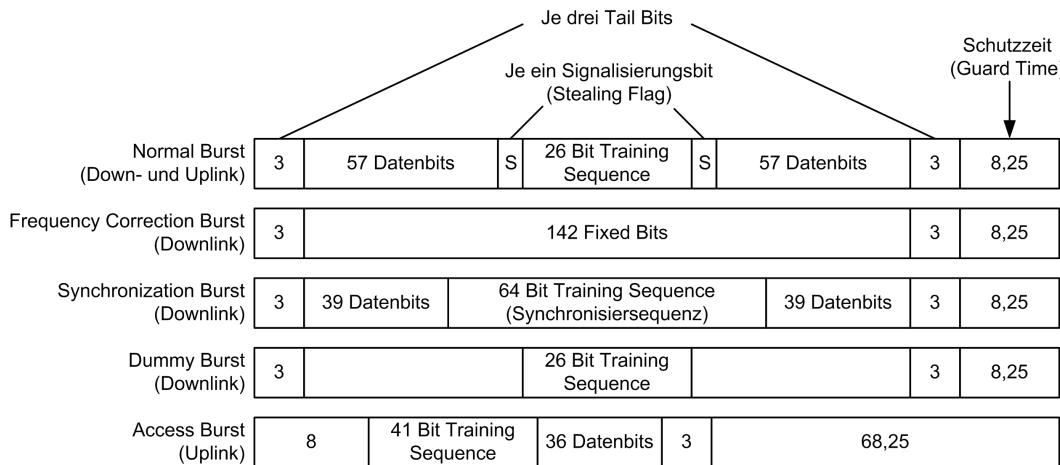


Abbildung 2.6.: Von GSM-TDMA verwendete Bursts (Vorlage nach [13])

sowie Signalisierungsdaten verwendet. Jeder Burst beginnt und endet mit drei "Tail Bits" die immer auf 0 gesetzt sind. Die Tail Bits sind für die Transmitter-Hardware und die Demodulierung der Daten notwendig. Die Signalisierungsbits vor jedem Datenblock geben an, ob der folgende Datenblock Signalisierungs- oder Nutzdaten enthält. Die Bits werden verwendet, um Datenblöcke für dringende Signalisierungsinformationen zu übernehmen. Die "Trainings Sequence" in der Mitte des Bursts enthält ein vordefinierteres Bitmuster um die Intersymbolinterferenz⁴ zu reduzieren. Die Intersymbolinterferenz tritt durch Laufunterschiede bei der Mehrwegausbreitung auf.

- **Frequency Correction Burst**

Dieser Burst wird von der BTS ausgestrahlt, um der MS eine Zeit- und Frequenzsynchro-nisation zu ermöglichen. Dieser Burst ist notwendig, um die Abweichung des internen Oszillators der MS zu korrigieren. Ohne diesen Burst wäre die Abweichung des Oszil-lators zu groß und eine Kommunikation nicht möglich, da es zu Überschneidungen der Bursts auf der Luftschnittstelle kommen würde. Das wiederholte Senden eines Fre-quency Correction Bursts wird als "Frequency Correction Channel" bezeichnet (siehe Kapitel 2.4.4).

- **Synchronization Burst**

Dieser Burst dient zur groben Synchronisation der MS zur BTS. Wird der Synchronisa-tion Burst wiederholt ausgestrahlt, wird dies als "Synchronization Channel" bezeichnet (siehe Kapitel 2.4.4).

- **Dummy Burst**

Dieser Burst wird von der BTS ausgesendet, wenn kein anderer Burst gesendet wird. Dies ermöglicht es der MS, die Signalstärke der BTS auch dann zu bestimmen, wenn keine Daten gesendet werden. Die MS ist somit in der Lage die Signalstärken von un-terschiedlichen BTS zu beobachten und die BTS mit der besten Signalstärke für eine Übertragung zu verwenden.

- **Access Burst**

Dieser Burst dient der Verbindungsaufnahme einer MS mit der BTS. Er wird benötigt damit die MS einen dedizierten Kanal für eine Kommunikation anfordern kann. Der Access Burst wird auf dem "Random Access Channel" (siehe Kapitel 2.4.4) gesendet und

⁴ Die Intersymbolinterferenz beschreibt Störungen zwischen zeitlich aufeinanderfolgenden Sendesymbolen.

ermöglicht einen wahlfreien Vielfachzugriff durch die MS. Durch den wahlfreien Vielfachzugriff kann es zu Kollisionen kommen. Um die Wahrscheinlichkeit einer Kollision zu verringern, ist die Schutzzeit beim Access Burst wesentlich länger.

2.4.4. Logische Kanäle

Aus einer Reihe von Zeitschlitten werden logische Kanäle gebildet, die zur Datenübertragung verwendet werden. Die logischen Kanäle haben folgende Aufgaben: Nutzdatenübertragung, Signalisierung, Broadcast für allgemeine Systeminformationen und Synchronisation. Die logischen Kanäle sind in Verkehrskanäle und Signalisierungskanäle unterteilt und werden nach einem vorgegebenen Muster in den acht physikalischen Zeitschlitten transportiert.

Traffic Channels

Der "Traffic Channel" (TCH) wird verwendet um Sprach- oder Paketdaten zu transportieren. Er enthält keinerlei Signalisierungsinformationen. Ein TCH kann entweder vollständig verwendet (Full-Rate TCH) oder halbiert werden (Half-Rate TCH). Bei einem Half-Rate TCH teilen sich zwei Teilnehmer einen TCH, wodurch sich die Bandbreite für jeden Teilnehmer halbiert. Die Abbildung dieses geteilten TCH auf physikalische Bursts erfolgt abwechselnd. Zum Zeitpunkt n überträgt Teilnehmer 1 die Daten seines TCH auf einem Burst. Dabei werden beide 57 Bit Blöcke im Burst benutzt. Im nächsten Burst ($n+1$) überträgt Teilnehmer 2 die Daten seines TCH. Durch half-rate TCH kann somit die Anzahl der versorgbaren Teilnehmer auf Kosten der Gesprächsqualität oder der Datenrate erhöht werden.

Signalisierungskanäle

Die Signalisierungskanäle sind unterteilt in "Broadcast Channel", "Common Control Channel" und "Dedicated Control Channel".

Broadcast Channel – BCH:

Der Broadcast Control Channel ist ein Punkt-zu-Multipunkt-Kanal. Er ist in die folgenden Kanäle unterteilt:

- Broadcast Control Channel – BCCH:
Auf diesem Kanal sendet die BTS Informationen über die Zelle. Es wird die Kanalkonfiguration und eine Liste von Nachbarzellen, Synchronisation und Registrierungsinformationen übertragen. In diesem Kanal werden die für diese Arbeit interessanten Informationen MCC, MNC, LAC und Cell-ID übertragen.
- Frequency Correction Channel – FCCH:
Hier werden der MS Informationen zur Frequenzkorrektur des internen Oszillators bereitgestellt.
- Synchronization Channel – SCH:
Dieser Kanal enthält Informationen zum aktuellen TDMA-Rahmen sowie die Cell-ID und dient der MS zur Rahmensynchronisation.

Common Control Channel – CCCH:

Der CCCH ist ein Punkt-zu-Multipunkt-Kanal. Über diesen Kanal werden der MS Daten-Kanäle zugewiesen. Auch das Paging einer MS wird über diesen Kanal vorgenommen. Der CCCH ist unterteilt in die folgenden Kanäle:

2. GSM

- Random Access Channel – RACH:

Der RACH ist der einzige logische Uplink-Kanal auf dem ausschließlich Daten von der MS zur BTS übertragen werden. Er wird von der MS verwendet, um einen Kanal zur Datenübertragung anzufordern. Der Zugriff auf diesen Kanal erfolgt nach dem Slotted Aloha Verfahren. Durch dieses Verfahren kann es auf diesem Kanal zu Kollisionen durch zeitgleiche Anfragen verschiedener MS kommen.

- Access Grant Channel – AGCH:

Dieser Kanal wird verwendet, um einer MS bei erfolgreicher RACH-Anfrage einen SD-CCH oder TCH Kanal zuzuweisen.

- Paging Channel – PCH:

Der PCH ist ein Downlink-Kanal. Er wird bei eingehenden Daten oder Gesprächen für eine MS verwendet, um die Zelle zu finden, in der sich diese gerade befindet. Dies ist notwendig, da von einer MS im Standby-Modus nur der "Location Area Code" bekannt ist und nicht die aktuelle Zelle.

- Notification Channel – NCH:

Der NCH wird verwendet, um die MS über eingehende Gruppen- oder Broadcast-Anrufe zu informieren.

Dedicated Control Channel - DCCH:

Der DCCH ist ein bidirekionaler Punkt-zu-Punkt-Signalisierungskanal.

- Stand-alone Dedicated Control Channel – SDCCH

Der SDCCH wird von der MS über den RACH angefordert und über den AGCH zugewiesen. Er wird für Signalisierung wie Gesprächsaufbau, Location Updates und Senden / Empfangen von SMS, sowohl während eines aktiven TCH, als auch ohne aktiven TCH verwendet.

- Slow Associated Control Channel – SACCH

Der SACCH wird zusammen mit einem TCH oder SDCCH zugewiesen. Er wird verwendet, um Informationen über die empfangene Signalstärke und Synchronisation während einer aktiven Verbindung zu übertragen. Auf diesem Kanal müssen kontinuierlich Daten übertragen werden, da sonst von einem Abbruch der Verbindung ausgegangen wird.

- Fast Associated Control Channel – FACCH

Der FACCH wird verwendet, wenn unverzüglich längere Signalisierungsinformationen während einem aktiven TCH ausgetauscht werden müssen. Dieser Kanal wird beispielsweise für die Signalisierung bei einem Handover verwendet. Der FACCH wird über die "Stealing Flags" im Burst angekündigt und belegt die Datenbits im folgenden Datenblock.

In Tabelle 2.5 ist eine Übersicht über die Gruppierung der logischen Kanäle gegeben. Der Tabelle kann auch die Kommunikationsrichtung des jeweiligen Kanals entnommen werden.

Die logischen Kanäle werden nach vorgegebenen Mustern auf die physikalischen Kanäle abgebildet und können nicht beliebig kombiniert werden. In Tabelle 2.6 sind die durch die Spezifikation vorgegebenen Kanalkombinationen für eine BTS zu sehen. Die Kanalkombinationen für die MS sind in Tabelle 2.7 aufgelistet.

Bezeichnung	Kanal	Funktion	Richtung
Traffic Channel	TCH	TCH/F TCH/H	Full-Rate TCH Halfrate TCH
Signalizing Channels	BCH	BCCH FCCH SCH	Broadcast Control Frequency Correction Synchronization
	CCCH	RACH AGCH PCH NCH	Random Access Access Grant Paging Notification
	DCCH	SDCCH SACCH FACCH	Stand-alone Dedicated Control Slow Associated Control Fast Associated Control

Tabelle 2.5.: Übersicht und Klassifizierung der logischen Kanäle (Vorlage nach [13])

	B1	B2	B3	B4	B5	B6	B7	B8
TCH/F	×							×
TCH/H		×	×					
TCH/H			×					
BCCH				×	×	×		
FCCH				×	×			
SCH				×	×			
CCCH				×	×	×		
SDCCH					×		×	
SACCH	×	×	×		×		×	×
FACCH	×	×	×					

Tabelle 2.6.: Von der BTS bereitgestellte Kanalkombinationen (Vorlage nach [13])

	M1	M2	M3	M4	M5	M6	M7
TCH/F					×		
TCH/H						×	×
TCH/H							×
BCCH	×		×				
CCCH		×	×				
SDCCH				×			
SACCH				×	×	×	×
FACCH					×	×	×

Tabelle 2.7.: Von der MS verwendete Kanalkombinationen (Vorlage nach [13])

Abbildung der logischen Kanäle auf physikalische Kanäle

Üblicherweise werden die Zeitschlitz 0 und 1 für Signalisierungsdaten verwendet. Bedingt durch die Vielzahl der Signalisierungskanäle, reichen jedoch die Zeitschlitz 0 und 1 nicht aus, um alle Signalisierungskanäle zu übertragen. Aus diesem Grund werden mehrere TDMA-Rahmen in einem Multirahmen zusammengefasst. Dabei kommen zwei unterschiedlich lange Multirahmen zum Einsatz, einer mit 26 TDMA-Rahmen, der andere mit 51 TDMA-Rahmen. Multirahmen erlauben es, logische Kanäle in physikalische Kanäle abzubilden. Der 26er TDMA-Rahmen bildet die logischen Verkehrskanäle FCH und die ihnen zugeordneten Steuerungskanäle SACCH und FACCH auf einen physikalischen Kanal ab. Dabei werden 26 TDMA-Rahmen hintereinander gehängt. Diese haben folglich eine Länge von $8 * (15/26) ms * 26 = 120 ms$. Im 51er-Multirahmen werden die Daten der Signalisierungskanäle mit Ausnahme der Associated Control Channels (SACCH, FACCH) übertragen. Der 51er Multirahmen besteht aus 51 TDMA-Rahmen und hat eine Länge von $8 * (15/26) ms * 51 = 3060/13 ms$. Mehrere Multirahmen bilden einen Superrahmen der Länge 6,12 s. Mehrere Superrahmen werden anschließend zu einem Hyperrahmen zusammengefasst. Dieser hat eine ungefähre Länge von 3,5 Stunden.

Eine Übersicht über die Hierarchie der einzelnen Rahmen ist in Abbildung 2.7 gegeben. Der Grafik ist auch die Dauer des jeweiligen Rahmens zu entnehmen.

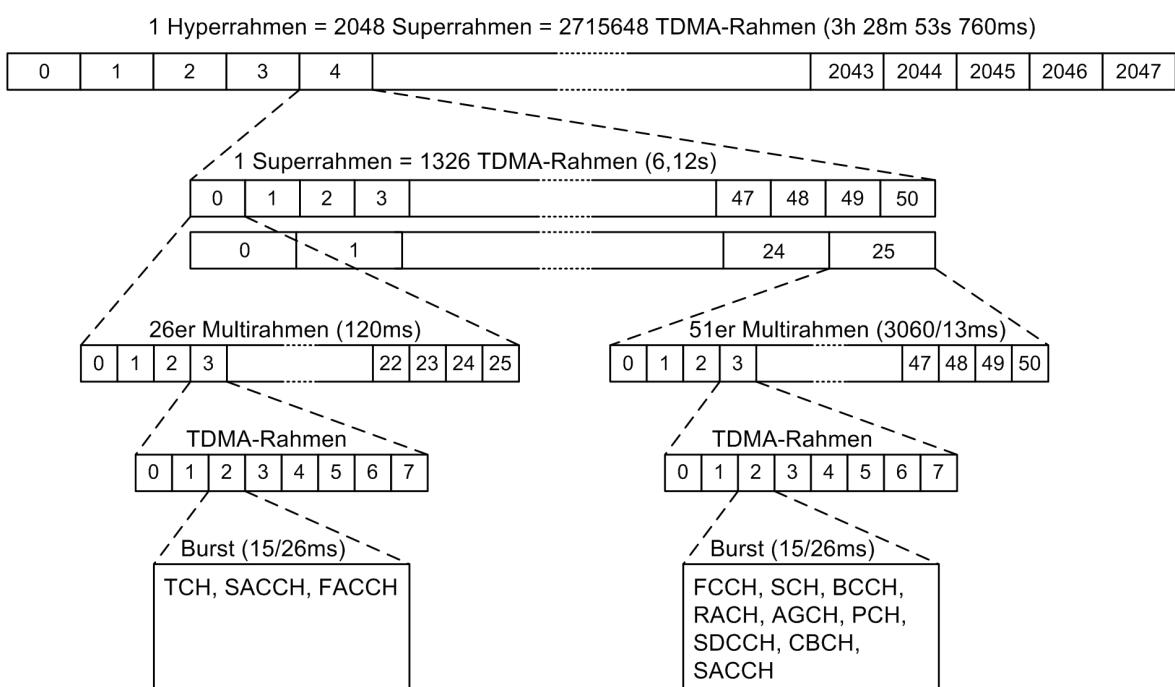


Abbildung 2.7.: Von GSM-TDMA verwendete Bursts

Abbildung 2.8 zeigt beispielhaft die Zuordnung der logischen Kanäle zu den physikalischen Kanälen. Auf Zeitschlitz 0 wird ein 51er Multirahmen mit der Konfiguration B5 (BCCH + FCCH + SCH + CCCH + SDCCH + FACCH) aus Tabelle 2.6 übertragen. Der Zeitschlitz 1 überträgt ebenfalls einen 51er Multirahmen und verwendet Konfiguration B7 (SDCCH + SACCH). Die restlichen 5 Zeitschlitzte verwenden die Konfiguration B1 (TCH + SACCH + FACCH) und übertragen einen 26er Multirahmen. Dem FACCH ist kein fester Zeitschlitz zugewiesen, da dieser nur bei Bedarf übertragen wird.

Nummer	Zeitschlitz 0	Zeitschlitz 1		Nummer	Zeitschlitz 0	...	Zeitschlitz 7
0	FCCH	SDCCH / 0		0	TCH		TCH
1	SCH	SDCCH / 0		1	TCH		TCH
2	BCCH	SDCCH / 0		2	TCH		TCH
3	BCCH	SDCCH / 0		3	TCH		TCH
4	BCCH	SDCCH / 1		4	TCH		TCH
5	BCCH	SDCCH / 1		5	TCH		TCH
6	AGCH / PCH	SDCCH / 1		6	TCH		TCH
7	AGCH / PCH	SDCCH / 1		7	TCH		TCH
8	AGCH / PCH	SDCCH / 2		8	TCH		TCH
9	AGCH / PCH	SDCCH / 2		9	TCH		TCH
10	FCCH	SDCCH / 2		10	TCH		TCH
11	SCH	SDCCH / 2		11	TCH		TCH
12	AGCH / PCH	SDCCH / 3		12	SACCH		SACCH
13	AGCH / PCH	SDCCH / 3		13	TCH		TCH
14	AGCH / PCH	SDCCH / 3		14	TCH		TCH
15	AGCH / PCH	SDCCH / 3		15	TCH		TCH
16	AGCH / PCH	SDCCH / 4		16	TCH		TCH
17	AGCH / PCH	SDCCH / 4		17	TCH		TCH
18	AGCH / PCH	SDCCH / 4		18	TCH		TCH
19	AGCH / PCH	SDCCH / 4		19	TCH		TCH
20	FCCH	SDCCH / 5		20	TCH		TCH
21	SCH	SDCCH / 5		21	TCH		TCH
22	SDCCH / 0	SDCCH / 5		22	TCH		TCH
23	SDCCH / 0	SDCCH / 5		23	TCH		TCH
24	SDCCH / 0	SDCCH / 6		24	TCH		TCH
25	SDCCH / 0	SDCCH / 6		25	frei		frei
26	SDCCH / 1	SDCCH / 6		0	TCH	26er Multiframe	TCH
27	SDCCH / 1	SDCCH / 6		1	TCH		TCH
28	SDCCH / 1	SDCCH / 7		2	TCH		TCH
29	SDCCH / 1	SDCCH / 7		3	TCH		TCH
30	FCCH	SDCCH / 7		4	TCH		TCH
31	SCH	SDCCH / 7		5	TCH		TCH
32	SDCCH / 2	SACCH / 0		6	TCH		TCH
33	SDCCH / 2	SACCH / 0		7	TCH		TCH
34	SDCCH / 2	SACCH / 0		8	TCH		TCH
35	SDCCH / 2	SACCH / 0		9	TCH		TCH
36	SDCCH / 3	SACCH / 1		10	TCH		TCH
37	SDCCH / 3	SACCH / 1		11	TCH		TCH
38	SDCCH / 3	SACCH / 1		12	SACCH		SACCH
39	SDCCH / 3	SACCH / 1		13	TCH		TCH
40	FCCH	SACCH / 2		14	TCH		TCH
41	SCH	SACCH / 2		15	TCH		TCH
42	SACCH / 0	SACCH / 2		16	TCH		TCH
43	SACCH / 0	SACCH / 2		17	TCH		TCH
44	SACCH / 0	SACCH / 3		18	TCH		TCH
45	SACCH / 0	SACCH / 3		19	TCH		TCH
46	SACCH / 1	SACCH / 3		20	TCH		TCH
47	SACCH / 1	SACCH / 3		21	TCH		TCH
48	SACCH / 1	frei		22	TCH		TCH
49	SACCH / 1	frei		23	TCH		TCH
50	frei	frei		24	TCH		TCH
			51er Multiframe	25	frei		frei

Abbildung 2.8.: Abbildung von logischen auf physikalische Kanäle
 Zeitschlitz 0: BCCH + FCCH + SCH + CCCH + SDCCH + FACCH
 Zeitschlitz 1: SDCCH + SACCH
 Zeitschlitz 2-7: TCH + SACCH + FACCH

2.5. GSM-Ortung

GSM-Ortung beschreibt die Lokalisierung eines eingeschalteten Mobilfunktelefons. Für eine Ortung des Mobilfunktelefons kann es verschiedene Gründe geben:

- Notfall
- Überwachung durch Strafverfolgungsbehörden
- Selbstlokalisierung durch Eigentümer des Mobilfunktelefons
- Location Based Services
- Verkehrstelematik

Die Ortung von Mobilfunktelefonen wurde 2001 zum ersten Mal durch die US-Regierung gesetzlich festgeschrieben [14]. Demzufolge muss bei einem Notruf die anrufende Person auf 125m genau geortet werden. Auch in Deutschland ist eine Ortung im Notfall möglich. Eine Genauigkeit ist jedoch gesetzlich nicht vorgeschrieben [15]. Die Ortung durch Strafverfolgungsbehörden geschieht meist durch das wiederholte Senden einer sog. lautlosen SMS. Diese dient dazu eine Verbindung herzustellen, ohne dass der Benutzer davon Kenntnis erlangt.

In einem Test konnte ein Mobilfunktelefon im O₂ Mobilfunknetz mehrfach 270 m vom Aufenthaltsort entfernt geortet werden (Standort: Hermann-Herder-Str.10; 79104 Freiburg). Die Ergebnisse der Ortung sind im Anhang B detailliert dargestellt. Bei diesem Test wurde eine sichtbare SMS durch das Mobilfunknetz übertragen. Während der Übertragung wurde das Mobilfunktelefon lokalisiert. Der Test wurde mit dem „Handy Finder“ des Anbieters durchgeführt.

2.5.1. Netzseitige Ortung

Für die aktive Ortung eines Teilnehmers durch das Netz gibt es vielfältige Techniken. Diese unterscheiden sich vor allem hinsichtlich ihrer Genauigkeit und der Notwendigkeit für Modifikationen am Mobilfunknetz und Mobilfunktelefon. Ein Überblick über verschiedene Verfahren wird in der Arbeit von H. Ingensand und P. Bitzi gegeben [16]. Die Autoren stellen fest, dass die GSM-Lokalisierung oft wesentlich ungenauer ist als GPS, jedoch eine Ergänzung zur GPS-Positionsbestimmung darstellen kann.

In der Arbeit werden verschiedene Technologien zur GSM-Positionsbestimmung vorgestellt:

- Cell of Origin – COO

Diese Methode ermittelt die Zelle, in der sich das Mobilfunktelefon befindet. Dies ist nur bei einer aktiven Verbindung möglich. Da Zellen sehr groß sein können, weist das Verfahren eine unzureichende Genauigkeit auf. Der Vorteil dieses Verfahrens ist, dass die Infrastruktur nicht verändert werden muss. Das Verfahren kann durch die Bestimmung der verwendeten Antenne und den Timing-Advanced Parameter verbessert werden.

- Angle of Arrival – AOA

Bei diesem Verfahren wird durch zwei Basisstationen der Winkel des eintreffenden Signals bestimmt. Der Schnittpunkt der beiden Geraden ergibt die Position des Senders. Für dieses Verfahren ist es notwendig, die Basisstationen mit mehreren Antennen zur Bestimmung des Winkels auszustatten.

- Received Signal Strength – RSS

Um eine ausreichende Genauigkeit zu erzielen, wird bei diesem Verfahren das Signal

eines Mobilfunktelefons von mindestens drei BTS empfangen. Jede BTS bestimmt die empfangene Signalstärke. Durch die Kombination der empfangenen Signalstärken kann die Position des Teilnehmers bestimmt werden.

- Time of Arrival – TOA

Bei dieser Methode wird die Signallaufzeit zwischen MS und BTS gemessen. Es wird zwischen Uplink- und Downlinkverfahren unterschieden. Beim Downlinkverfahren berechnet das Mobilfunktelefon seine eigene Position aus den Signallaufzeiten. Dies wird als "Enhanced Observed Time Difference" (E-OTD) bezeichnet und benötigt spezielle Hard- und Software auf dem Mobilfunktelefon. Beim Uplinkverfahren wird die Ankunftszeit des Signals durch die BTS gemessen. Dieses Verfahren wird als "Time Difference of Arrival" (TDOA) bezeichnet und benötigt zusätzliche Hardware im Mobilfunknetz.

2.5.2. Ortung durch das Mobilfunktelefon

Die Selbstlokalisierung über GSM-Signale setzt nicht die Kontrolle über das Mobilfunknetzwerk voraus und wird über die vom Benutzer empfangenen Informationen realisiert. Ein mögliches Verfahren wird in Kapitel 6 (ab Seite 51) genauer beschrieben. In diesem Kapitel werden zudem praktische Experimente zur Bestimmung des aktuellen Standorts durchgeführt.

3. Hardware

Zum Empfangen und Verarbeiten von GSM-Signalen ist spezielle Hardware notwendig. Die Grundlage zum Empfangen der Signale ist das “Universal Software Radio Peripheral”, das in Kapitel 3.1 beschrieben wird. Darauf aufbauend wird in Kapitel 3.2 und 3.3 beschrieben, wie der Empfang von GSM-Signalen durch Hardwareoptimierungen verbessert werden kann. Damit die empfangenen Informationen in ihrer Qualität und Vollständigkeit bewertet werden können, werden diese mit den Informationen des Mobilfunktelefons Nokia 3310 verglichen. Die notwendigen Veränderungen an diesem Mobilfunktelefon werden in Kapitel 3.4 beschrieben.

3.1. Universal Software Radio Peripheral

Das “Universal Software Radio Peripheral”, kurz USRP, ist ein Software Defined Radio, das von der Firma Ettus Research hergestellt wird. Ein Software Defined Radio (SDR) besteht aus einer Hardware- und einer Softwarekomponente, die zusammen einen kompletten Hochfrequenzsender und Empfänger bilden. Bei einem SDR wird die Hardware möglichst einfach und universell gestaltet, um diese für ein breites Anwendungsfeld nutzbar zu machen. Die komplexe Signalverarbeitung erfolgt anschließend in Software. Auf diese Weise werden Hardwareprobleme in Softwareprobleme transferiert. Dies ermöglicht eine schnelle Prototypenentwicklung, da Software wesentlich flexibler als Hardware ist. Die Möglichkeiten eines SDR sind optimalerweise durch den Quellcode und nicht durch Hardware-Beschränkungen limitiert. Gerade bei der Entwicklung neuer Geräte kann ein SDR von großem Nutzen sein, da es sich jederzeit an die aktuellen Anforderungen anpassen lässt. In Abbildung 3.1 ist der Aufbau eines SDR schematisch abgebildet.

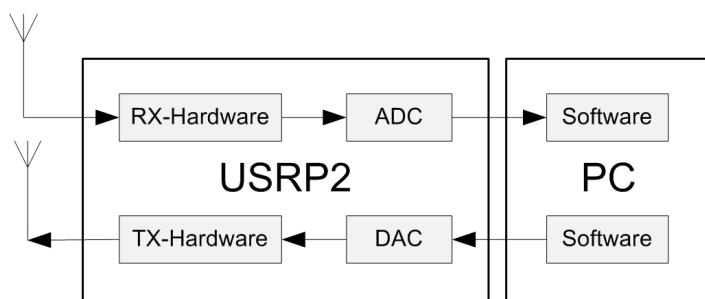


Abbildung 3.1.: Aufbau eines Software-Radios

Die Hardwarekomponente besteht sehr vereinfacht dargestellt aus einem Analog-Digital-Konverter für die Empfangsrichtung und einem Digital-Analog-Konverter für die Senderichtung sowie einer Sende- und Empfangseinheit mit angeschlossenen Antennen. Beim Empfangen werden die analogen Signale digitalisiert und an den angeschlossenen Computer weitergeleitet. Zum Senden müssen die Signale auf dem Computer digital moduliert werden, damit diese anschließend im SDR in analoge Hochfrequenzsignale transferiert werden können.

Von der Firma Ettus werden zwei Versionen des USRP angeboten, das USRP1 und das USRP2. Dabei ist das USRP2 das Nachfolgemodell des USRP1 und unterscheidet sich in

wesentlichen Ausstattungsmerkmalen vom USRP1. In Abbildung 3.2 sind das USRP1 und das USRP2 abgebildet. Einen Vergleich der Ausstattung beider Geräte zeigt Tabelle 3.1.



Abbildung 3.2.: Universal Software Radio Peripheral Version 1 (links) und Version 2 (rechts)

	USRP1	USRP2
Anschluss	USB 2.0	Gigabit Ethernet
FPGA	Altera EP1C12	Xilinx Spartan 3 2000
RF Bandbreite	8 MHz @ 16 Bits	25 MHz @ 16 Bits
Preis	\$700	\$1400
ADC Samples	12 Bit, 64 MS/s	14 Bit, 100 MS/s
DAC Samples	14 Bit, 128 MS/s	16 Bit, 400 MS/s
Daughterboard-Kapazität	2 TX, 2 RX	1 TX, 1 RX
SRAM	-	1 MB
Stromversorgung	6 V, 3 A	6 V, 3 A

Tabelle 3.1.: Ausstattungsvergleich USRP1 und USRP2

Beide Geräte ermöglichen es, Frequenzen zwischen 1 MHZ und 5.85 GHz zu verarbeiten. Das USRP2 besitzt im Vergleich zum USRP1 eine erheblich höhere RF-Bandbreite¹. Dies ist im Rahmen dieser Arbeit von Interesse, da möglichst viele GSM-Kanäle gleichzeitig betrachtet werden sollen. Beim USRP1 wird ein USB 2.0 Interface verwendet, um die Daten an den Computer zu senden. Aus der höheren RF-Bandbreite des USRP2 resultiert eine erheblich höhere Datenrate. Diese kann von einem USB-Port nicht übertragen werden. Aus diesem Grund ist das USRP2 mit einem Gigabit-Ethernet-Port ausgestattet. Das FPGA des USRP2 ist wesentlich leistungsfähiger als das Altera FPGA des USRP1. Beide Geräte müssen mit sogenannten "Daughterboards" ausgestattet werden, um empfangen und senden zu können. Das USRP1 kann zwei Tranceiverkarten aufnehmen, das USRP2 hingegen nur eine. Im Rahmen der Arbeit zeigte sich, dass die höhere RF-Bandbreite des USRP2 zweckdienlicher ist, anstelle von zwei Receiverkarten im USRP1. Wegen der höheren RF-Bandbreite wurde im Rahmen dieser Arbeit das USRP2 verwendet. Das USRP2 mit aufgestecktem DBSRX-Daughterboard ist in Abbildung 3.3 zu sehen.

3.1.1. Daughterboards

Sowohl USRP1 als auch USRP2 können mit denselben Receiver-/Transceiverkarten ausgestattet werden. Die Karten sind jeweils für ein spezielles Frequenzband optimiert. Für den Einsatz in Frequenzbändern von GSM sind die in Tabelle 3.2 gelisteten Karten von Interesse. Da das USRP2 nur eine Receiver-/Transceiverkarten aufnehmen kann und sowohl das GSM900 als auch das GSM1800 Band empfangen werden sollen, kommen die Karten RFX900 und

¹ Radio-Frequency-Bandbreite beschreibt die Differenz zwischen höchster und niedrigster Frequenz die betrachtet wird.

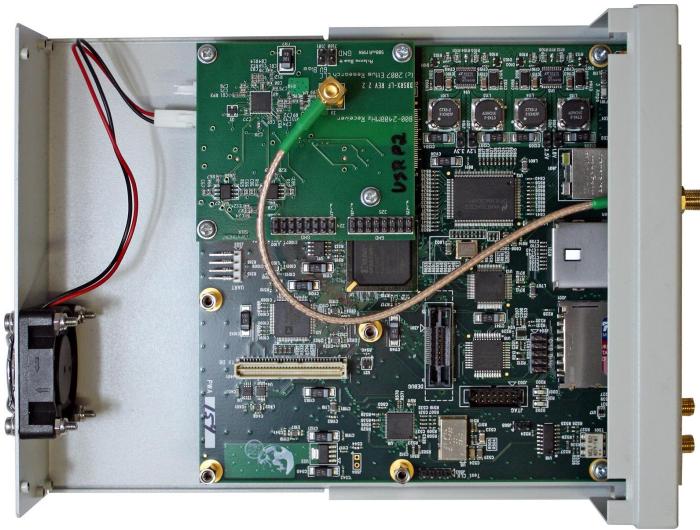


Abbildung 3.3.: USRP2 mit aufgesteckter DBRX-Receiverkarte

Name	Frequenzbereich	Sendestärke
RFX900	800 – 1000 MHz	200 mW
RFX1800	1500 – 2100 MHz	100 mW
DBSRX	800 – 2400 MHz	–
WBX	50 – 2200 MHz	100 mW

Tabelle 3.2.: Vergleich Receiver-/Transceiverkarten

RFX1800 nicht in Frage. Theoretisch ist ein Umprogrammieren einer RFX900 in eine RFX1800 Karte möglich. Jedoch kann dies nur mit dem USRP1 durchgeführt werden. Das Umprogrammieren ist zudem nicht immer erfolgreich.

Da zu Beginn dieser Masterarbeit die WBX-Karte noch nicht verfügbar war und ein Senden nicht erforderlich ist, wird im Folgenden die DBSRX-Karte verwendet. Diese erlaubt es Frequenzen zwischen 800 MHz und 2400 MHz zu empfangen. Die Karte deckt somit das EGSM900 und das GSM1800 Band ab. Damit die Karte mit dem USRP2 funktioniert, muss sie wie im Anhang D beschrieben modifiziert werden. In Abbildung 3.4 sind die Karten RFX900/1800 und DBSRX abgebildet.

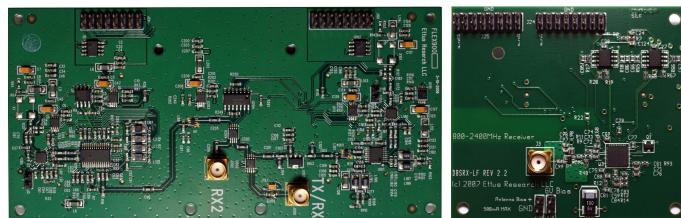


Abbildung 3.4.: links: Transceiverkarten RFX900/RFX1800; rechts: Receiverkarte DBRX

3.2. Antennen

Im Rahmen dieser Arbeit wurden Möglichkeiten evaluiert, wie der Empfang von GSM-Signalen optimiert werden kann. In diesem Zusammenhang wurden verschiedene Antennen untersucht,

um den Empfang von schwachen Signalen zu ermöglichen und somit die Menge der decodierbaren GSM-Signale zu erhöhen. Zu Beginn wurden die Anforderungen an die Antennen analysiert, um die Menge der Antennen, die getestet werden sollen zu minimieren. Folgende Anforderungen sind bei der Wahl der Antennen zu berücksichtigen:

- Omnidirektionale Charakteristik
- Hoher Antennengewinn
- Kleine Bauart
- Empfang von EGSM900 und GSM1800

Gerichtete Antennen, die Signale aus einer bestimmten Richtung bevorzugen, können einen höheren Antennengewinn als omnidirektionale Antennen erzielen. Diese entsprechen jedoch nicht den Anforderungen, da alle Sendemasten in der Umgebung empfangen werden sollen und nicht nur aus einer Richtung. Ein hoher Antennengewinn ist wünschenswert, damit auch schwache Signale ausreichend stark empfangen werden, jedoch ist ein hoher Antennengewinn und geringe Abmessungen der Antenne nicht gleichzeitig zu erzielen. Eine Antenne ist immer ein Kompromiss zwischen den genannten Anforderungen.

Insgesamt wurden die fünf verschiedenen Antennen aus Abbildung 3.5 betrachtet.

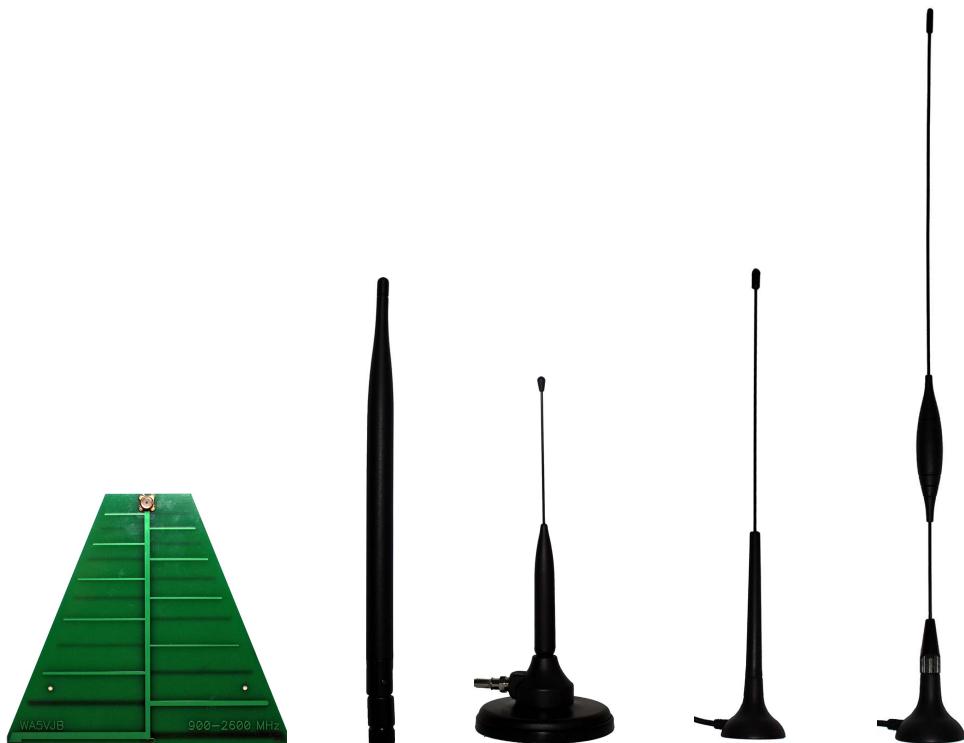


Abbildung 3.5.: Untersuchte GSM-Antennen, von links nach rechts: LP0926, VERT900, MAG2100, SLM155 und SLM17

Die Antennen VERT900 und LP0926 sind als Zubehör zum USRP im Online-Shop der Firma Ettus erhältlich. Bei den Antennen MAG 2100 und SLM155 sowie SLM17 handelt es sich um Magnetfußantennen der Firma Thieking². Bei diesen Antennen war es notwendig den Stecker

²Thieking, <http://www.thiecom.de> [Online; letzter Aufruf 17.02.2010]

3. Hardware

des Anschlusskabels gegen einen SMA-Stecker zu tauschen, um die Antennen direkt an das USRP2 anschließen zu können. In Tabelle 3.3 sind die Frequenzbereiche und der Antennengewinn laut Hersteller angegeben. Die Angaben der Hersteller schienen zum Teil willkürlich und wurden durch Vergleichsmessungen überprüft. Für jede Antenne wurde sowohl im GSM900

Name	Frequenzbereich in MHz	Antennengewinn
VERT900	824–960 MHz, 1710–1990 MHz	3 dBi
LP0926	900 MHz bis 2.6 GHz	5–6 dBi
MAG 2100	890–960, 1710–1880, 1850–1990, 1900–2170	2–5 dBi
SLM155	890–960, 1850–1990, 1850–1990, 1900–2170, 2400	NA
SLM17	890–960, 1850–1990, 1850–1990, 1900–2170	5 dBi

Tabelle 3.3.: Vergleich Receiver-/Transceiverkarten

als auch im GSM1800 Band eine Signalstärke bestimmt. Dabei wurden zwei BTS mit starkem Signal ausgewählt. Es wurde auf eine identische Position der Antennen geachtet um vergleichbare Resultate zu erhalten. Die Ergebnisse wurden mit dem Script `usrp2_fftp.py` von GNU Radio bestimmt. GNU Radio wird im folgenden Kapitel 4 beschrieben. Ein Beispiel für die Signalstärkenbestimmung ist in Abbildung 3.6 zu sehen.

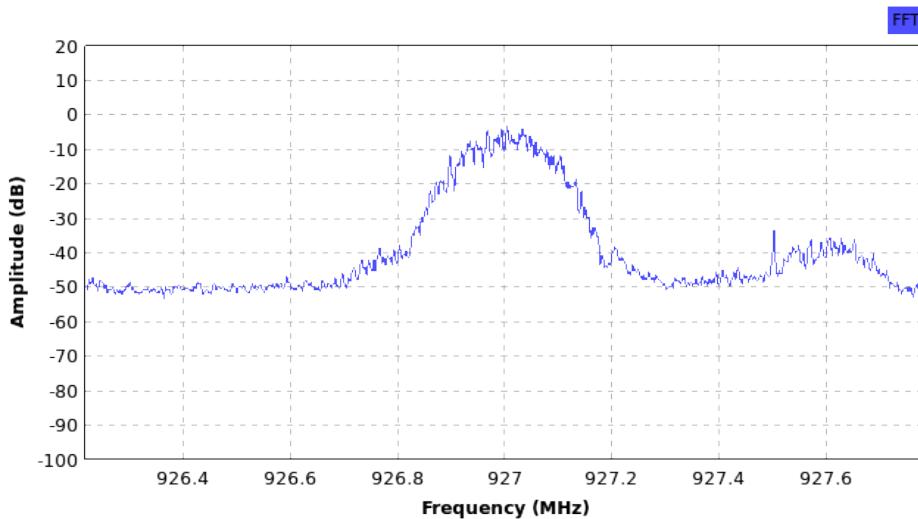


Abbildung 3.6.: Bestimmung der Signalstärke mit der Antenne SLM17

Antenne	Signalstärke bei 927.0 MHz	Signalstärke bei 1846.2 MHz
VERT900	-14 dB	-5 dB
LP0926	-5 dB	-4 dB
MAG 2100	-13 dB	0 dB
SLM155	-7 dB	+3 dB
SLM17	-6 dB	+2 dB

Tabelle 3.4.: Messergebnisse der Antennen

Die Messergebnisse aus Tabelle 3.4 zeigen, dass die Antenne LP0926 im GSM900 Band die beste Signalstärke liefert. Die Antenne SLM17 und SLM155 zeigen die besten Ergebnisse im

GSM1800 Band. Werden das GSM900 und das GSM1800 Band zusammen betrachtet, zeigen die Antennen SLM155 und SLM17 die besten Ergebnisse. Für die folgenden Experimente wurde daher die Antenne SLM155 verwendet.

3.3. Externe Taktgeber

Das USRP2 verfügt über einen internen Oszillatator "CVHD-950 100M" von Crystek³ mit 100 MHz. Dieser wird als Referenztakt für alle Komponenten des USRP2 verwendet. Ein ungenauer Taktgeber wirkt sich direkt auf die Qualität der empfangenen Daten aus. In der GSM-Spezifikation [17] wird vorgeschrieben, dass GSM-Signale eine maximale Frequenzabweichung von 0,1 ppm (parts per million) aufweisen dürfen. Das bedeutet, dass ein GSM900-Signal bei einer Frequenz von 950 MHz maximal 95 Hz abweichen darf. Der interne Taktgeber ist mit einer Abweichung von ± 20 ppm spezifiziert [18] und somit zu ungenau. Das USRP2 hat werkseitig einen Anschluss für einen externen Taktgeber mit 10 MHz und einen Anschluss für Sekundenpulse (pps). Wird ein externer Takt bereitgestellt, kann über einen Softwarebefehl der interne Taktgeber zum externen Takt synchronisiert werden.

In Tabelle 3.5 ist eine Übersicht verschiedener Taktgeber mit ihren Genauigkeiten gegeben. Um möglichst genaue Signale zu erhalten, wurde das USRP2 mit einem "GPS Disciplined Oscillator" (GPSDO) von der Firma Trimble⁴ verbunden.

Bezeichnung	Genauigkeit
Quarz Oszillatator (XO)	10^{-5} bis 10^{-4}
Temperaturgeregelter Oszillatator (TCXO)	10^{-6}
Oven controlled crystal Oscillator (OCXO)	$2 * 10^{-8}$
Rubidium atomic frequency standard (RbXO)	10^{-9}
Caesium atomic frequency standard (CsXO)	10^{-12} bis 10^{-11}
GPS Disciplined oscillator (GPSDO)	10^{-12} bis 10^{-9}

Tabelle 3.5.: Vergleich Taktgeber ($10^{-6} = 1$ ppm)

Der verwendete GPSDP ist in Abbildung 3.7 abgebildet. Die Entscheidung fiel auf diesen Oszillatator, da er gebraucht für unter 200 USD gekauft werden kann und eine sehr gute Genauigkeit aufweist. Initial braucht der GPSDO einige Minuten, um den internen temperaturgeregelten Oszillatator aufzuwärmen und nach GPS-Satelliten zu suchen. Jeder GPS-Satellit ist mit Atomuhr ausgestattet, um ein möglichst exaktes Timing-Signal zu senden. Das empfangene GPS-Signal kann somit als Referenztakt für den internen Oszillatator des GPSDO verwendet werden. Nach einer Initialisierungsphase wird die interne Abweichung des Oszillators über das GPS-Signal ausgeglichen. Durch ein gutes GPS-Signal können somit Genauigkeiten von bis zu 10^{-12} ($\cong 1$ ppt (parts per trillion) = 0,000001 ppm) erreichen werden. In der Abbildung 3.7 sind die externen Anschlüsse RS-232, 1 PPS, 10 MHz, und ANT zu sehen. Der RS-232 Anschluss dient zur Konfiguration und zum Auslesen von Statusinformationen über das mitgelieferte Monitor-Programm (Abbildung 3.7 rechts). Der aktuelle Satellitenstatus wird in der Software rechts dargestellt. Über die Software kann auch die Abweichung des internen Oszillators vom GPS-Signal ausgelesen werden. Diese liegt meist im Bereich von 0,1ppb (parts per billion). Der Standard Oszillatator des USRP2 ist also um den Faktor 10^5 ungenauer.

³Crystekcrystals, <http://www.crysteckrystals.com> [Online; letzter Aufruf 17.02.2010]

⁴Trimble, <http://www.trimble.com> [Online; letzter Aufruf 17.02.2010]

3. Hardware



Abbildung 3.7.: Links: GPSDO von Trimble; Rechts: Monitor-Programm

Vereinfacht dargestellt besteht ein GPSDO aus einem GPS-Receiver-Chip, einem Oszillator und einem Kontrollchip, der die beiden ersten Komponenten ansteuert. Die einzelnen Komponenten des GPSDO sind in Abbildung 3.8 zu sehen.

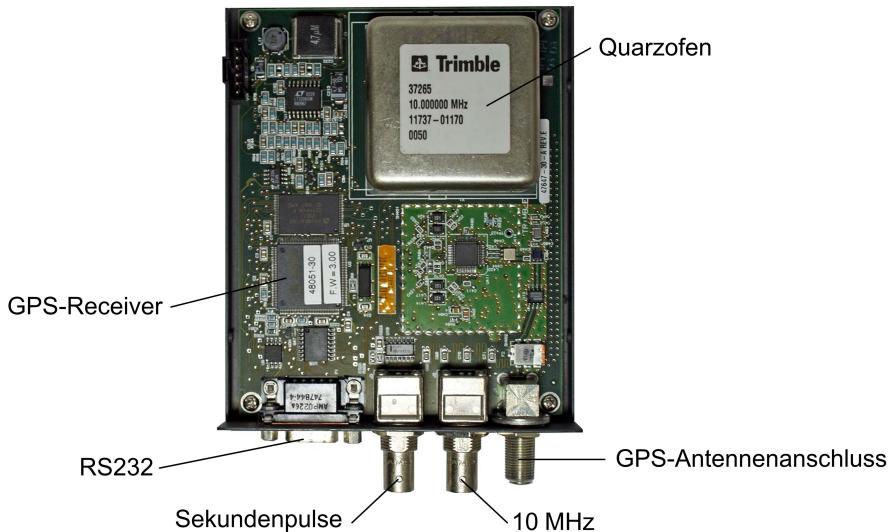


Abbildung 3.8.: Interner Aufbau GPSDO von Trimble

Damit der GPS-Chip einen Kalibrierungstakt bereitstellen kann, ist ein GPS-Fix⁵ und somit der Empfang von mindestens vier Satelliten erforderlich. Ist diese Voraussetzung gegeben, wird vom GPS-Chip ein zur GPS-Zeit synchrones Taktsignal bereitgestellt. Das Taktsignal wird vom Kontrollchip verwendet, um den internen Oszillator zu kalibrieren.

Es hat sich gezeigt, dass auch ohne Satellitensignal der Takt des GPSDO als Referenzsignal für den USRP2 verwendet werden kann. Der Referenztakt ist in diesem Fall nicht so genau wie mit Satellitensignal, jedoch immer noch genauer als der interne Oszillator des USRP2. Die relativ hohe Genauigkeit ohne GPS-Signal ist auf den eingebauten Quarzofen zurückzuführen. Die Genauigkeit des Quarzofens liegt im Bereich zwischen 10^{-6} bis 10^{-8} (1 ppm bis 0,01 ppm). Der Quarzofen ist in Abbildung 3.8 oben rechts als silberner Block zu sehen.

⁵ GPS-Fix: 3D Position auf der Erde gegeben durch Longitude, Latitude und Höhe über Meeresspiegel

3.4. Nokia 3310

Das Nokia 3310 ist ein Mobilfunktelefon der DCT-3 Serie. Bei dieser Serie kann ein Testmodus aktiviert werden. Dieser sogenannte Netmonitor ermöglicht es, interne Informationen zum Zustand des Telefons auszulesen.

Der Netmonitor besteht aus einer Vielzahl verschiedener Ansichten (Seiten), über die der Zustand des Handys angezeigt wird.

3.4.1. Aktivierung des Netmonitors

Für die Aktivierung des Netmonitors wird ein Datenkabel und die Software `gammu`⁶ benötigt. Als Datenkabel kann sowohl ein F-Bus⁷ als auch ein M-Bus⁸ Kabel verwendet werden [19]. Im Folgenden wurde ein F-Bus Kabel genutzt.

Die `gammu` Konfigurationsdatei kann mit dem Programm `gammu-config` angepasst werden und wird unter `~/.gammurc` gespeichert:

```
port = /dev/ttyUSB0
model = 6110
connection = fbus
synchronizetime = yes
logfile =
logformat = nothing
use_locking = yes
gammuloc =
```

Die Freischaltung des Netmonitors erfolgt über den folgenden Befehl:

```
gammu --nokianetmonitor 243
```

Nach einem erforderlichen Neustart des Mobilfunktelefons, ist im Menü der Eintrag Netmonitor zu finden. Hier muss der Wert 01 zum Aktivieren und 00 zum Deaktivieren eingetragen werden. Um die Anzeige des Netmonitors auf die ersten 19 Seiten zu beschränken, muss im Menü der Code 242 eingegeben werden. Die ersten 19 Seiten enthalten alle für diese Arbeit relevanten Daten.

3.4.2. Informationen im Netmonitor



Abbildung 3.9.: Nokia 3310 Netmonitor: Seite 1, 3, 4, 5 und 11

Die Informationen im Netmonitor sind in Seiten unterteilt. Zwischen den Seiten kann mit den Pfeiltasten auf dem Mobilfunktelefon gewechselt werden. Die aktuelle Seite wird im Display oben links angezeigt. Für diese Arbeit sind die in Abbildung 3.9 gezeigten Seiten 1, 3, 4, 5 und 11 von Interesse, da diese Zellinformationen anzeigen. Auf Seite 1 und 11 sind Informationen über die Zelle zu sehen, in der das Mobilfunktelefon aktuell eingebucht ist. Auf den Seiten 3,

⁶ gammu, <http://www.mwiacek.com/gsm/soft/gammu.html> [Online; letzter Aufruf 26.01.2010]

⁷ F-Bus: bidirektionaler half-duplex Bus; 9600 bps 8N1; Eindrahtverbindung

⁸ M-Bus: bidirektionaler full-duplex Bus; 115200 bps 8N1; Zweidrahtverbindung

3. Hardware

4 und 5 ist die aktuell im Handy gespeicherte Nachbarschaftsliste dargestellt.

Allgemeine Erklärung der relevanten Seiten [20]:

Seite 1:

a: Zeichen "H" wird angezeigt, wenn Frequency Hopping aktiv ist.

bbb: Aktueller Kanal

ccc: Signalstärke des aktuellen Kanals in dBm. Bei Werten kleiner als -99 wird das Vorzeichen weggelassen

ddd: Sendestärke; nur bei einer aktiven Verbindung

e: Anzahl der verwendeten Zeitschlitz

ff: Timing Advance; wird von der BTS berechnet und bei einer aktiven Verbindung an das Mobilfunktelefon übermittelt. Damit das vom Mobilfunktelefon gesendete Signal zum richtigen Zeitpunkt bei der BTS eintrifft, wird dem Mobilfunktelefon über den Timing Advance Parameter mitgeteilt, wie weit vor dem Zeitschlitz die Übertragung gestartet werden muss.

g: Fehlerrate während einer Verbindung

mmmm: Radio Link Timeout

nnn: Berechneter Pfadverlust (Wertebereich -99 bis 99) dient der Entscheidung, welche Zelle verwendet werden soll. Es werden nur Zellen mit positiven Werten verwendet.

ppp: (Beim 3310 gleich nnn)

oooo: Aktuell verwendete Kanalkonfiguration

abbb	ccc	ddd
e	ff	g mmmm
nnn		ppp
		oooo

Seite 3, 4, 5:

aaa: Kanalnummer

bbb: Berechneter Pfadverlust (Wertebereich -99 bis 99) dient der Entscheidung, welche Zelle verwendet werden soll. Es werden nur Zellen mit positiven Werten verwendet.

aaabb	bbccc	ddd
aaabb	bbccc	ddd
aaabb	bbccc	ddd

ccc: Signalstärke in dBm

ddd: (Beim 3310 gleich bbb)

Seite 11:

aaa: Mobile Country Code, MCC

CC:aaa	NCbbb
LAC:ccccc	
CH : deee	
CID:fffff	

bbb: Mobile Network Code, MNC

ccccc: Location Area Code, LAC

d: Zeichen "H" wird angezeigt, wenn Frequency Hopping aktiv ist

eee: Aktueller Kanal, ARFCN

fffff: Cell-ID

4. Software

Zum Empfangen, Decodieren und Interpretieren von GSM-Signalen mittels USRP2 sind verschiedene Softwarepakete notwendig. Alle Softwarekomponenten sind frei verfügbar und können beliebig angepasst werden. Die Softwareseite besteht aus den Open Source-Projekten GNU Radio und Airprobe. Die Komponenten arbeiten dabei wie in Abbildung 4.1 gezeigt zusammen. GNU Radio ist für die Kommunikation mit dem USRP2 und für das Empfangen und Speichern der Daten zuständig. Für die Decodierung und Interpretation der Daten wird Airprobe verwendet. Eine strikte Trennung der beiden Projekte GNU Radio und Airprobe ist jedoch nicht möglich, da Airprobe Signalverarbeitungsblöcke von GNU Radio verwendet.

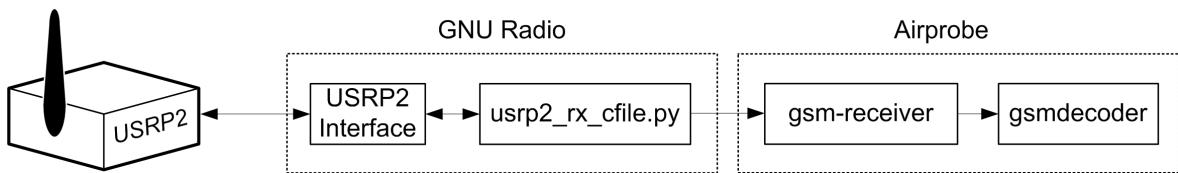


Abbildung 4.1.: Zusammenspiel der Softwarekomponenten

4.1. GNU Radio

GNU Radio¹ ist eine freie Software, die es ermöglicht mit Computern Signalverarbeitung in Software durchzuführen. Es wird damit möglich, mit geringem Hardwareaufwand Radiosignale zu modulieren und zu demodulieren. GNU Radio ist in Signalverarbeitungsblöcke unterteilt, die beliebig kombiniert werden können.

In GNU Radio werden Programme in Python oder C++ geschrieben. Die einzelnen Signalverarbeitungsblöcke liegen als C++ Code vor, um eine möglichst hohe Performance zu erzielen. Die Verbindung der einzelnen Blöcke wird anschließend durch Python-Skripte realisiert. Die Kombination von Python und C++ ermöglicht es, die Signalverarbeitungsblöcke auf einfache Art zu kombinieren und gleichzeitig eine gute Effizienz der Blöcke zu erreichen. Dabei ist die hohe Performance essenziell, da erst durch diese eine Signalverarbeitung in Echtzeit ermöglicht wird. Die Installation von GNU Radio ist im Anhang A.2 beschrieben.

Für einen ersten Test des Setups kann das Skript `usrp2_fft.py` verwendet werden. In Abbildung 4.2 wurde die Frequenzmitte bei 937.5 MHz so gewählt, dass mit dem Decimation-Faktor 4 die Frequenzen zwischen 925 MHz und 950 MHz dargestellt werden. Ein Großteil des EGSM900 Frequenzbandes ist somit sichtbar. Um die stark fluktuierende Darstellung zu glätten, wurde die Funktion "Average" mit Alpha = 0,1 aktiviert. Die Darstellung ermöglicht es, auf einfache Weise Basisstationen mit starken Signalen visuell zu erkennen. In Abbildung 4.2 sind zwei besonders starke Signale bei 927MHz und 929.6 MHz zu sehen.

Um das Signal eindeutig als GSM-Basisstation zu identifizieren, wird nach dem "Frequency Correction Burst" gesucht. Die Funktion des Frequency Correction Burst wurde bereits in

¹ GNU Radio, <http://gnuradio.org/redmine/wiki/gnuradio/WikiStart> [Online; letzter Aufruf 18.02.2010]

4. Software

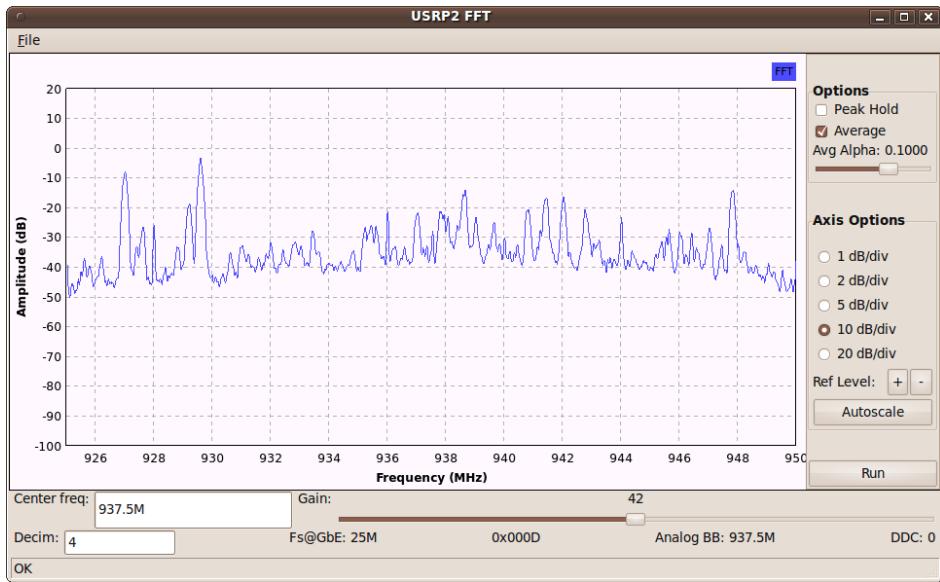


Abbildung 4.2.: Frequenzspektrum zwischen 925 MHz und 950 MHz

Kapitel 2.4.3 beschrieben. Um diesen sichtbar zu machen, wird die Frequenzmitte auf 927 MHz und die Decimation auf 174 gesetzt. Der Decimation-Faktor bestimmt dabei die Bandbreite des Signals, das empfangen werden soll und muss zwischen 4 und 512 liegen. Dabei berechnet sich die Bandbreite des Signals aus der Sampling Rate des USRP2 (100 Mega-Samples Per Second) wie folgt: $\text{RF-Bandbreite} = 100 \text{ MSPS} / \text{decimation}$

Im Unterschied zu Abbildung 4.2 wurde in Abbildung 4.3 die Funktion “Peak Hold” aktiviert, um den Frequency Correction Burst sichtbar zu machen. Dieser ist bei +67,7 kHz deutlich als Ausschlag in der grünen Linie zu sehen. Das Signal wurde somit eindeutig als Funksignal einer BTS identifiziert.

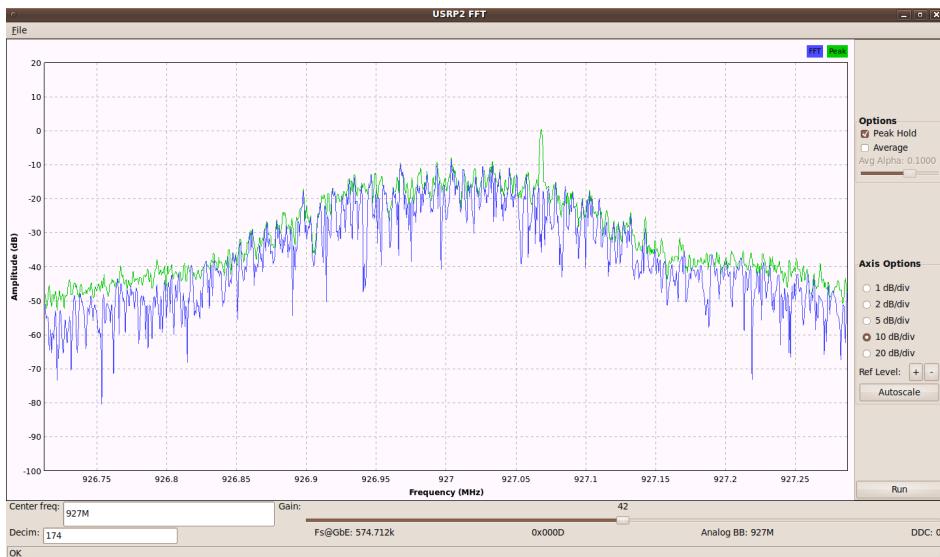


Abbildung 4.3.: Frequenzspektrum einer GSM-Basisstation bei 927 MHz

Um Signale zu empfangen und für die weitere Verarbeitung abzuspeichern, wird das Skript `usrp2_rx_cfile.py` verwendet. Es ist damit möglich, die empfangenen Rohdaten auf die

Festplatte zu schreiben. Es werden dabei die Parameter Decimation (-d), Frequenz (-f), Gain (-g), die Anzahl der Samples (-N) sowie eine Ausgabedatei benötigt.

Beispiel: `usrp2_rx_cfile.py -d 174 -f 927.0M -g 42 -N 200000 out.cfile`

Um die abgespeicherten Daten im Nachhinein zu visualisieren, kann das Programm `baudline` verwendet werden. Dabei werden die Daten wie in Abbildung 4.3 als Frequenzspektrum dargestellt. Zusätzlich wird der Zeitverlauf auf der Y-Achse abgebildet. Diese Art der Visualisierung wird auch als Wasserfallplot bezeichnet. Abbildung 4.4 zeigt die BTS bei 927 MHz. Insgesamt sind 350 ms auf der Y-Achse abgebildet. Auch hier kann der Frequency Correction Burst als periodisch auftretender roter Punkt 67,7 kHz rechts neben der Mitte ausgemacht werden. Frequenzanteile mit hoher Energie sind in dieser Darstellung rot gefärbt.

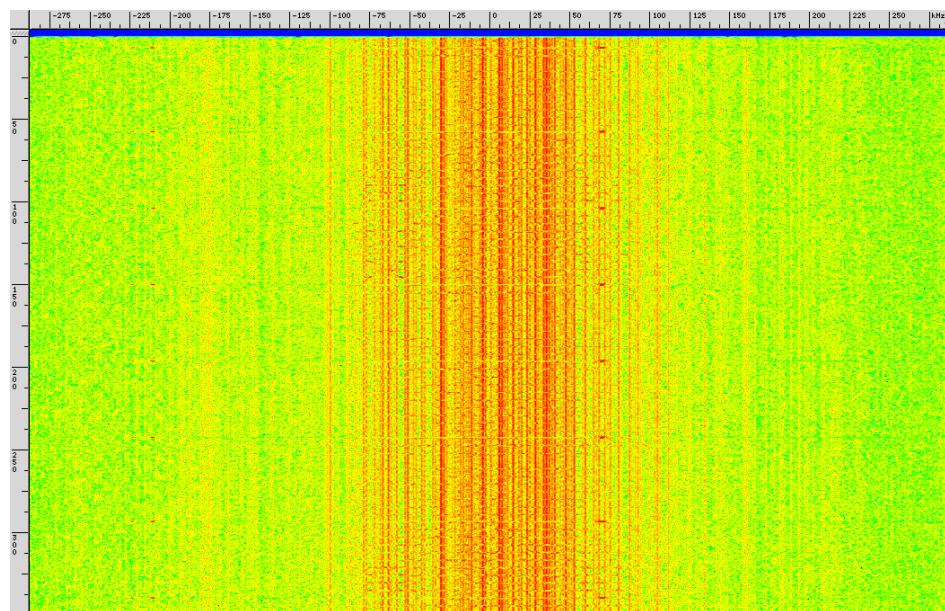


Abbildung 4.4.: Empfangenes Signal bei 927 MHz als Wasserfallplot

Bei der Visualisierung mit `baudline` sind die folgenden Einstellungen notwendig:

- Decompression: Auto magic
- Initial byte offset: 0
- Sample Rate: custom = (100 MSPS/Decim)
- Channels: 2, quadrature aktiv, flip complex aktiviert
- Decode Format: 32 bit linear
- Normalization: auto measure

4.2. Airprobe

Airprobe² ist ein Projekt des Chaos Computer Clubs, das sich zum Ziel gesetzt hat Software zum Empfangen und Analysieren von GSM-Signalen bereitzustellen. Dadurch soll der GSM-Standard besser verstanden und eine Analyse des Standards im Hinblick auf dessen Sicherheit ermöglicht werden. Das Projekt ist in drei Gruppen aufgeteilt: Empfang, Demodulierung und Interpretation von GSM-Signalen. Das Empfangen der Daten wird in dieser Arbeit nicht von Airprobe übernommen, sondern, wie zuvor in Kapitel 4.1 beschrieben, durch das GNU Radio Skript `usrp2_rx_cfile.py`.

Die Namen der Airprobe Programme sind missverständlich gewählt. Zum Decodieren der empfangenen Rohdaten wird das Programm `gsm-receiver` verwendet. Anschließend werden die Daten mit dem Programm `gsmdecode` interpretiert und somit lesbar gemacht.

4.2.1. Decodieren der Daten mit `gsm-receiver`

Im Rahmen dieser Arbeit wurde der original `gsm-receiver` von Airprobe durch eine Weiterentwicklung von Piot Krysik ersetzt³, da diese beim Decodieren der Rohdaten wesentlich bessere Ergebnisse liefert.

Die Programmversion von Piot Krysik war nicht ohne eigene Anpassungen lauffähig, da der `gsm-receiver` ursprünglich für den USRP1 entwickelt wurde. Die notwendigen Anpassungen sind im Patch `gsm-receiver.patch` auf der CD im Anhang zusammengefasst.

Anschließend kann der `gsm-receiver` über ein übliches

`./bootstrap && ./configure && make` kompiliert werden.

Das Python Skript `src/python/gsm_receive.py` steuert den `gsm-receiver` und wird wie folgt verwendet:

Beispiel für das Empfangen und Decodieren einer BTS:

```
Empfangen: usrp2_rx_cfile.py -d 174 -f 927.0M -g 42 -N 1000000 out.cfile
Decodieren: ./gsm_receive.py -d 174 -I out.cfile > out.dfile
```

Das Empfangen der Daten wurde bereits in Kapitel 4.1 beschrieben. Beim Decodieren muss darauf geachtet werden, dass die gleiche Decimation wie beim Empfangen der Daten verwendet wird. Im Beispiel wird die Decimation 174 verwendet. Als Eingabe nimmt der `gsm-receiver` den Rohdatenstrom vom `usrp2_rx_cfile.py` Skript. Die Ausgabe wird in die Datei `out.dfile` umgeleitet, damit sie zur weiteren Verarbeitung bereitsteht.

Auszug aus `out.dfile`:

```
59 06 1a 9b ea 06 fe 09 cf c0 80 00 00 00 00 00 00 00 00 08 94 00 00
15 06 21 00 01 f0 2b 2b
25 06 21 00 05 f4 1a 45 c6 af 2b 2b
49 06 1b d7 c6 62 f2 30 02 4c c9 05 78 46 65 03 94 00 00 89 1f 40 4b
...
...
```

² Airprobe, <https://svn.berlin.ccc.de/projects/airprobe> [Online; letzter Aufruf 22.04.2010]

³ GSM-Receiver von Piot Krysik, <http://home.elka.pw.edu.pl/~pkrysik/GSM/gsm-receiver.tar.gz> [Online; letzter Aufruf 22.04.2010]

Die vom `gsm-receiver` decodierten Daten werden hexadezimal in die Ausgabedatei geschrieben. Diese Daten müssen jetzt durch einen Interpreter lesbar gemacht werden. Diese Aufgabe übernimmt `gsmdecode`.

4.2.2. Interpretieren der Daten mit `gsmdecode`

`gsmdecode` wird verwendet, um die von `gsm-receiver` decodierten Daten zu interpretieren. Dabei stand für die Entwickler eine möglichst einfache Darstellungsweise im Vordergrund.

Interpretieren der Daten:

```
cat out.dfile | gsmdecode/src/gsmdecode -i
```

Gekürzte Ausgabe:

```
HEX 12_data_out_Ebis:462 Format Bbis DATA
000: 49 06 1b d7 c6 62 f2 30 - 02 4c c9 05 78 46 65 03
001: 94 00 00 89 1f 40 4b
    0: 49 010010-- Pseudo Length: 18
    1: 06 0----- Direction: From originating site
    1: 06 -000---- 0 TransactionID
    1: 06 ----0110 Radio Resouce Management
    2: 1b 00011011 RRsystemInfo3C
    3: d7 55238      [0xd7c6] Cell identity
    5: 62 262      Mobile Country Code (Germany)
    6: f2 03f      Mobile Network Code (E-Plus Mobilfunk GmbH & Co. KG)
    8: 02 588      [0x024c] Local Area Code
   10: c9 1----- Spare bit (should be 0)
   10: c9 -1----- MSs in the cell shall apply IMSI attach/detach procedure
   10: c9 --001--- Number of blocks: 1
   10: c9 ----001 1 basic physical channel for CCCH, combined with SDCCHs
   11: 05 00000--- spare bits (should be 0)
   11: 05 ----101 7 multi frames period for paging request
   12: 78 01111000 T3212 TimeOut value: 120
   13: 46 0----- spare bit (should be 0)
   13: 46 -1----- Power control indicator is set
   13: 46 --00---- MSs may use uplink DTX
   13: 46 ----0110 Radio Link Timeout: 28
   14: 65 011----- Cell Reselect Hyst. : 6 db RXLEV
   14: 65 ---xxxxx Max Tx power level: 5
   15: 03 0----- No additional cells in SysInfo 7-8
   15: 03 -0----- New establishm cause: not supported
   15: 03 --xxxxxx RXLEV Access Min permitted = -110 + 3dB
   16: 94 10----- Max. of retransmiss : 4
   16: 94 --0101-- slots to spread TX : 8
   16: 94 -----0- The cell is barred : no
   16: 94 -----0 Call reestabl.i.cell: allowed
   17: 00 -----0-- Emergency call EC 10: allowed
   17: 00 00000--- Acc ctrl cl 11-15: 0 = permitted, 1 = forbidden
   17: 00 -----00 Acc ctrl cl 8- 9: 0 = permitted, 1 = forbidden
   17: 00 -----0 Ordinary subscribers (8)
```

4. Software

```
17: 00 -----0- Ordinary subscribers (9)
17: 00 -----0-- Emergency call (10): Everyone
17: 00 ----0--- Operator Specific (11)
17: 00 ---0---- Security service (12)
17: 00 --0----- Public service (13)
17: 00 -0----- Emergency service (14)
17: 00 0----- Network Operator (15)
18: 00 00000000 Acc ctrl cl 0- 7: 0 = permitted, 1 = forbidden
18: 00 00000000 Ordinary subscribers (0-7)
19: 89 YYYYYYYY REST OCTETS (4)
```

In dieser Ausgabe ist ein Radio Resource Management Datenpaket zu sehen. Die für diese Arbeit interessanten Informationen Cell-ID (Byte 3), Mobile Country Code (Byte 5), Mobile Network Code (Byte 6), Local Area Code (Byte 8) können direkt abgelesen werden.

Um die Arbeit mit `gsm-receiver` und `gsmdecode` zu erleichtern, kann das Skript `gsm-receive/src/python/go.sh` verwendet werden. Die Decodierung und Interpretation der Daten wird sequenziell durchgeführt und die interpretierten Daten werden direkt ausgegeben.

5. GSM-Scanner

Im Rahmen dieser Arbeit wurde die Software **GSM-Scanner** entwickelt. Der **GSM-Scanner** empfängt GSM-Signale über den USRP2 und verarbeitet diese. Folgende Anforderungen an die Software wurden definiert:

- Empfang von GSM-Broadcast-Informationen von BTS auf den Frequenzbändern EGSM900 und GSM1800
- Decodieren und Verarbeiten der GSM-Signale
- Darstellung der Daten, die eine Basisstation eindeutig definieren
- Optimierung der Empfangsgeschwindigkeit

Insgesamt müssen 548 Kanäle untersucht werden. Die Informationen MCC, MNC, LAC und Cell-ID identifizieren eine BTS eindeutig und sollen im Rahmen dieser Arbeit empfangen und visualisiert werden. Die Informationen werden auf dem logischen Broadcast-Kanal BCCH übertragen. Der BCCH wird im 51er Multirahmen alle 235 ms^1 gesendet (siehe Kapitel 2.4.4). Die Darstellung der empfangenen Informationen soll dem Benutzer einen Überblick über die verfügbaren GSM-Basisstationen in der Umgebung geben. Diese Funktion ist auch im Rahmen von Lehrveranstaltungen an der Universität von Interesse.

Es wurden verschiedene Versionen des **GSM-Scanners** entwickelt und evaluiert. Während der Entwicklung stand vor allem im Vordergrund, die Zeit zu minimieren, die für eine komplette Abtastung des EGSM900 und GSM1800-Frequenzbandes benötigt wird.

5.1. Aufbau des GSM-Scanners

Zum Empfangen der GSM-Signale wird das USRP2 aus Kapitel 3.1 verwendet. Das Zusammenspiel der einzelnen Softwarekomponenten zeigt Abbildung 5.1.

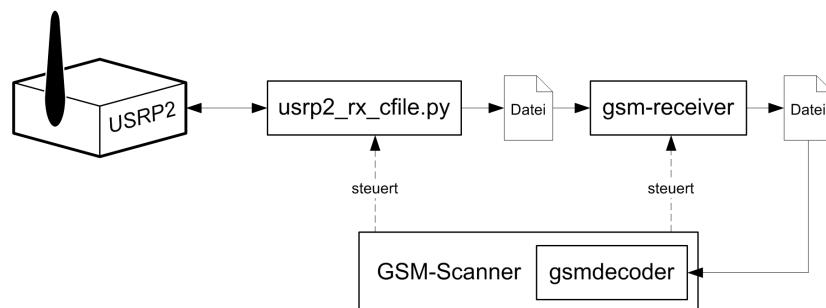


Abbildung 5.1.: Zusammenspiel der verwendeten Softwarekomponenten

Das in Kapitel 4.1 vorgestellte Python Script `usrp2_rx_cfile.py` steuert den USRP2 und schreibt die empfangenen Signale in eine Datei auf die Festplatte. Dieses Script wird durch das

¹ genauer: Einmal pro Multirahmen $\hat{=}$ alle 3060/13 ms

Programm **GSM-Scanner** aufgerufen. Die Verarbeitung der Signale wird über die Programme **gsm-receiver** und **gsmdecode** des Airprobe-Projektes ermöglicht. Airprobe wurde in Kapitel 4.2 vorgestellt. Der **gsm-receiver** wird als eigenständiges Programm aufgerufen und erfordert als Eingabe die empfangenen Daten des GNU Radio Scripts **usrp2_rx_cfile.py**. Die Ausgabe wird in einer Datei abgelegt. Der Programmcode von **gsmdecoder** wurde in das entwickelte Programm **GSM-Scanner** integriert, um benötigte Informationen direkt auslesen zu können.

5.2. Probleme mit dem gsm-receiver

Während der Entwicklung des **GSM-Scanners** wurden verschiedene Probleme mit dem verwendeten Decoder **gsm-receiver** festgestellt.

1. Der Decoder arbeitet nicht deterministisch. Wiederholtes Decodieren identischer Eingangssignale führt in seltenen Fällen zu unterschiedlichen Ergebnissen. Dies hat zur Folge, dass beim Decodieren der Kanäle nicht davon ausgegangen werden kann, dass alle decodierbaren Daten auch wirklich decodiert wurden. Das Problem konnte auf fehlerhafte Behandlung der Eingangsdaten im Decoder zurückgeführt werden. Im zeitlichen Rahmen dieser Arbeit, konnte das Problem jedoch nicht behoben werden, da der geschätzte Arbeitsaufwand wesentlich zu hoch ist.
2. Der Decoder empfängt Daten auf einem Nachbarkanal. Der ursprüngliche Decoder hatte Probleme die GSM-Kanäle zu trennen. Es konnte vorkommen, dass die Informationen eines Kanals mit hoher Signalstärke auch auf den Nachbarkanälen auftauchen. Dies äußert sich durch zwei Basisstationen mit gleicher Cell-ID auf benachbarten Kanälen. Das Problem konnte durch eine Anpassung des Eingangsfilters gelöst werden. Dabei wurde die Signalbandbreite des Eingangsfilters verringert, um das Übersprechen herauszufiltern. Die Modifikationen am Decoder sind auf der CD im Anhang im Ordner **/gsm-receiver/patch/** zu finden.
3. Empfangene Signale können nicht immer decodiert werden. Auch bei einem statischen Setup mit identischer Antennenposition hat der Decoder mit bestimmten Eingangssignalen Probleme. Dies führt dazu, dass trotz ausreichender Signalstärke auf einem Kanal keine Daten decodiert werden. Der Grund für dieses Verhalten konnte nicht eindeutig identifiziert werden. Vermutlich führen bestimmte Eingangssignale zu einem blockierenden Zustand im Decoder.

5.3. Erste Implementierung

Die erste entwickelte Programmversion empfängt Signale auf allen GSM-Kanälen. Der Ablauf des Programms ist wie folgt:

1. M = Menge aller Kanäle aus EGSM900 und GSM1800
2. Empfange auf jedem Kanal aus M Daten
3. Decodiere für jeden Kanal aus M die Daten

Da bei der ersten Implementierung jeder Kanal betrachtet wird, werden nur selten BTS übersehen. Jedoch dauert ein kompletter Scan-Vorgang für das EGSM900 und GSM1800 Band zusammen über zehn Minuten. Dabei kann es vorkommen, dass die Cell-ID nicht von jeder BTS empfangen wurde. Dies tritt auf, wenn die empfangenen Daten teilweise nicht decodiert werden konnten, entweder weil die Signalstärke nicht ausreichend war oder weil es zu Störungen auf dem Kanal gekommen ist. Ein weiterer Grund ist, dass die Cell-ID nicht in jedem

Paket des BCCH enthalten ist. Tabelle 5.1 enthält die für diese Arbeit relevanten “System Information Messages”, die auf dem BCCH gesendet werden. Die “System Information Message” Type 3 enthält die Informationen, die eine BTS eindeutig identifizieren. Bei Typ 4 fehlt die Cell-ID. Aus diesem Grund kann es beim GSM-Scanner vorkommen, dass die Cell-ID nicht empfangen wird.

Wann welcher Typ gesendet wird, hängt von der Variablen TC ab. Diese wird über die Formel $TC = (FN \text{ DIV } 51) \bmod (8)$ berechnet. Dabei ist FN die aktuelle Rahmennummer im 51er Multirahmen. Es gibt weitere “System Information Messages”, die für diese Arbeit nicht

System Information Message	TC	enthaltene Daten
Typ 1	0	Von der Zelle verwendete Frequenzen
Typ 2	1	Nachbarschaftsliste
Typ 3	2 und 6	MCC, MNC, LAC und Cell-ID
Typ 4	3 und 7	MCC, MNC und LAC

Tabelle 5.1.: Auswahl der relevanten “System Information Messages”
(GSM Spezifikation 05.02 Abschnitt 6.3.1.3 und 04.08 Abschnitt 9.1.31)

relevant sind und auch nur in speziellen Netzkonfigurationen verwendet werden. Bei einer Vodafone BTS konnte folgende Sequenz an “System Information Messages” empfangen werden: 1, 2, 3, 4, 3, 4, 1, 2, 3, 4, 3, 4 ...

Um zu gewährleisten, dass auf jedem Kanal die Daten des BCCH auch empfangen werden, müssen die Signale des Kanals ausreichend lange empfangen werden. Da insgesamt 548 Kanäle betrachtet werden, sollte die Aufzeichnungszeit pro Kanal möglichst kurz gehalten werden, um die Gesamtzeit für den Empfang aller Kanäle zu optimieren. Die Mindestempfangsdauer für einen BCCH beträgt 235 ms. Wird jedoch nur eine “System Information Messages” empfangen, kann diese vom Typ 1, 2 oder 3 sein und somit die gesuchten Informationen nicht oder nur teilweise enthalten. Es wurde eine Aufzeichnungsdauer von 1000 ms gewählt, da bei dieser Länge vier “System Information Messages” enthalten sind. Somit kann auch im ungünstigen Fall gewährleistet werden, dass eine “System Information Message Typ 3” Nachricht empfangen wird. Es wurden Experimente mit längeren Aufzeichnungszeiten durchgeführt. Diese haben gezeigt, dass eine längere Aufzeichnungszeit bei schwachen Signalen eine Verbesserung bringt, da bei schwachen Signalen die Fehlerrate des `gsm-receiver` beim Decodieren der Daten ansteigt. In diesem Fall steigt mit längerer Aufzeichnungszeit die Wahrscheinlichkeit, ein “System Information Message Type 3” Paket vollständig zu decodieren.

Die Decodierung der empfangenen Daten erfolgt parallel zum Empfangen der Daten. Wird Kanal n empfangen, wird gleichzeitig Kanal n-1 decodiert. Diese Parallelisierung der beiden Vorgänge bringt einen Geschwindigkeitsgewinn von annähernd 50%, da das Empfangen und Decodieren der Daten nahezu gleich lange dauert. Bei der Parallelisierung der beiden Vorgänge musste darauf geachtet werden, dass die beiden Prozesse nicht gleichzeitig auf geteilte Ressource zugreifen, da hieraus inkonsistente Daten resultieren können. Um dies zu verhindern, wurden die geteilten Ressourcen mit einem Mutex² geschützt.

Nach dem Decodieren eines Kanals werden die gewonnenen Informationen in der Benutzeroberfläche angezeigt. Die sofortige Ausgabe der Daten hat den Vorteil, dass der Benutzer die Informationen direkt auswerten kann und nicht auf das Ende des Programmablaufs warten muss.

² Mutex: Verfahren zum Sicherstellen des wechselseitigen Ausschlusses.

5.4. Verbesserung der Scan-Geschwindigkeit

Um die Aktualisierungsrate der empfangenen BTS zu beschleunigen, werden im Folgenden zwei verschiedene Ansätze betrachtet. Ziel ist es, eine möglichst hohe Aktualisierungsrate zu erreichen, ohne dabei Basisstationen zu übersehen. Beim ersten Ansatz werden möglichst viele Kanäle gleichzeitig empfangen und parallel decodiert. Der zweite Ansatz versucht, die Kanäle herauszufiltern, die von Interesse sein könnten und nur diese zu betrachten.

5.4.1. Filterbank

Mithilfe des USRP2 kann ein 25 MHz breites Frequenzband empfangen werden. Bei einer GSM-Kanalbreite von 200 kHz ergeben sich daraus 125 GSM-Kanäle. Diese Daten zu empfangen und gleichzeitig zu verarbeiten ist nicht möglich, da sowohl das Trennen der Kanäle, als auch das Decodieren der GSM-Kanäle sehr rechenintensiv ist. Aus diesen Gründen wurden die Daten zwischengespeichert, um sie nach dem Empfangen weiter zu verarbeiten. Es stellte sich jedoch heraus, dass selbst das Abspeichern der Daten nicht ohne Weiteres möglich ist, da die Datenrate mit 200 MB/s zu hoch ist, um direkt auf die Festplatte geschrieben zu werden. Um das hohe Datenaufkommen zwischenzuspeichern, wurde eine RAM-Disk verwendet. Der folgende Befehl legt eine 300 MB große RAM-Disk im Verzeichnis ramdisk an:

```
sudo mount -t tmpfs -o size=300M tmpfs /ramdisk
```

Um einen ersten Eindruck von den empfangenen Daten zu erhalten, wurden diese mit dem Programm **baudline**³ dargestellt. In Abbildung 5.2 ist das komplette GSM900 Frequenzbande (935 MHz - 960 MHz) als Wasserfallplot in **baudline** abgebildet. Diese Darstellung veranschaulicht eindeutig, ob auf den einzelnen Kanälen Signale gesendet werden. Dabei sind die Signalstärken von schwach bis stark wie folgt farblich hervorgehoben: blau (schwach), grün, gelb, rot (stark)

Die zwischengespeicherten Daten müssen anschließend in einzelne GSM-Kanäle aufgeteilt werden, um diese zu decodieren. Das Aufsplitten übernimmt der Signalverarbeitungsblock **blk2.analysis_filterbank** von **gnuradio**. Die Filterbank unterliegt einigen Einschränkungen. Die Ausgangskanäle besitzen alle die gleiche Bandbreite und können nicht selektiert werden. Das bedeutet, dass es nicht möglich ist, nur Kanäle mit einer guten Signalstärke auszugeben. Dies hat zur Folge, dass auch Kanäle ohne Signal oder mit sehr schwachem Signal berechnet werden, wodurch wiederum der Rechenaufwand steigt. Eine weitere Einschränkung ergibt sich aus dem verwendeten Decoder von Airprobe. Dieser wurde ursprünglich für 500 kHz breite Eingangssignale entwickelt. Tests haben gezeigt, dass der Decoder erheblich weniger Daten decodieren kann, wenn die Eingangssignale eine Bandbreite kleiner als 400 kHz aufweisen. Um dieses Problem zu umgehen, wurden zwei Filterbänke verwendet, die jeweils 400 kHz breite Ausgangssignale liefern. Dies ist notwendig, da die Ausgangskanäle der Filterbank nicht überlappend sind und eine Filterbank mit 400 kHz breiten Ausgangssignalen somit nur 62 Ausgangskanäle besitzt. Das Eingangssignal der zweiten Filterbank wurde um 200 kHz verschoben, um die andere Hälfte der Kanäle zu erhalten. Dieses Verfahren wird in Abbildung 5.3 veranschaulicht. Der Decoder liefert mit 400 kHz und 500 kHz breiten Eingangssignalen gleich gute Ergebnisse.

Die im Folgenden aufgeführten Rechenzeiten beziehen sich auf das verwendete Setup aus Kapitel 6.2 auf Seite 54. Die Zeit zum Aufteilen der 125 Kanäle beträgt 30 Sekunden. Dabei wurde eine Aufzeichnung von der Dauer einer Sekunde aus dem EGSM900 Band verwendet. Das Decodieren eines einzelnen Kanals benötigt anschließend etwa 0,5 Sekunden, wenn keine Daten auf dem Kanal decodiert werden können, und 0,8 Sekunden, wenn Daten decodiert

³ baudline, <http://www.baudline.com> [Online; letzter Aufruf 16.04.2010]

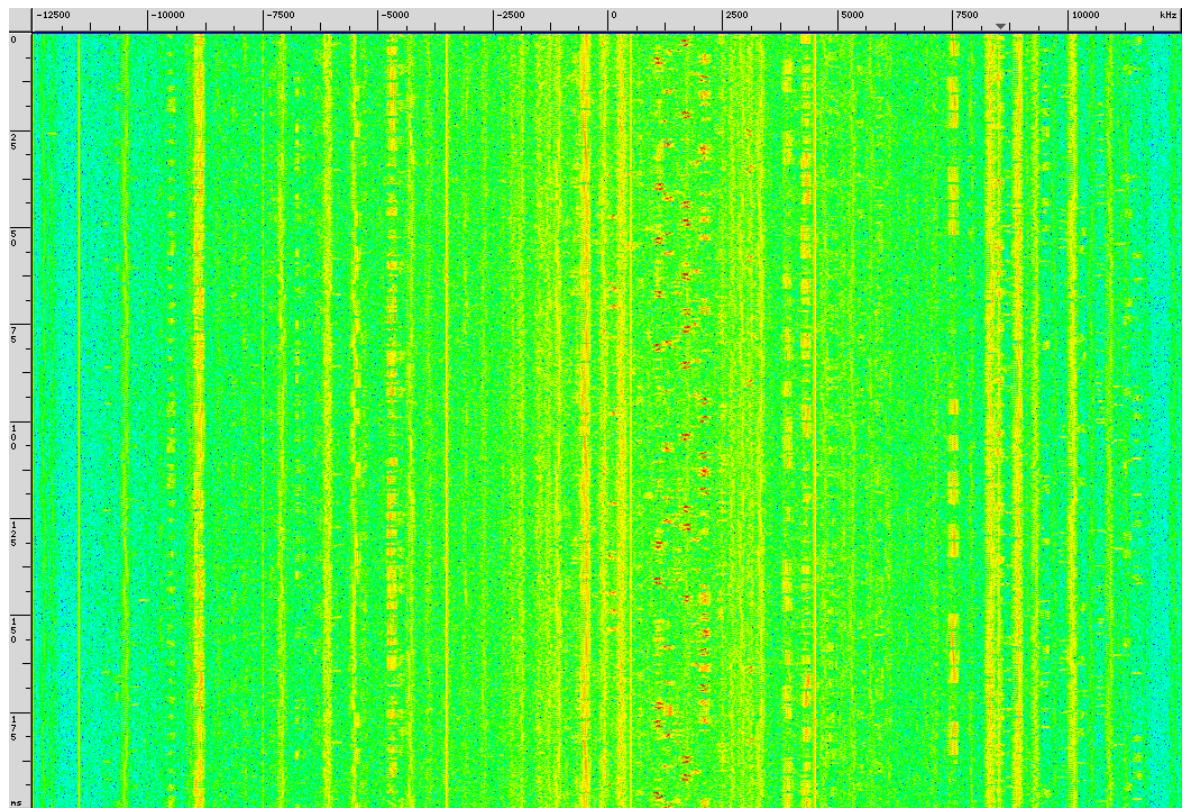


Abbildung 5.2.: Komplettes GSM900 Frequenzbank als Wasserfallplot;
X-Achse: ± 12.5 MHz; Y-Achse 200 ms, Mitte bei 947.5 MHz

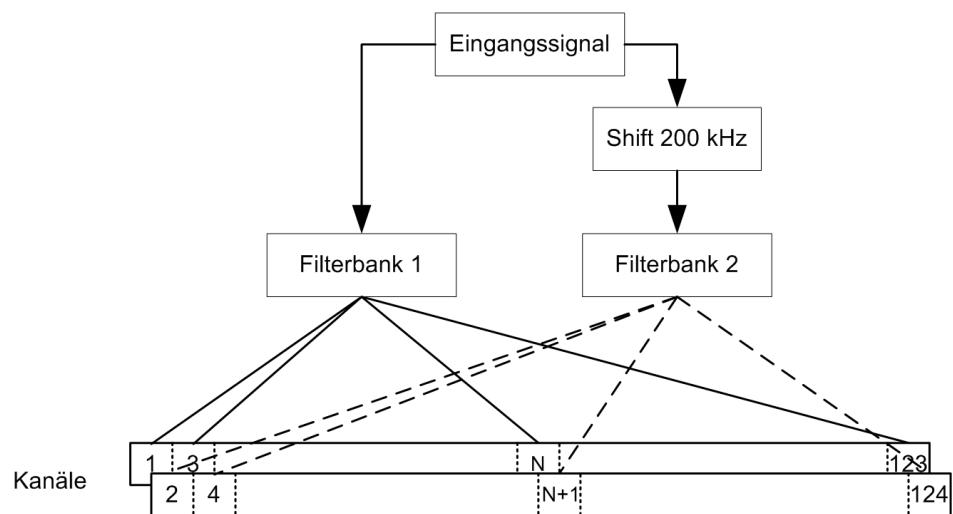


Abbildung 5.3.: Aufteilen der Kanäle mit einer Filterbank

werden.

Jeden einzelnen Kanal zu decodieren, würde bei 548 Kanälen und 25 gefundenen BTS 281,5 Sekunden beanspruchen ($523 * 0,5 + 25 * 0,8 = 281,5$). Eine Parallelisierung der Decodierung würde nur eine geringfügige Beschleunigung bringen, da die Decodierung in der verwendeten Version mehrere CPU Kerne auslastet. Der Filterbankansatz muss wegen des erheblichen Rechenaufwandes somit kritisch betrachtet werden. Um alle 548 Kanäle zu empfangen und anschließend zu trennen, muss mindestens fünf Mal ein 25 MHz breites Frequenzband durch den USRP2 empfangen und anschließend durch die Filterbank getrennt werden. Die Rechenzeit zum Trennen der Kanäle beträgt zusätzliche 150 Sekunden. Wegen der geschätzten Gesamtverarbeitungszeit von 431,5 Sekunden, wurde der Filterbankansatz nicht weiter verfolgt.

Bei diesem Ansatz ist die Geschwindigkeit abhängig von der Rechenleistung. Für aktuelle Computer ist die benötigte Rechenleistung zu hoch, jedoch ist er mit entsprechender Rechenleistung in Zukunft denkbar. Der wesentliche Vorteil ist hierbei, dass alle Kanäle betrachtet werden (vgl. erste Implementierung).

5.4.2. Kanäle mit guter Signalstärke

Da das Trennen aller Kanäle sehr rechenaufwändig ist und nur Kanäle mit einer ausreichenden Signalstärke auch decodiert werden können, liegt die Idee nahe, nur die Kanäle mit ausreichender Signalstärke zu betrachten. Dies erfordert für jeden Kanal eine Berechnung der Signalstärke.

Für jeden Kanal wurde ein “Signal to Noise Ratio” kurz SNR berechnet. Das SNR beschreibt das Verhältnis der mittleren Leistung des Nutzsignals zur mittleren Leistung des Rauschens. Zur Berechnung eines SNR müssen die folgenden Schritte betrachtet werden:

1. Eingangssignale in den Frequenzraum transformieren
2. Signalstärke für das Rauschen bestimmen
3. Gefundene Signale ins Verhältnis zum Rauschen setzen

Frequenzspektrum berechnen

Für die Berechnung des Frequenzspektrums wurde der GNU Radio Signalverarbeitungsblock `gr.fft_vcc` verwendet. Der Signalverarbeitungsblock realisiert die schnelle Fourier-Transformation und ermöglicht es, die Amplitude der einzelnen Frequenzanteile des Frequenzspektrums zu berechnen. Für jeden GSM-Kanal wurden zehn FFT-Bins⁴ gewählt. Somit ergibt sich eine Auflösung von 1250 für die Fourier-Transformation.

Das berechnete Frequenzspektrum wird anschließend genutzt, um die Signalstärke jedes einzelnen Kanals zu bestimmen. Dabei muss jedoch beachtet werden, dass die Signalstärke des Frequenzspektrums eine Nichtlinearität aufweist. Der Ausgleich der Nichtlinearität ist wichtig, da andernfalls die Signalstärke der Kanäle in den Randbereichen falsch berechnet würde. Die Nichtlinearität der Signale ist auf die Signalverarbeitung im USRP2 durch den FPGA sowie auf die Empfangscharakteristik des DBSRX Daughterboards zurückzuführen. In Abbildung 5.4 ist das Frequenzspektrum von Rauschen mit und ohne den Ausgleich der Nichtlinearität zu sehen.

Der Ausgleich erfolgt über eine Addition der fehlenden Signalpegel und kann nur für das beschriebene Setup genutzt werden, da die Nichtlinearität von den verwendeten Komponenten abhängt. Ein Beispiel für ein berechnetes Frequenzspektrum ist in Abbildung 5.5 gegeben.

⁴FFT-Bin: Datenpunkt eines Frequenzspektrums. Alle FFT-Bins zusammen ergeben die Auflösung des Frequenzspektrums.

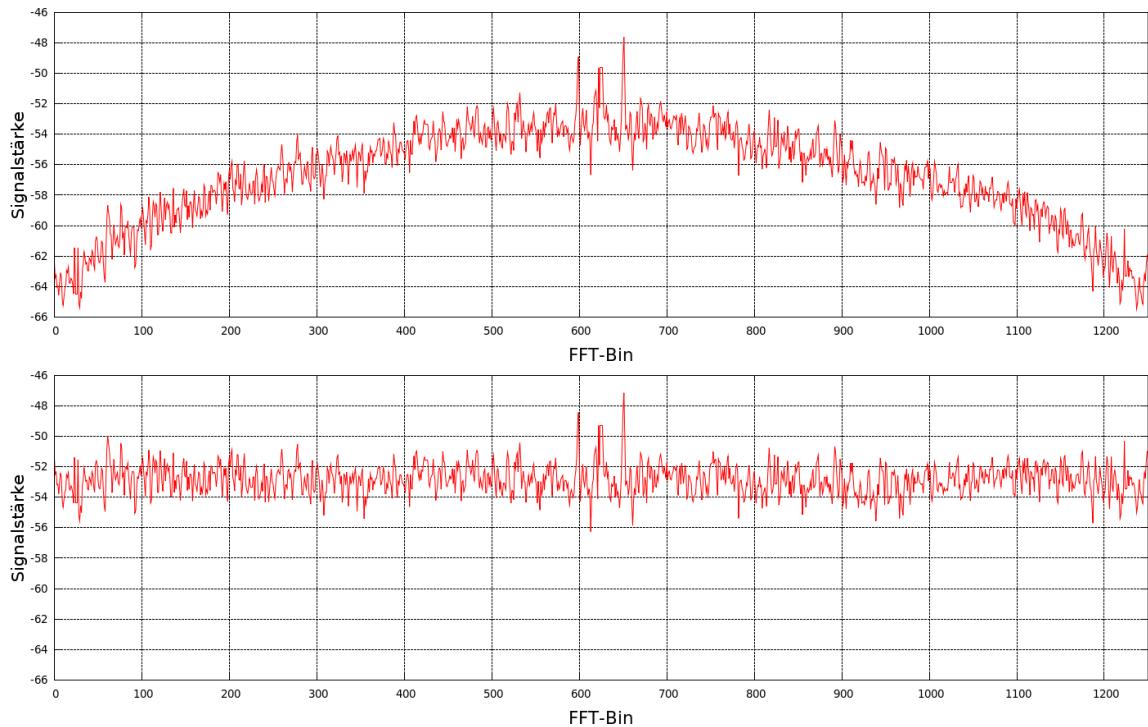


Abbildung 5.4.: Frequenzspektrum des Rauschens ohne Ausgleich der Nichtlinearität (oben) und mit Ausgleich (unten)

Signalstärke für das Rauschen schätzen

Für die Berechnung des Verhältnisses zwischen der Leistung des Nutzsignals und der Leistung des Rauschens ist es notwendig zuerst einen Leistungswert für das Rauschen zu bestimmen. Um dies zu erreichen, müssen die Kanäle mit Signal von den Kanälen ohne Signal getrennt werden. Anschließend kann über alle Kanäle ohne Signal gemittelt werden, um eine Schätzung des Leistungswertes für das Rauschen zu erhalten. Die Leistung des Rauschens wird anschließend ins Verhältnis zu den Kanälen mit Signalen gesetzt. Der folgende Programmablauf fasst die Schritte zusammen:

1. $K = \text{Menge aller FFT-Bins}$
2. Berechne Mittelwert m über K
3. Vergleiche Signalstärke jedes FFT-Bins aus K mit m
 - 3.1 falls Signalstärke kleiner: den Kanal der Menge R hinzufügen
4. Berechne Mittelwert m_2 über alle Kanäle aus R
 $m_2 = \text{Signalstärke des Rauschens}$

Der Algorithmus zur Berechnung des SNR geht davon aus, dass nicht auf allen Kanälen Signale gesendet werden. Wäre dies der Fall würde die Berechnung des SNR schwache Signale als Rauschen identifizieren. Tests haben jedoch gezeigt, dass nur auf einem kleinen Anteil der Kanäle eine BTS mit konstanter Energie sendet.

In Abbildung 5.5 ist das Frequenzspektrum des GSM900 Bandes dargestellt. Der Mittelwert über alle Kanäle ist als grüne horizontale Linie zu sehen. Der berechnete Rauschwert ist als blaue Linie dargestellt. Es ist zu sehen, dass die berechnete Leistung für das Rauschen nicht mit dem korrekten Leistungswert für das Rauschen übereinstimmt. Der berechnete Wert liegt zu hoch. Dies hat jedoch keine negativen Auswirkungen, da der korrekte Rauschwert sich nur um eine Konstante vom berechneten Wert unterscheidet.

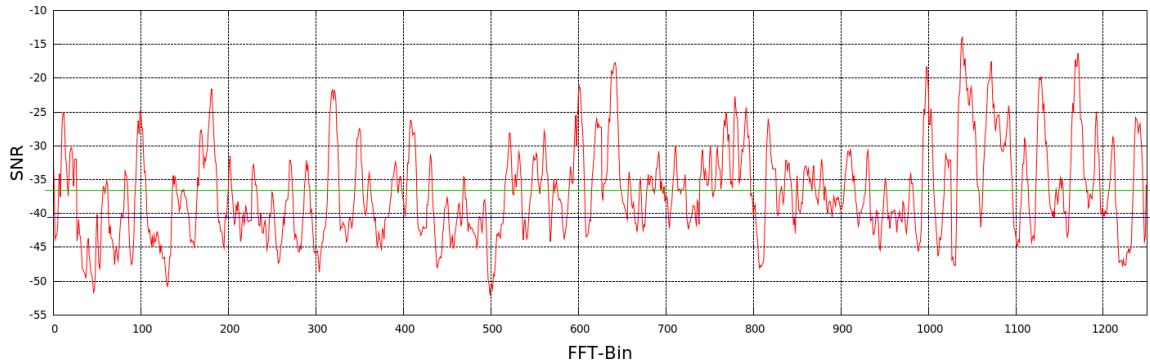


Abbildung 5.5.: GSM900 Frequenzspektrum mit Mittelwert (grün) und Rauschwert (blau)

SNR berechnen

Zur Berechnung des SNR wird neben einer Signalstärke für das Rauschen eine Signalstärke für jeden der 125 GSM-Kanäle benötigt. Jeder GSM-Kanal wird durch 10 FFT-Bins repräsentiert. Für die Berechnung der Signalstärke werden nur die sechs FFT-Bins aus der Mitte eines jeden Kanals betrachtet, da ein starkes Signal auf einem GSM-Kanal die Berechnung der Signalstärke auf dem Nachbarkanal beeinflussen kann. Aus diesem Grund werden die beiden äußeren FFT-Bins verworfen. Das Ergebnis der SNR Berechnung ist in Abbildung 5.6 abgebildet. In der Abbildung ist die für jeden Kanal berechnete Signalstärke zu sehen.

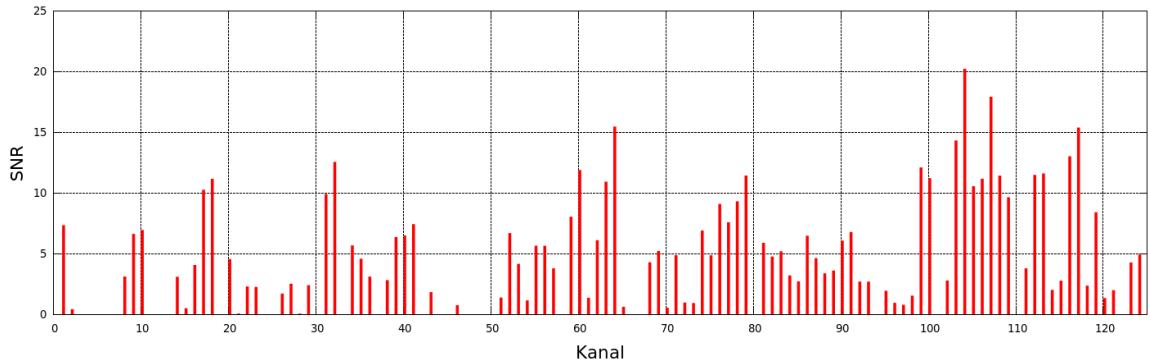


Abbildung 5.6.: Ergebnis der SNR-Berechnung im EGSM900-Band für 125 GSM-Kanäle

Um zu überprüfen, ob die berechnete Signalstärke stabile Werte über die Zeit liefert, wurden insgesamt 100 Messungen eines GSM-Kanals durchgeführt. Die Ergebnisse sind in Abbildung 5.7 gezeigt. Der Mittelwert über alle Messungen beträgt 5,98 und ist in der Abbildung eingezeichnet. Die Standardabweichung beträgt 0,39 und die maximale Abweichung 1,3. Der berechnete SNR ist somit ausreichend stabil.

5.5. Zweite Implementierung

Die in Kapitel 5.4.2 beschriebenen Schritte wurden in einem C++ Programm umgesetzt. Dabei wurde der **GSM-Scanner** der ersten Implementierung als Grundlage verwendet.

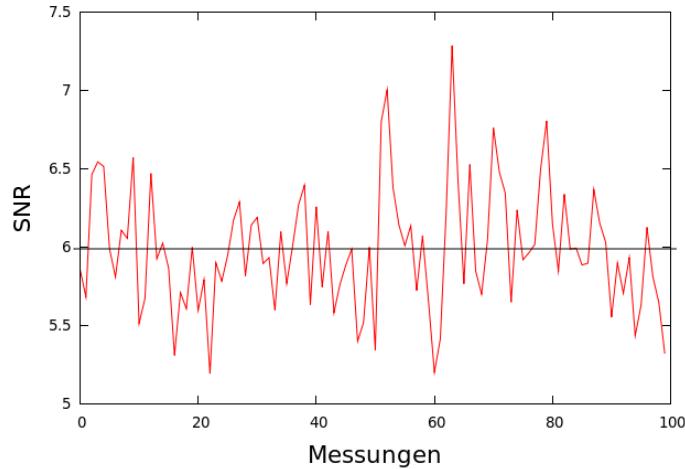


Abbildung 5.7.: Stabilität des berechneten SNR-Wertes mit Mittelwert.

5.5.1. Programmablauf

Der folgende Programmablauf beschreibt die Umsetzung des Programms:

1. SNR für jeden GSM-Kanal bestimmen
2. Menge M potenzieller BTS bestimmen
3. Alle BTS in M empfangen und decodieren
4. Gefundene BTS als Menge B speichern

5. SNR für jeden GSM-Kanal bestimmen
 - 5.1 Signalstärken bei B aktualisieren
 - 5.2 Menge M potenzieller BTS bestimmen
 - 5.3 $M' = M \setminus B$
6. M' empfangen und decodieren
7. Gefundene BTS zu B hinzufügen
8. Springe zu 5.

Das entwickelte Programm besteht aus zwei Phasen. In der ersten Phase ist die Liste der empfangenen BTS leer und alle Kanäle mit ausreichender Signalstärke werden empfangen und decodiert. Die Menge potenzieller BTS wird über einen SNR-Schwellwert definiert. Gefundene BTS werden direkt nach dem Decodieren in der Benutzeroberfläche angezeigt.

In der zweiten Phase werden die empfangenen BTS aus der Menge der Kanäle mit ausreichender Signalstärke herausgenommen. Dieser Schritt beschleunigt den zweiten Durchlauf. Kanäle, die im ersten Durchlauf nicht decodiert werden konnten, werden im zweiten Durchlauf wiederholt betrachtet. Ein wiederholtes Betrachten der Kanäle ist aufgrund der in Kapitel 5.2 beschriebenen Probleme mit dem `gsm-receiver` notwendig.

Die zweite Phase wird beliebig oft wiederholt und zusätzlich gefundene BTS werden in der Benutzeroberfläche ergänzt.

5.5.2. Benutzeroberfläche

Um die Daten übersichtlich darzustellen, wurde eine graphische Oberfläche entwickelt. Die Oberfläche ist in Abbildung 5.8 dargestellt. Die von den Basisstationen empfangenen Informationen werden in der Benutzeroberfläche tabellarisch aufgelistet. Dabei lässt sich die Tabelle über jede Spalte sortieren, um den Inhalt den Benutzerwünschen entsprechend auszugeben.

5. GSM-Scanner

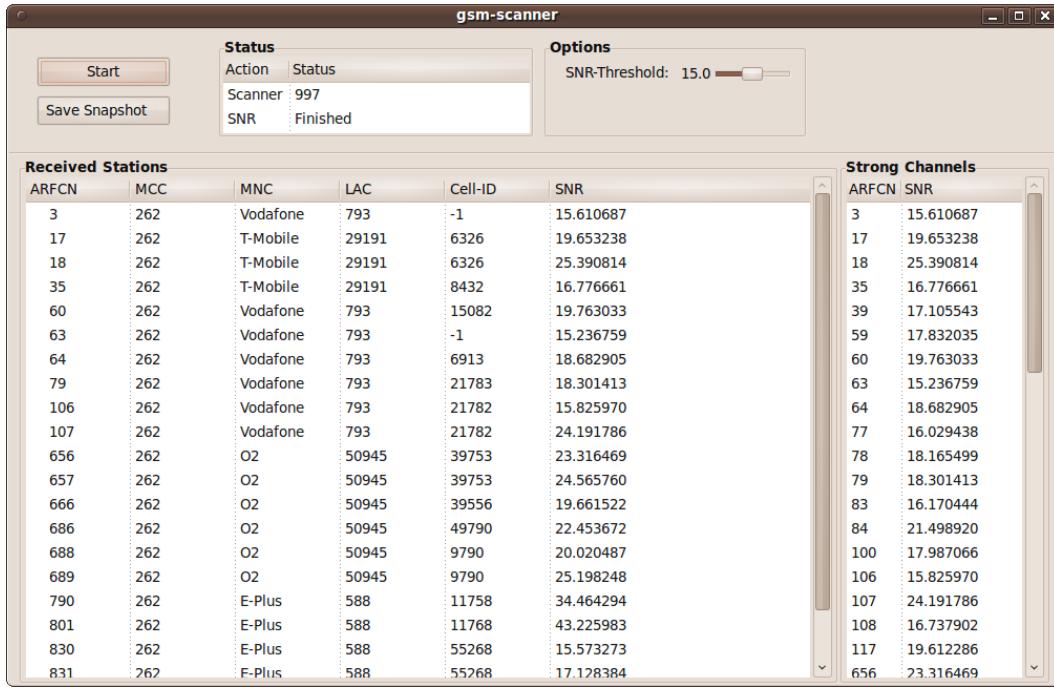


Abbildung 5.8.: Benutzeroberfläche des GSM-Scanners

Die gesamte Tabelle kann über die Schaltfläche "Save Snapshot" in einer Textdatei im CSV-Format gespeichert werden. Eine Beispieldatei ist in Anhang C gegeben. Der Status des Scanners wird in der Benutzeroberfläche oben mittig angezeigt. Dabei wird der Kanal angezeigt, der gerade über den USRP2 empfangen wird, sowie der Status der SNR-Bestimmung. Das Ergebnis der SNR-Bestimmung wird in der Tabelle rechts dargestellt. Die Tabelle enthält alle Kanäle, deren Signalstärke besser als der eingestellte Schwellwert ist. Der Schwellwert für die SNR-Bestimmung kann über einen Schieberegler in den Optionen eingestellt werden. Der Scan-Vorgang wird über eine Start/Stop Schaltfläche gestartet oder unterbrochen.

5.5.3. Die empfangenen Daten

Die empfangenen Daten des entwickelten **GSM-Scanners** wurden daraufhin überprüft, ob der berechnete SNR ein guter Indikator für eine Basisstation darstellt.

In Tabelle 5.2 sind die durch das entwickelte Programm gefundenen BTS aufgelistet. Die Tabelle ist nach der Kanalnummer sortiert und enthält die Informationen MCC, MNC, LAC, Cell-ID sowie das berechnete SNR. Die Informationen wurden im Rechenzentrum der Universität Freiburg (Hermann-Herder-Str. 10; 79104 Freiburg) aufgenommen. Die in Kapitel 5.2 beschriebenen Probleme mit dem GSM-Receiver wurden beim Erstellen der Tabelle umgangen, indem mehrere Scan-Durchläufe zusammengefasst wurden. Somit konnte verhindert werden, dass sich die Probleme mit dem GSM-Receiver auf die erhaltenen Ergebnisse auswirken.

5.5.4. Analyse des SNR-Schwellwertes

Wie der Tabelle 5.2 entnommen werden kann, wurde keine BTS mit einem SNR kleiner 5 empfangen. Ein SNR von 5 ist somit Voraussetzung dafür, dass die empfangenen Signale durch den **gsm-receiver** decodiert werden können.

ARFCN	MCC	MNC	LAC	CID	SNR
1	262	Vodafone	793	15081	12.6076
2	262	Vodafone	793	19232	8.5364
10	262	Vodafone	793	9601	11.5646
18	262	T-Mobile	29191	6326	18.5044
35	262	T-Mobile	29191	8432	10.5497
41	262	T-Mobile	29191	47562	5.22143
57	262	Vodafone	793	4901	10.7978
60	262	Vodafone	793	15082	13.0892
64	262	Vodafone	793	6913	14.0305
77	262	Vodafone	793	20483	10.3105
78	262	Vodafone	793	19771	10.4384
79	262	Vodafone	793	21783	9.46275
100	262	T-Mobile	29191	16023	12.7119
104	262	Vodafone	793	58641	16.0155
107	262	Vodafone	793	21782	20.6841
108	262	Vodafone	793	21751	13.0799
109	262	Vodafone	793	21721	8.61312
113	262	Vodafone	793	20482	13.7537
659	262	O ₂	50945	19753	9.06804
665	262	O ₂	50945	39556	15.128
685	262	O ₂	50945	49790	19.8975
686	262	O ₂	50945	39753	28.6561
688	262	O ₂	50945	9790	23.5985
694	262	O ₂	50945	29804	9.04963
789	262	E-Plus	588	11758	28.59
800	262	E-Plus	588	11768	30.3136
830	262	E-Plus	588	55268	10.2142
838	262	E-Plus	588	36658	8.77891
848	262	E-Plus	588	32988	12.9886
852	262	E-Plus	588	32978	5.44955
860	262	E-Plus	588	7108	6.3782
984	262	E-Plus	588	8158	8.34599
997	262	E-Plus	588	55248	21.3123
1012	262	O ₂	50945	41218	9.28821

Tabelle 5.2.: Durch den GSM-Scanner gefundene BTS

Auswirkung des SNR-Schwellwertes auf die Scan-Geschwindigkeit

Die Wahl des SNR-Schwellwertes hat Auswirkungen auf die Geschwindigkeit des Scanners, da die Anzahl der Kanäle, die betrachtet werden, vom SNR-Schwellwert abhängt. In Abbildung 5.9 ist der Zusammenhang zwischen Zeit und SNR-Schwellwert gegeben. Es ist deutlich zu erkennen, dass die Zeit für einen kompletten Scan-Vorgang bei kleiner werdendem SNR-Schwellwert stark ansteigt.

Die Scan-Geschwindigkeit hängt direkt von der Anzahl betrachteter Kanäle ab. Abbildung 5.10 zeigt das Verhältnis zwischen der Anzahl der betrachteten Kanäle und der Kanäle mit einer gefundenen BTS in Abhängigkeit vom gewählten SNR. Die Grafik zeigt deutlich, dass bei einem niedrigen SNR wesentlich mehr Kanäle betrachtet werden müssen, um eine BTS

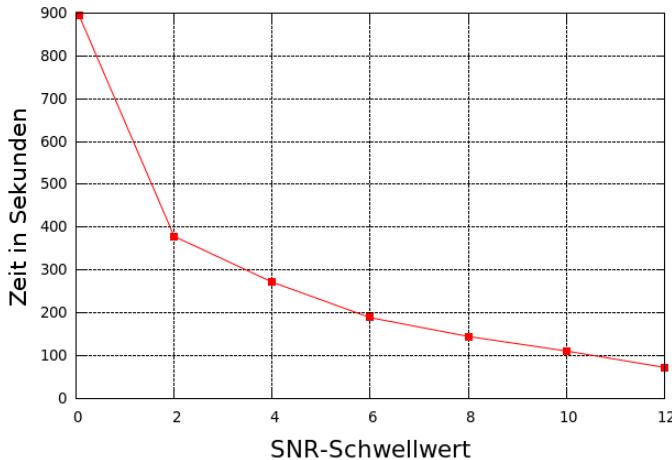


Abbildung 5.9.: Scan-Geschwindigkeit bei verschiedenen SNR-Schwellwerten

zu finden als bei einem höheren SNR. Bei einem SNR von 8 müssen für jede gefundene BTS dreimal so viele Kanäle betrachtet werden. Ab einem SNR von 8 ändert sich das Verhältnis nur noch geringfügig.

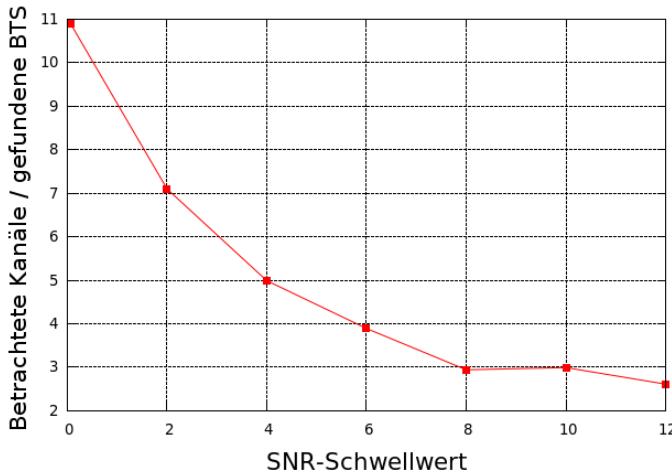


Abbildung 5.10.: Verhältnis zwischen betrachteten Kanälen und gefundenen BTS bei steigendem SNR

Es gibt zwei Gründe warum Kanäle eine gute Signalstärke aufweisen, jedoch keine BCCH Informationen empfangen werden können:

1. Starke Signale auf einem Kanal beeinflussen die Signalstärke auf den Nachbarkanälen.
Es wurde versucht diesen Effekt bei der Bestimmung der Signalstärke zu minimieren, er konnte jedoch nicht vollständig beseitigt werden.
2. Auf dem Kanal wird kein BCCH gesendet. Dies ist der Fall, wenn durch eine BTS mehr als eine Frequenz genutzt wird und nur auf einer Frequenz ein BCCH gesendet wird. Auf den weiteren Frequenzen werden bei aktiven Verbindungen zwischen einer BTS und MS Signale gesendet. Die aktiven Verbindungen zwischen BTS und MS sind in Abbildung 5.2 auf Seite 39 als kurze Impulse auf einem Kanal zu sehen.

Auswirkung des SNR-Schwellwertes auf die Anzahl gefundener BTS

Mit steigendem SNR-Schwellwert wächst die Wahrscheinlichkeit, dass schwache BTS übersehen werden. Dieser Zusammenhang wird in Abbildung 5.11 veranschaulicht. Die Abbildung zeigt die Anzahl gefundener BTS zusammen mit unterschiedlichen SNR-Schwellwerten. Es ist deutlich zu sehen, dass mit steigendem Schwellwert die Anzahl der gefundenen BTS sinkt. Beispielsweise werden bei einem SNR-Schwellwert von 10 insgesamt 23 BTS gefunden. Alle BTS mit einem SNR kleiner als 10 werden nicht betrachtet. Dies führt dazu, dass im Vergleich zu einem SNR-Schwellwert von acht 8 BTS weniger gefunden werden.

Der geringe Abfall gefundener BTS bei einem Schwellwert kleiner 8, ist darauf zurückzuführen, dass BTS-Signale nur dann decodiert werden können, wenn die Signalstärke mindestens einen SNR-Wert von 6-8 hat.

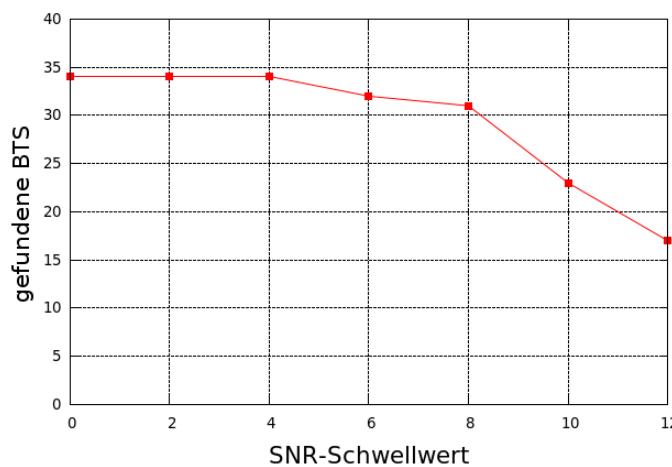


Abbildung 5.11.: Anzahl der gefundenen BTS bei verschiedenen SNR-Schwellwerten

5.6. Vergleich der empfangenen Daten mit dem Nokia 3310

Die Ergebnisse des GSM-Scanners wurden mit dem Mobilfunktelefon Nokia 3310 verglichen. Das Nokia 3310 zeigt mit aktivem Netzmonitor die Nachbarschaftsliste im Display. In Tabelle 5.3, 5.4, 5.5 und 5.6 sind die empfangenen Zellen und ihre Signalstärken aufgelistet. Für jede Liste musste das Nokia 3310 mit einer SIM-Karte des jeweiligen Anbieters ausgestattet werden, da nur die Zellinformationen eines Anbieters vom Mobilfunktelefon angezeigt werden. Das Nokia 3310 betrachtet im Gegensatz zum entwickelten GSM-Scanner nur die Nachbarschaftslisten, die es über die Zelle empfängt, in die es gerade eingebucht ist. Das Mobilfunktelefon sucht nur dann im gesamten Frequenzband, wenn es keine BTS in der Nachbarschaftsliste mit ausreichender Signalstärke empfängt.

Das Mobilfunktelefon Nokia 3310 sieht weniger BTS als der entwickelte GSM-Scanner, da sich die Sicht des Nokia 3310 immer auf ein Mobilfunknetz eines Anbieters beschränkt. Jedoch sieht das Mobilfunktelefon auch Basisstationen, die über den GSM-Scanner nicht gefunden werden. Gerade im Mobilfunknetz von T-Mobile sieht das Mobilfunktelefon wesentlich mehr BTS als der GSM-Scanner. Der Grund, warum im T-Mobile Netz weniger BTS durch den GSM-Scanner gefunden werden, liegt an den schlechten Signalstärken der BTS. Im Mobilfunknetz von Vodafone wurden alle BTS gefunden. Im Netz von E-Plus wurde nur die BTS mit der schlechtesten Signalstärke nicht gefunden und im Netz von O2 wurden drei von sieben BTS gefunden.

Kanal	Signalstärke
57	-83
60	-91
64	-75
78	-83
104	-75
107	-88
108	-84
113	-88

Kanal	Signalstärke
14	-92
18	-77
27	-95
47	-100
82	-91
89	-91
91	-96
93	-88
100	-83
124	-89

Tabelle 5.3.: Zellübersicht Vodafone

Tabelle 5.4.: Zellübersicht T-Mobile

Kanal	Signalstärke
656	-81
659	-83
679	-96
685	-79
688	-83
693	-84
717	-48

Kanal	Signalstärke
789	-64
800	-63
830	-83
838	-86
984	-64
995	-86
997	-72

Tabelle 5.5.: Zellübersicht O₂

Tabelle 5.6.: Zellübersicht E-Plus

Der Vergleich der Ergebnisse zeigt, dass die Empfangsempfindlichkeit des Nokia 3310 wesentlich höher ist, als die des USRP2. BTS mit einer Signalstärke schwächer als -86 dBm werden durch den GSM-Scanner nicht gefunden. Der Grund für die höhere Empfindlichkeit des Mobilfunktelefons ist die jahrelange Optimierung der verwendeten Komponenten für den Empfang von GSM-Signalen. Das USRP2 hingegen wurde nicht ausschließlich für den Empfang von GSM-Signalen optimiert.

Eine Erklärung, warum der **GSM-Scanner** BTS findet, die dem Nokia 3310 verborgen bleiben, folgt mit der Betrachtung der Signalstärke im folgenden Abschnitt.

Vergleich der empfangenen Signalstärke

Die Signalstärken des 3310 und des GSM-Scanners lassen sich nicht direkt vergleichen, da sie unterschiedliche Einheiten besitzen. Die Signalstärken, die durch das Nokia 3310 ausgegeben werden, sind in dBm⁵ angegeben. Für einen exakten Vergleich der Signalstärken müssten die SNR-Werte des GSM-Scanners kalibriert werden. Eine Kalibrierung konnte allerdings nicht vorgenommen werden, da die notwendige Kalibrierungsausrüstung nicht verfügbar war. Die gewonnenen Signalstärken können aber über eine Sortierung verglichen werden. Dabei wurde erwartet, dass die Sortierung der SNR-Werte eine ähnliche Reihenfolge ergibt, wie die Sortierung über die Signalstärken des Nokia 3310. In Tabelle 5.7 sind die Signalstärken des GSM-Scanners und des Nokia 3310 gegenübergestellt. Die Tabelle ist nach den Signalstärken des GSM-Scanners sortiert. Wie der Tabelle 5.7 entnommen werden kann, ist die Reihenfolge der Kanäle mit höchster Signalstärke beim Nokia 3310 nicht identisch mit den SNR des GSM-Scanners. Die Messungen des Nokia 3310 bei Kanal 107 und 113 unterscheiden sich von den

⁵ dBm: Leistungspegel mit der Bezugsgröße 1 mW (0 dBm ≡ 1mW)

ARFCN	SNR GSM-Scanner	dBm 3310
107	20,68	-88
104	16,02	-75
64	14,03	-75
113	13,75	-88
60	13,09	-79
108	13,08	-84
1	12,61	
10	11,56	
57	10,79	-83
78	10,44	-83
77	10,31	
79	9,46	
109	8,61	
2	8,54	

Tabelle 5.7.: Vergleich der Signalstärken von GSM-Scanner und Nokia 3310 im Vodafone Netz

SNR-Messungen des GSM-Scanners. Ein eindeutiger Grund für die Abweichung konnte nicht gefunden werden. Möglich ist, dass durch die kleinere Antenne des Nokia 3310 der Empfang der beiden Kanäle ungünstig war.

Die Kanäle 77, 79, 109 und 2 wurden vom 3310 nicht in der Nachbarschaftsliste angezeigt, da die Signalstärke im Vergleich zu den anderen Kanälen zu schwach ist und nur die Kanäle mit den besten Signalstärken ausgegeben werden. Die Ausgabe des 3310 ist beschränkt auf die Kanäle mit der besten Signalstärke, auch wenn das Mobilfunktelefon in der Lage wäre, Kanäle mit schwacher Signalstärke zu empfangen.

Bei Kanal 1 und 10 war zuerst unklar, warum diese nicht betrachtet werden. Eine Analyse der Nachbarschaftslisten zeigt, dass Kanal 10 in keiner der anderen Nachbarschaftslisten eingetragen war. Abbildung 5.12 verdeutlicht die Zusammenhänge zwischen den Nachbarschaftslisten im Vodafone Mobilfunknetz.

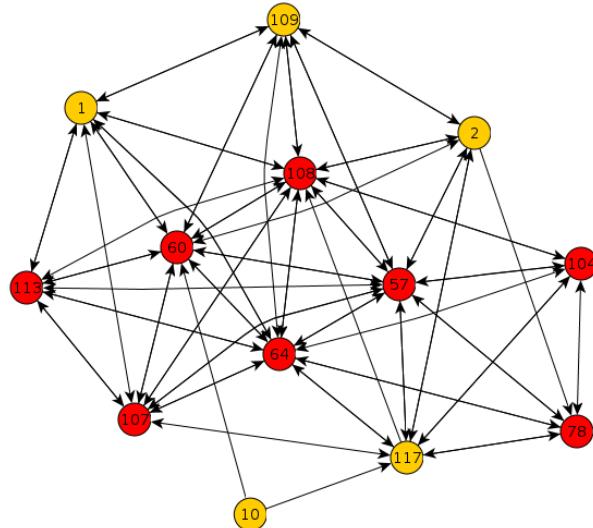


Abbildung 5.12.: Visualisierung der Nachbarschaftsliste im Vodafone GSM-Netz

5. GSM-Scanner

Die Kanäle, die vom 3310 als Nachbarschaftsliste ausgegeben werden, sind in der Abbildung rot hervorgehoben. Je nachdem welche Nachbarschaftsliste aktuell betrachtet wird, ist Kanal 1 ebenfalls dem Mobilfunktelefon nicht bekannt. Dies kann beispielsweise geschehen, wenn die Nachbarschaftsliste von Kanal 104 betrachtet wird.

Die Visualisierung der Nachbarschaftslisten in Abbildung 5.12 zeigt, dass die Einträge in den Nachbarschaftslisten nicht immer eine bidirektionale Verknüpfung darstellen. Ein Beispiel hierfür ist die Kante zwischen 2 und 78. Die Grafik gibt nicht die reale geographische Position der Basisstationen wieder. Jedoch könnten die Positionen der Basisstationen über die Kombination von weiteren Nachbarschaftslisten geschätzt werden. Dies impliziert jedoch die Annahme, die Nachbarschaftslisten ließen einen Rückschluss auf die tatsächliche Position zu. Diese Vermutung müsste durch weitere Untersuchungen gestützt oder widerlegt werden.

6. Lokalisierung mittels GSM

Für einen Nutzer mobiler Dienste kann es in bestimmten Situationen von Interesse sein, die eigene Position zu bestimmen. Hierfür wird meistens GPS verwendet, jedoch benötigt dies zusätzlichen Strom. Dadurch verkürzt sich die Standbyzeit des Mobilfunktelefons stark. Auch ist eine Positionsbestimmung über GPS nicht in jeder Situation möglich. In Gebäuden oder Häuserschluchten können GPS-Signale nur eingeschränkt empfangen werden. GSM-Signale hingegen können typischerweise auch in Gebäuden empfangen werden.

Für eine Selbstlokalisierung des Mobilfunktelefons ist es wünschenswert, keine Modifikationen an der Hardware des Mobilfunktelefons vornehmen zu müssen. Veränderungen am Mobilfunknetzwerk sind für die Betreiber oftmals kostspielig und deswegen nach Möglichkeit ebenso zu vermeiden.

Beide Anforderungen werden vom Fingerprinting-Verfahren erfüllt. Das Verfahren wird bei der WLAN-Lokalisierung erfolgreich eingesetzt und wird in der Arbeit "Place Lab" von LaMarca et al. 2005 ausführlich beschrieben [21]. Das WLAN-Fingerprinting Verfahren wird mittlerweile u.a. von der Firma Skyhook Wireless¹ als kommerzielles Software-Modul angeboten. Hierbei werden die von WLAN Access-Points gesendeten eindeutigen Kennungen verwendet, um den aktuellen Aufenthaltsort zu charakterisieren. Das Fingerprinting-Verfahren besteht aus zwei Schritten:

1. Erstellen einer Fingerprint-Datenbank:

In diesem Schritt wird ein Gebiet abgefahren. In regelmäßigen Zeitabständen werden die aktuell sichtbaren Funkzellen zusammen mit einer Referenzposition in einer Datenbank abgelegt. Für die Referenzposition wird meist ein GPS-Empfänger verwendet.

2. Positionsbestimmung mit Hilfe der Datenbank:

Im zweiten Schritt wird die aktuelle Position mit Hilfe der Datenbank berechnet. Die empfangenen Funkzellen werden als Lookup-Datensatz gespeichert und mit den in der Datenbank gespeicherten Informationen verglichen. Dabei wird aus den Informationen die aktuelle Position extrahiert.

Das Verfahren kann auch für die Lokalisierung über GSM verwendet werden, da bei GSM wie auch bei WLAN von jeder Funkzelle Broadcast-Informationen gesendet werden, die die Zelle eindeutig identifizieren. Jedes Mobilfunktelefon misst ständig die Signalstärken zu den Basistationen in der Umgebung und verfügt somit über einen Datensatz, der für eine Lokalisierung verwendet werden kann.

Jedoch können die für die Lokalisierung benötigten Daten bei den meisten aktuellen Mobilfunktelefonen nicht ausgelesen werden. Aus diesem Grund wird für die Lokalisierung in diesem Kapitel das USRP2 verwendet.

In diesem Kapitel wird untersucht, ob die durch den **GSM-Scanner** gewonnenen Informationen zur Lokalisierung verwendet werden können. Dabei soll überprüft werden, ob die Informationen, die eine BTS eindeutig identifizieren, ausreichen, um den aktuellen Aufenthaltsort zu charakterisieren. Dies soll in einem praktischen Versuchsaufbau getestet werden. Hierbei soll

¹Skyhook Wireless, <http://www.skyhookwireless.com> [Online; letzter Aufruf 26.03.2010]

6. Lokalisierung mittels GSM

berücksichtigt werden, ob bei der Betrachtung mehrerer Basisstationen die aktuelle Position treffender charakterisiert wird.

Um die mit dem **GSM-Scanner** gewonnenen Daten aufzuzeichnen, musste dieser angepasst werden. Die notwendigen Modifikationen werden in Kapitel 6.1 erläutert. Im anschließenden Kapitel 6.2 wird der Versuchsaufbau zum Aufzeichnen der benötigten Daten beschrieben.

6.1. Software

Die Zellinformationen zur Lokalisierung sollen periodisch in einer Ausgabedatei abgelegt werden. Hierfür wurde der **GSM-Scanner** um eine Aufzeichnungsfunktion erweitert, die über die Optionsschaltfläche "Logg Data to XML-File" aktiviert werden kann.

Zum Erstellen einer Datenbank für die Lokalisierung, wird eine GPS-Position als Referenzposition benötigt. Um die anschließende Verarbeitung der Daten zu erleichtern, wurden die durch das angeschlossene GPS empfangenen Koordinaten an den **GSM-Scanner** weitergereicht. Diese werden in der neuen Oberfläche unter den Statusoptionen angezeigt. Die GPS-Schnittstelle kann über eine Optionsschaltfläche aktiviert und deaktiviert werden.

Die erweiterte Oberfläche des **GSM-Scanners** ist in Abbildung 6.1 zu sehen.

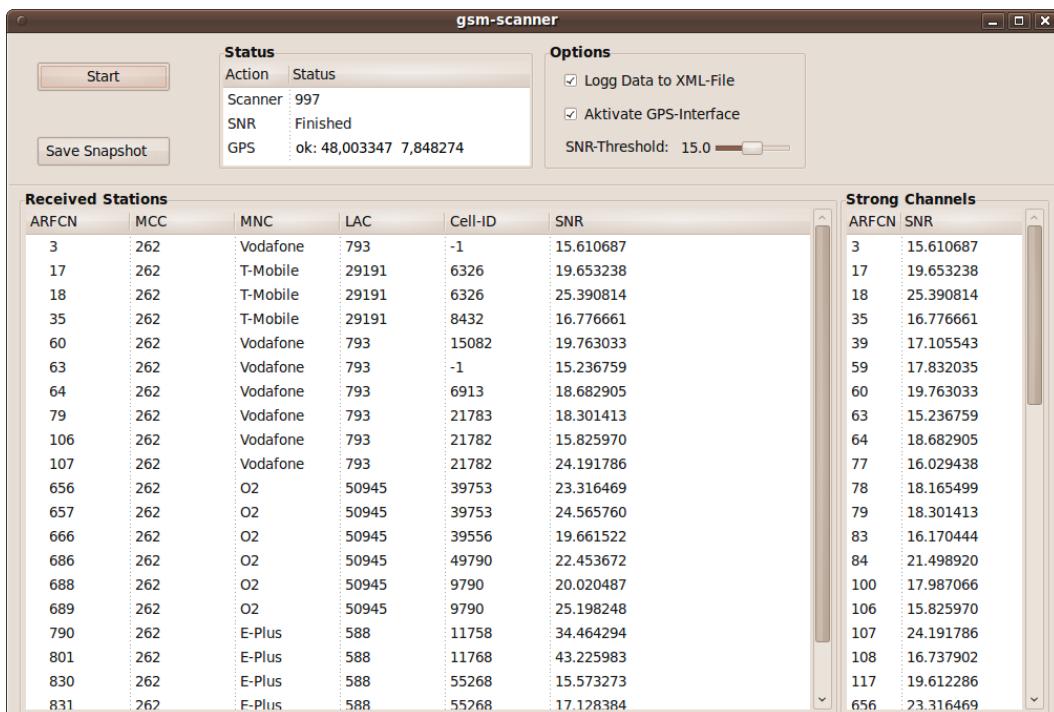


Abbildung 6.1.: Erweiterte Benutzeroberfläche des GSM-Scanners zum Erstellen der Datensätze

Der **GSM-Scanner** sucht alle 30 Sekunden nach neuen Signalen, indem er die Signalstärken auf allen Kanälen von EGSM900 und GSM1800 überprüft. Die gewählte Zeit ist ein Kompromiss zwischen schneller Aktualisierungsrate und einer möglichst langen Zeit zum Betrachten neuer Kanäle mit dem Ziel, keine BTS zu übersehen. Direkt nach dem Bestimmen der Signalstärken werden die aktuell in der Benutzeroberfläche angezeigten BTS in die Ausgabedatei geschrieben. Das Bestimmen der Signalstärke dauert 5 Sekunden. Die restliche Zeit werden die Kanäle mit einer Signalstärke über dem SNR-Schwellwert empfangen und decodiert. BTS mit schwacher Signalstärke werden gelöscht, wenn der halbe SNR-Schwellwert dreimal in Folge unterschritten wurde. Dies verhindert, dass Datensätze gelöscht werden, die beim Bestimmen

der Signalstärke kurzzeitig einen schlechten Empfang aufweisen. Erst wenn der Empfang dreimal in Folge unter dem halben Grenzwert liegt, kann davon ausgegangen werden, dass es sich nicht um ein Funkloch handelt, sondern die Entfernung zur Basisstation so groß geworden ist, dass die Signalstärke stark abfällt. Wird die Anzahl der benötigten Unterschreitungen größer gewählt, ist es möglich, dass die zurückgelegte Entfernung so groß ist, dass die selbe Frequenz von einer anderen Funkzelle verwendet wird. Dies würde zu falschen Informationen in den gesammelten Datensätzen führen.

Die beschriebenen Erweiterungen am **GSM-Scanner** wurden im folgenden Programmablauf umgesetzt:

1. Signalstärken aller Kanäle bestimmen
2. Mit den ermittelten Signalstärken die Menge M potenzieller BTS bestimmen
3. Signal aller BTS in M empfangen und decodieren
4. Gefundene BTS als Menge B speichern

5. Sind 30 Sekunden vergangen?
 - 5.1 Ja: Signalstärken auf allen Kanälen bestimmen
 - 5.1.1 Signalstärken bei B aktualisieren
 - 5.1.2 Signalstärke < Schwellwert : lösche BTS aus B
 - 5.1.3 Menge M potenzieller BTS bestimmen
 - 5.1.4 $M' = M \setminus B$
 - 5.1.5 Speichern aller BTS aus B in der Ausgabedatei
6. Kanal k aus M' empfangen. Kanal $k-1$ aus M' decodieren
 - 6.1 $k = \text{nächster Kanal aus } M'$
7. Gefundene BTS zu B hinzufügen
8. Zu 5 springen

Die empfangenen Daten werden im XML-Format abgespeichert. Dies erleichtert die anschließende Verarbeitung der Daten, da für das Parsen von XML-Dateien fertige Bibliotheken verwendet werden können.

Das XML-Format hat folgende Struktur:

```
<logfile>
  <gps latitude="48,001543" longitude="7,845548" time="1268847674">
    <bts channel="683" mcc="262" mnc="02" lac="50945" cid="39093" snr="23.72">
    </bts>
    <bts channel="851" mcc="262" mnc="E-Plus" lac="588" cid="7108" snr="17.61">
    </bts>
  </gps>
  <gps latitude="48,017050" longitude="7,860330" time="1268847395">
    <bts channel="1" mcc="262" mnc="Vodafone" lac="793" cid="15081" snr="26.86">
    </bts>
    <bts channel="3" mcc="262" mnc="Vodafone" lac="793" cid="45352" snr="13.29">
    </bts>
  </gps>
</logfile>
```

Im Beispiel werden zwei Datenpunkte in der XML-Ausgabedatei gespeichert. Ein Datenpunkt beginnt mit `<gps>` und endet mit `</gps>`. Die GPS-Koordinaten sowie ein Zeitstempel werden als Attribute eines Datenpunktes gespeichert. Jeder Datenpunkt enthält im gegebenen Beispiel jeweils zwei BTS, die mit dem Tag `<bts>` beginnen und mit dem Tag `</bts>` enden. Zu jeder

6. Lokalisierung mittels GSM

BTS werden die Informationen Channel, MCC, MNC, LAC, Cell-ID und SNR als Attribute gespeichert.

6.2. Erster Versuchsaufbau

Um Messergebnisse von unterschiedlichen geographischen Punkten zu erhalten, wurde die Hardware in ein Auto eingebaut. Es wurde folgender Versuchsaufbau gewählt:

- USRP2 mit DBSRX
- GPSDO als Referenzoszillatator
- Antenne: SLM155
- Laptop: Compaq 6910p (Core 2 Duo 2 GHz; 2 GByte RAM)
- GPS: Wintec WBT-201

Da GSM-Basisstationen auch in Städten eine Reichweite von mehreren Kilometern haben, musste ein ausreichend großes Versuchsgebiet für die Aufzeichnung der Daten gewählt werden. Es wurde eine annähernd quadratische, 13 Kilometer lange Versuchsstrecke innerhalb von Freiburg im Breisgau abgefahren.

6.3. Ergebnisse

Für die Erstellung der Datenbank wurden insgesamt 67 Datenpunkte aufgezeichnet. Jeder Datenpunkt enthält die gefundenen BTS sowie eine aktuelle Signalstärke. Zur Visualisierung der empfangenen Daten, wurde ein Programm entwickelt, das die Daten konvertiert, damit diese als Google-Maps Overlay dargestellt werden können. Anhand der Darstellung wurde die geographische Verteilung der Datenpunkte erfassbar. Wird ein Datenpunkt angeklickt, werden die bei diesem Datenpunkt aufgezeichneten BTS tabellarisch dargestellt. Das Google-Maps Overlay ist in Abbildung 6.2 abgebildet.

Für die Lokalisierung mit Hilfe der erstellten Datenbank wurde ein zweiter Datensatz aufgezeichnet. Außerdem wurde ein Programm entwickelt, das die Positionsbestimmung anhand der Informationen in der Datenbank realisiert. Der zweite Datensatz ist in Abbildung 6.3 über Google-Maps visualisiert. Er enthält 63 Datenpunkte und wird im folgenden Lookup-Datensatz genannt. Auch der Lookup-Datensatz enthält für jeden Datenpunkt eine GPS-Position. Diese wird zur Überprüfung der ermittelten Position verwendet.

Das entwickelte Programm zur Bestimmung der Position erwartet einen einzelnen Datenpunkt als Eingabe und vergleicht diesen mit allen Datenpunkten in der Datenbank. Dabei sucht das Programm den Datenpunkt in der Datenbank mit der geringsten Abweichung vom Eingabedatensatz. Der verwendete Algorithmus ist der Arbeit von Paramvir Bahl und Venkata N. Padmanabhan [22] entnommen.

Der Algorithmus minimiert die Abweichung der beiden folgenden Kriterien:

1. Anzahl nicht übereinstimmender BTS
2. SNR-Abweichung auf übereinstimmenden BTS

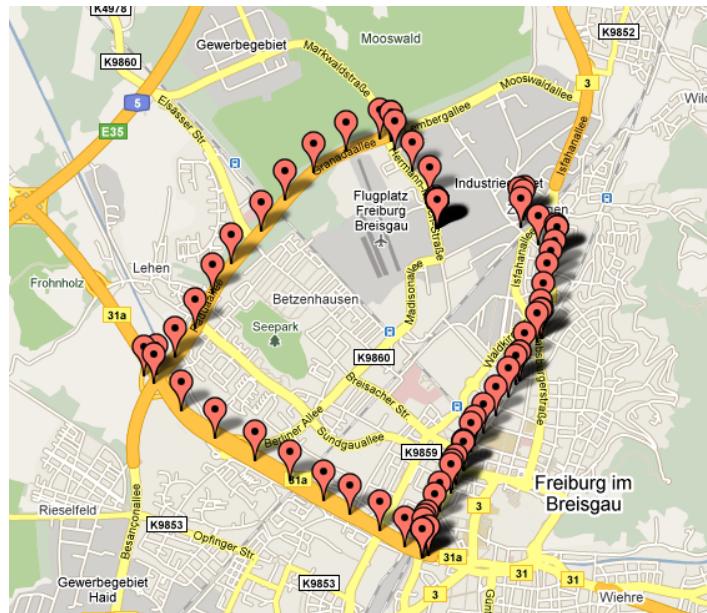


Abbildung 6.2.: Visualisierung der Datenpunkte der Datenbank über Google Maps



Abbildung 6.3.: Lookup-Datensatz

6. Lokalisierung mittels GSM

Bei der Auswertung der Daten wurde festgestellt, dass anders als erwartet, nicht der Datenpunkt in der Datenbank gefunden wird, der am nächsten an der korrekten Position liegt. In Abbildung 6.4 wurden sechs zufällige Datenpunkte aus dem Lookup-Datensatz lokalisiert. Die Datenpunkte der Datenbank sind rot markiert. Um die gefundene Position zu überprüfen, wurde die Position, an der die Lookup-Daten aufgezeichnet wurden, blau eingefärbt. Die gefundene Position ist mit einer roten Linie mit der gesuchten Position verbunden, um die Zuordnung zu verdeutlichen.



Abbildung 6.4.: Visualisierung der gefundenen Positionen

In der Abbildung 6.4 ist deutlich zu sehen, dass die gefundene Position meist erheblich von der tatsächlichen Position abweicht. Es wird nicht, wie erwartet, ein Datenpunkt in der Nähe zur gesuchten Position gefunden. Einer der Gründe hierfür ist, dass sich die Datensätze erheblich in der Anzahl gefundener BTS unterscheiden. In Abbildung 6.5 sind die Anzahl der gefundenen BTS in der Datenbank und im Lookup-Datensatz gegenübergestellt.

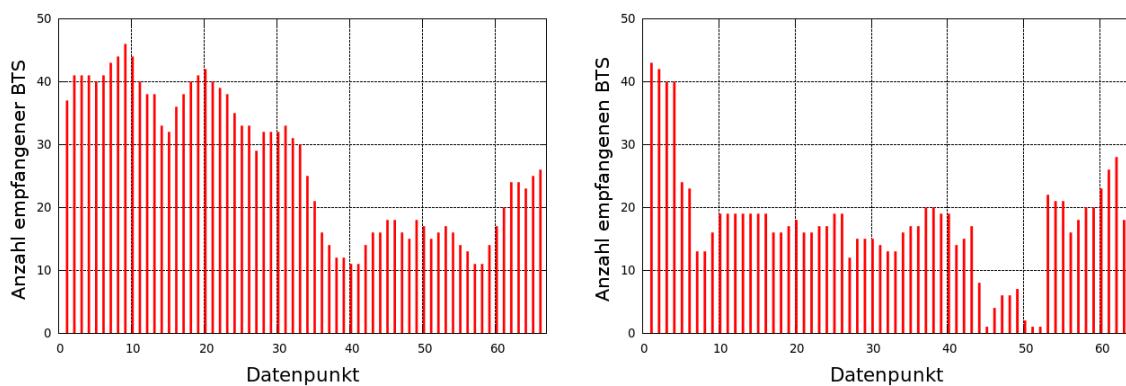


Abbildung 6.5.: Links: Anzahl empfangener BTS pro Datenpunkt in der Datenbank
Rechts: Anzahl empfangener BTS pro Datenpunkt im Lookup-Datensatz

Zu Beginn der Aufzeichnung im Lookup-Datensatz wurden vergleichbar viele BTS wie im Datensatz der Datenbank gefunden. Durch ein länger andauerndes Funkloch wurden bei den

weiteren Datenpunkten des Lookup-Datensatzes nur noch sehr wenige BTS gefunden. Anscheinend war es dem **GSM-Scanner** nicht möglich die BTS erneut zu empfangen.

Werden alle 63 Lookup-Datenpunkte lokalisiert, fällt auf, dass die gefundenen Positionen nicht gleich verteilt über alle Datenbankpunkte sind. Sechs Datenpunkte der Datenbank wurden sehr häufig als beste Übereinstimmung zur Eingabe gefunden. Die Abbildung 6.6 links veranschaulicht, wie oft ein Datenpunkt in der Datenbank als beste Übereinstimmung gefunden wurde.

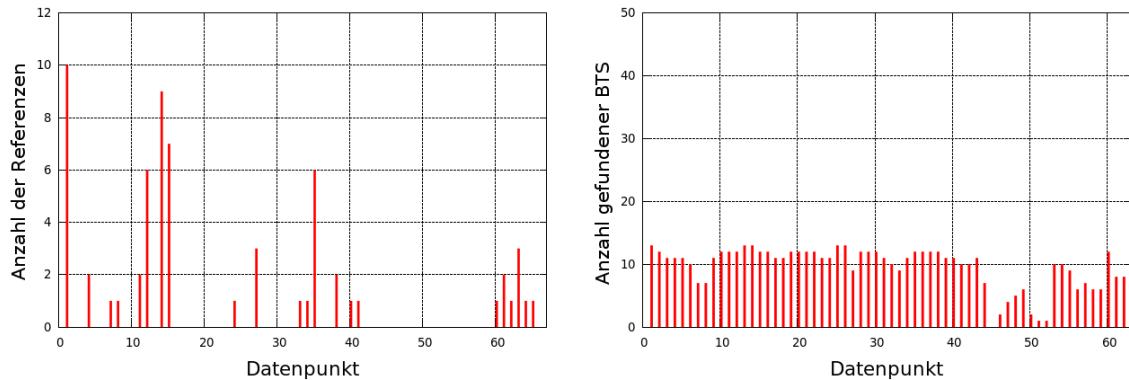


Abbildung 6.6.: Links: Anzahl der Referenzierungen auf einen Datenpunkt in der Datenbank
Rechts: Anzahl Übereinstimmungen zwischen den Lookup-Datensätzen und dem besten Treffer in der Datenbank

Bei einer manuellen Auswertung der Daten konnte festgestellt werden, dass sich die Daten der ersten Aufzeichnung an einem bestimmten Ort erheblich von den Daten unterschieden, die bei der zweiten Aufzeichnung am selben Ort gespeichert wurden. Das bedeutet, dass beim Erstellen der Datenpunkte immer nur eine Teilmenge der verfügbaren Daten auch wirklich aufgezeichnet wurden. Dies hat zur Folge, dass die Datenpunkte in den Datensätzen keine vollständige Repräsentation der verfügbaren Informationen an einem bestimmten Ort darstellen. Die Bestimmung der Position aus einer unvollständigen Datenbank birgt erhebliche Probleme, da die Schnittmenge der beiden Datensätze klein ist. Das Problem wird durch die Abbildung 6.6 rechts veranschaulicht. Die Abbildung zeigt für jeden Lookup-Datenpunkt die Anzahl übereinstimmender BTS mit dem besten Datenpunkt der Datenbank. Auch für Lookup-Datenpunkte mit vielen gefundenen BTS ist die beste Übereinstimmung mit der Datenbank bezüglich der Anzahl identischer BTS klein. Diese Probleme haben zur Folge, dass der gefundene Datenpunkt in der Datenbank nicht der Datenpunkt mit der korrekten Position sein muss, da sich die verglichenen Datensätze teilweise erheblich unterscheiden.

6.3.1. Schlussfolgerung

Der Versuchsaufbau und die daraus gewonnenen Daten zeigen, dass eine Lokalisierung mit dem gewählten Ansatz nur bedingt möglich ist. Es konnte gezeigt werden, dass die gewonnenen Datensätze für eine Lokalisierung verwendet werden können, jedoch in den meisten Fällen keine exakte Position gewährleisten. Die Unterschiede zwischen der Datenbank und den Lookup-Daten sind zu groß, um daraus die genaue Position zu extrahieren. Beim hier gewählten Ansatz war es zwar möglich, die Daten in Echtzeit zu verarbeiten und auszugeben, jedoch ist der Datensatz in vielen Fällen unvollständig und enthält nicht alle Basisstationen in der Umgebung. Der Grund hierfür ist, dass die Zeit zwischen den einzelnen Datenpunkten nicht ausreicht, um alle neuen BTS zu empfangen. Dies wird durch die in Kapitel 5.2 beschriebenen Probleme mit dem **gsm-receiver** verstärkt, da nicht davon ausgegangen werden kann,

6. Lokalisierung mittels GSM

dass eine BTS gefunden wird, selbst wenn sie eine ausreichende Signalstärke aufweist. Eine Verlängerung der Zeitintervalle zwischen den Aufzeichnungspunkten ließe dem **GSM-Scanner** mehr Zeit, um weitere Kanäle zu empfangen. Jedoch stellt dies nur dann eine Lösung dar, wenn die zurückgelegte Entfernung während des Scan-Vorganges nicht zu groß ist. Optimalerweise sollte beim Erstellen eines Datenpunktes der Standort statisch sein, um die gewonnenen Informationen eindeutig dem Ort zuzuordnen.

Um einen besseren und somit für eine Position repräsentativen Datensatz zu erhalten, sind folgende Erweiterungen denkbar:

- Die Daten werden breitbandig empfangen und mit der Filterbank aus Kapitel 5.4.1 verarbeitet. Da diese sehr rechenintensiv ist, können die Daten nicht in Echtzeit decodiert werden. Deshalb wird die Datenbank erst nach dem Aufzeichnen aller Daten erstellt:

1. Empfangen der Daten und Abspeichern der Daten
2. Decodieren der Daten und Erstellen der Datenbank

Dieser Ansatz birgt den Vorteil, dass bei der Decodierung der Daten alle Kanäle betrachtet werden können. Somit ist sichergestellt, dass kaum Basisstationen übersehen werden.

- Für die aktuelle Position wird ein Fingerabdruck anhand der empfangenen Signalstärken auf allen Kanälen in EGSM900 und GSM1800 erstellt. Es werden keine Daten decodiert. Die durch die BTS ausgesendeten Informationen werden nicht betrachtet. Die aktuelle Position wird bei diesem Ansatz anhand der empfangenen Signalstärken eindeutig definiert. Das Verfahren ist in Echtzeit möglich, da das rechenintensive Decodieren der Daten entfällt.

Bei Ansatz zwei muss überprüft werden, ob die Betrachtung der Signalstärken alleine ausreichend ist, um eine eindeutige Identifizierung zu ermöglichen.

6.4. Zweiter Versuchsaufbau

Die Ergebnisse der Versuche wurden in einem zweiten Versuchsaufbau berücksichtigt. Im Mittelpunkt der zweiten Versuchsreihe stand die Erstellung einer möglichst vollständigen Datenbank, um die zuvor beschriebenen Probleme zu vermeiden. Dabei wurde bewusst auf eine mobile Datenaufzeichnung verzichtet. Es wurden zehn Orte im Versuchsgebiet ausgewählt. Diese Orte sind in Abbildung 6.7 markiert. Jeder Aufzeichnungsort besitzt eine eindeutige Nummer. Für diese Versuchsreihe wurden die in Kapitel 6.2 beschriebenen Geräte verwendet.

Jeder Ort wurde zweimal angefahren, um die benötigten Datensätze zu generieren. Der zweite Aufzeichnungsort liegt 10 - 50 m vom ersten Aufzeichnungsort entfernt. An jedem Aufzeichnungsort wurden jeweils zwei Datensätze für die Datenbank und zwei Datensätze für den Look-up aufgezeichnet. Bei diesem Versuchsaufbau wurden die Frequenzbänder über das USRP2 in 25 MHz breiten Blöcken empfangen. Um beide Frequenzbänder abzudecken sind fünf Aufzeichnungen notwendig.

6.4.1. Auswertung

Insgesamt wurden 72,6 GByte Daten aufgezeichnet. Die Verarbeitung der Daten wurde in folgenden Schritten durchgeführt:



Abbildung 6.7.: Aufzeichnungsorte im zweiten Versuchsaufbau

1. Trennen der Kanäle:

Aus den breitbandigen Aufzeichnungen wurden die einzelnen Kanäle extrahiert. Da an jedem Ort insgesamt vier Aufzeichnungen vorgenommen wurden und jede Aufzeichnung 548 GSM-Kanäle enthält, wurden 21920 GSM-Kanäle mit einem Datenvolumen von 167 GByte extrahiert. Die Rechenzeit zum Trennen der Kanäle betrug zehn Stunden².

2. Bestimmen der Signalstärke:

Für jeden GSM-Kanal wurde direkt aus den breitbandigen Aufzeichnungen eine Signalstärke berechnet.

3. Decodieren der Kanäle:

Da die Anzahl der Kanäle extrem hoch war, wurden nur Kanäle mit einer Signalstärke größer als vier betrachtet. Insgesamt hat die Decodierung der Daten 4,5 Stunden Rechenzeit beansprucht².

4. Erstellen der Datensätze für Datenbank und Lookup-Datensatz

Für jeden Datensatz wurden jeweils zwei Aufzeichnungen zusammengeführt, um einen möglichst kompletten Datensatz zu erhalten. Dies minimiert die beschriebenen Probleme mit dem `gsm-receiver`.

6.4.2. Ergebnisse

In Abbildung 6.8 links ist die Anzahl der gefunden BTS für jeden Datenpunkt der Datenbank zu sehen. Diese unterscheiden sich teilweise von der Anzahl gefundener BTS im Lookup-Datensatz in der gleichen Abbildung rechts.

Jeder Datenpunkt aus dem Lookup-Datensatz wurde über die Datenbank lokalisiert. Dabei wird zu jedem Lookup-Datenpunkt eine Abweichung zu allen Datenpunkten der Datenbank

² Rechenzeit bestimmt mit Laptop aus Kapitel 6.2

6. Lokalisierung mittels GSM

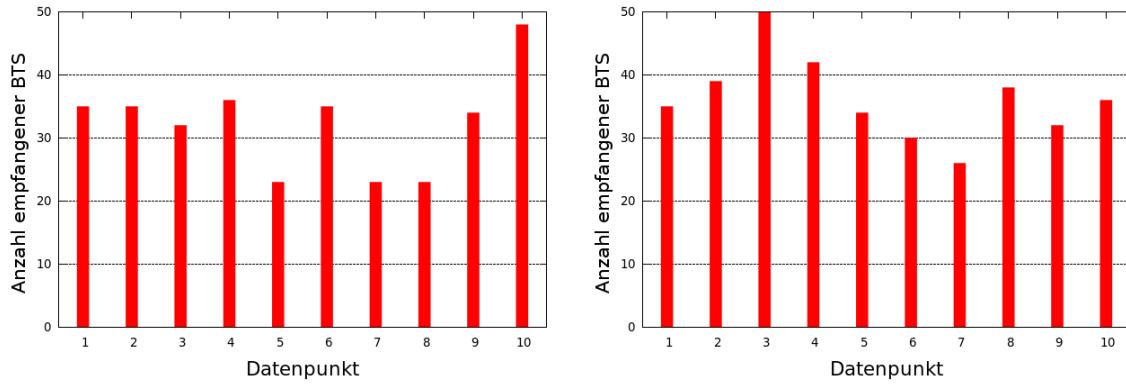


Abbildung 6.8.: Links: Anzahl empfangener BTS pro Datenpunkt in der Datenbank
Rechts: Anzahl empfangener BTS pro Datenpunkt im Lookup-Datensatz

berechnet. Die Abweichung ist für alle zehn Lookup-Datensätze in Abbildung 6.9 in unterschiedlichen Farben dargestellt. Das jeweilige Minimum stellt den gefundenen Ort dar und ist über ein farbiges Viereck hervorgehoben.

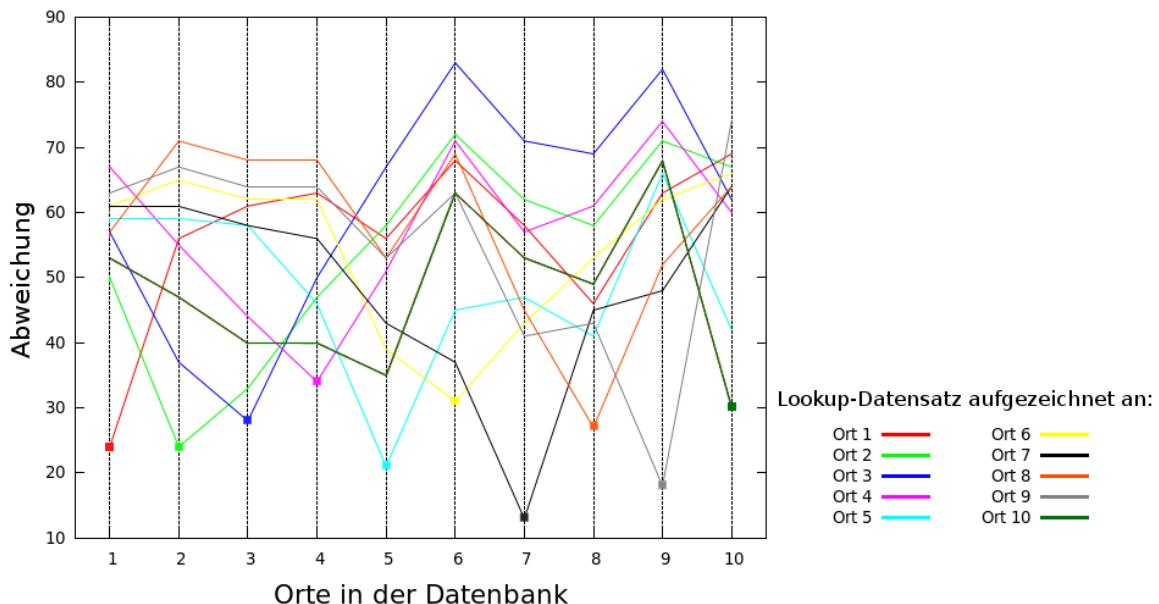


Abbildung 6.9.: Bestimmung der minimalen Abweichung für zehn Lookup-Datenpunkte

Der Grafik kann entnommen werden, dass die gefundene Position der jeweils geographisch nächste Aufzeichnungsort ist. Es konnten alle zehn Lookup-Datensätze richtig lokализiert werden. Abbildung 6.10 zeigt die Ergebnisse der Zuordnung. Hier sind die Datenpunkte der Datenbank blau und die Lookup-Datenspunkte rot eingefärbt. Die Abbildung zeigt deutlich, dass jeder Lookup-Datenpunkt seinem jeweils nächsten Datenpunkt aus der Datenbank zugeordnet wird.

Die Anzahl der BTS, die sowohl im Lookup-Datensatz als auch im Datenpunkt der Datenbank enthalten sind, können der Abbildung 6.11 rechts entnommen werden. Im Vergleich zu den Ergebnissen aus dem ersten Versuchsaufbau, ist die Anzahl gefundener BTS wesentlich höher. Dies spricht dafür, dass die Datenpunkte eine, im Vergleich zum ersten Versuchsaufbau, wesentlich bessere Repräsentation der empfangbaren BTS am jeweiligen Ort darstellen.



Abbildung 6.10.: Visualisierung der gefundenen Positionen im zweiten Versuchsaufbau

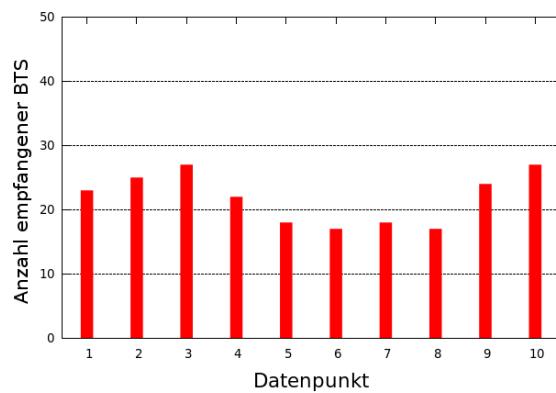


Abbildung 6.11.: Anzahl der Übereinstimmungen zwischen den Lookup-Datensätzen und dem besten Treffer in der Datenbank

6. Lokalisierung mittels GSM

Da die Lokalisierung von Datenpunkten in nächster Nähe zu einem Datenpunkt in der Datenbank funktioniert, wurde im folgenden überprüft, ob eine Lokalisierung möglich ist, wenn ein Lookup-Datenpunkt von den Orten in der Datenbank abweicht. Es wurden zwei Datenpunkte aufgezeichnet. Datenpunkt A liegt in der Nähe von Ort 1 und Datenpunkt B liegt zwischen Ort 2 und 3. Wie in Abbildung 6.12 zu sehen ist, wird Datenpunkt A korrekt lokalisiert. Die Entfernung von Datenpunkt B zu Ort 2 beträgt 428 m und zu Ort 3 475 m. Somit ist eine Zuordnung zu Ort 3 nicht richtig. Jedoch zeigt Abbildung 6.12 rechts, dass sich die berechnete Abweichung von Datenpunkt B zu Ort 2 und 3 nur geringfügig unterscheidet.

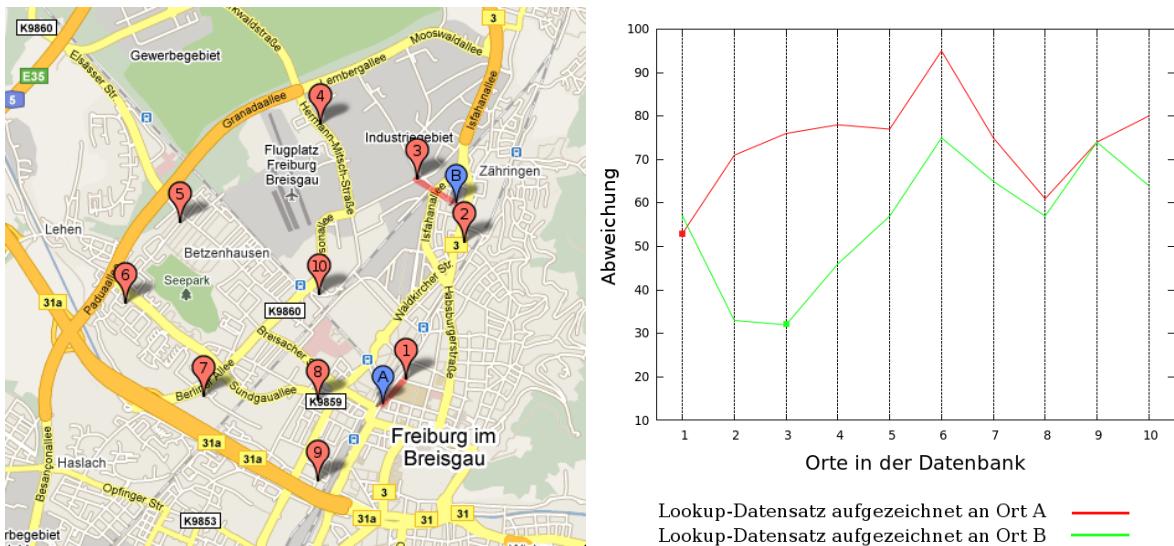


Abbildung 6.12.: Zuordnung der gefundenen Datenpunkte in der Datenbank

Um die Positionsbestimmung zu verfeinern, könnte zwischen den Datenpunkten mit der geringsten berechneten Abweichung interpoliert werden. Im Beispiel aus Abbildung 6.12 könnte die Position des Datenpunktes B über eine Interpolation zwischen den beiden Orten 2 und 3 genauer bestimmt werden.

6.5. Fazit

Der zweite Versuchsaufbau zeigt, dass eine Lokalisierung über den verwendeten Ansatz funktioniert, wenn die verwendeten Datensätze eine gute Repräsentation der empfangbaren BTS an einem Ort darstellen.

Wird eine Lokalisierung nur anhand einer empfangenen Cell-ID durchgeführt, hängt die erreichte Genauigkeit von der jeweiligen Zellgröße ab. Bei GSM kann eine Zelle einen Durchmesser von bis zu 35 km haben und ermöglicht somit eine relativ schlechte Lokalisierung. Im Vergleich hierzu liefert die Betrachtung mehrerer Zellen eine deutlich höhere Genauigkeit. Die minimale Distanz zwischen zwei Datenpunkten in der Datenbank beträgt beim zweiten Versuchsaufbau 822 m. Die erreichbare Genauigkeit kann durch eine feinmaschigere Datenbank oder durch eine Interpolation zwischen den Datenpunkten gesteigert werden.

7. Fazit und Ausblick

Ziel dieser Arbeit war es, Daten von GSM-Basisstationen zu empfangen, diese übersichtlich darzustellen und im Hinblick auf eine mögliche Lokalisierung zu betrachten. Die entwickelte Software **GSM-Scanner** empfängt über den USRP2 “System Information Messages”. Die empfangenen Daten werden nach ihrer Decodierung in der eigens programmierten Oberfläche dargestellt. Der **GSM-Scanner** erlaubt es, ähnlich dem Nokia Netmonitor, einen Überblick über Basisstationen in der Umgebung zu erhalten. Der große Vorteil gegenüber dem Nokia Netmonitor ist die Unabhängigkeit von einem Anbieter. So können mittels der entwickelten Software wesentlich mehr Basisstationen empfangen werden. Es wurden unterschiedliche Ansätze zum Verbessern der Scan-Geschwindigkeit analysiert und umgesetzt. Für jeden Kanal wurde ein SNR berechnet, der einen Indikator für eine Basisstation darstellt. Durch Auswertung des SNR konnte die Scan-Geschwindigkeit erheblich gesteigert werden.

Über einen Vergleich von unterschiedlichen GSM-Antennen und nach der Optimierung des Taktsignals über einen Referenzoszillator konnte die verwendete Hardware für den Empfang von GSM-Signalen optimiert werden. Ein Vergleich der empfangenen Daten hat jedoch gezeigt, dass die stark optimierte Hardware des Nokia 3310 wesentlich empfindlicher ist als die universelle Hardware des USRP2.

Die Lokalisierung anhand der empfangenen Daten wurde als praktisches Feldexperiment geplant und durchgeführt. Der erste Versuchsaufbau bestätigt, dass eine Lokalisierung mit Hilfe der empfangenen GSM-Basisstationen möglich ist. Die Ergebnisse zeigen jedoch, dass die Anzahl der gefundenen BTS bei wiederholten Aufzeichnungen stark schwankt. Aufgrund der Vielzahl zu betrachtender Kanäle und der Probleme mit dem Decoder waren die empfangenen Datensätze unvollständig. Die Datenaufzeichnung wurde durch einen mobilen Versuchsaufbau zusätzlich erschwert. Die Erkenntnisse wurden in einem zweiten, verbesserten Feldexperiment umgesetzt. Dabei wurde ein statischer Aufbau mit einer definierten Anzahl an Datenpunkten gewählt. Eine Lokalisierung mit Hilfe der erstellten Datensätze lieferte gute Ergebnisse. Die maximal erreichbaren Genauigkeiten müssen in weiteren Untersuchungen analysiert werden. Beim entwickelten **GSM-Scanner** sind Verbesserungen denkbar. Die Scan-Geschwindigkeit kann durch Betrachten der Nachbarschaftsliste gesteigert werden. In diesem Zusammenhang muss jedoch darauf geachtet werden, dass keine Basisstationen übersehen werden, da die Nachbarschaftslisten nicht zwingend alle empfangbaren Basisstationen enthalten (siehe Kapitel 5.6). Ebenso können die von der Zelle verwendeten Frequenzen als zusätzlicher Filter benutzt werden. Diese Informationen werden in der “System Information Message Type 1” übertragen. Die Benutzeroberfläche kann erweitert werden, so dass zusätzliche Informationen über die Zellkonfiguration angezeigt werden. Denkbar ist auch, die Benutzeroberfläche um eine graphische Darstellung der gefundenen BTS im Frequenzspektrum zu erweitern.

Der verwendete Decoder **gsm-receiver** hat erhebliche Probleme verursacht und sollte dringend verbessert werden. Vor allem der Umstand, dass manche Eingangssignale nicht decodiert werden können, macht den Decoder unzuverlässig. Dies führt dazu, dass bei einem einmaligen Empfangen nicht davon ausgegangen werden kann, dass auch alle Basisstationen gefunden werden. Um aussagekräftige Ergebnisse zu erhalten, war es somit notwendig, einen Kanal mehrfach zu empfangen und die Ergebnisse zu kombinieren.

Im Hinblick auf die Lokalisierung über empfangene BTS muss überprüft werden, ob das Mobilfunknetzwerk statisch ist oder regelmäßig durch den Anbieter umkonfiguriert wird. Bei

7. Fazit und Ausblick

einer Veränderung der eindeutigen Zellinformationen würden die erstellten Lokalisierungsdatenbanken falsche Informationen enthalten und müssten korrigiert werden. Eine Veränderung der Konfiguration des Mobilfunknetzes durch den Anbieter ist zumindest denkbar. Der Anbieter könnte somit auf sich ändernde Auslastungen reagieren. Ein Beispiel ist ein Fussballspiel bei dem sich an einer geographischen Position mehrere tausend Personen befinden. Diese Auslastungsextreme könnten durch dynamisches Hinzuschalten von Basisstationen abgefangen werden.

Die Experimente wurden mit dem Softwareradio USRP2 durchgeführt und können nicht ohne weitere Untersuchungen auf Mobilfunktelefone übertragen werden. Wie am Beispiel des Nokia 3310 gezeigt werden konnte, unterscheiden sich die Informationen, die von einem Mobilfunktelefon ausgegeben werden, von den Informationen des **GSM-Scanners**. In weiteren Untersuchungen muss deshalb überprüft werden, welche Genauigkeiten mit den Informationen aus dem Mobilfunktelefon erreicht werden können.

Literaturverzeichnis

- [1] GSMA: *Market Data Summary (Q2 2009)*. WWW-Dokument, http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm. [Online; letzter Aufruf 11.02.2010].
- [2] HOLGER BERTSCH: *Open Source GSM BTS Setup und Analyse für Demo-Zwecke*. Masterarbeit am LfKs Universität Freiburg, http://www.ks.uni-freiburg.de/php_arbeitdet.php?id=154 [Online; letzter Aufruf 01.05.2010], Oktober 2009.
- [3] JOCHEN H. SCHILLER und AGNÈS VOISARD (Herausgeber): *Location-Based Services*. Morgan Kaufmann, 2004.
- [4] B. RAO und L. MINAKAKIS: *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*. Seite 8 pp., jan. 2004.
- [5] STEPHAN HESSBERGER: *Das B-Netz*. WWW-Dokument, <http://www.oeb1.de/B-Netz/BNetz.html>. [Online; letzter Aufruf 24.3.2010].
- [6] GSM ASSOCIATION: *GSM Technology*. WWW-Dokument, <http://www.gsmworld.com/technology/gsm/index.htm>. [Online; letzter Aufruf 9.3.2010].
- [7] 3GPP TS 45.005: *Radio Access Network; Radio transmission and reception (Release 9)*. WWW-Dokument, http://www.3gpp.org/ftp/Specs/archive/45_series/45.005/45005-900.zip. [Online; letzter Aufruf 11.02.2010].
- [8] MATTHIAS FONFARA: *GSM Technik FAQ*. WWW-Dokument, <http://www.senderlisteffm.de/techfaq.html#sendeleistung>. [Online; letzter Aufruf 24.3.2010].
- [9] ETSI EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE: *Digital cellular telecommunications system (phase 2+); Radio transmission and reception (3GPP TS 45.005 version 9.1.0 Release 9)*. PDF-Dokument, <http://www.etsi.com>, Februar 2010.
- [10] ETSI EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE: *Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode (GSM 03.22 version 5.3.1 Release 1996)*. PDF-Dokument, <http://www.etsi.com>, Februar 2010.
- [11] DENIS DILBA: *Da schreit das Handy*. WWW-Dokument, <http://www.heise.de/tr/artikel/Da-schreit-das-Handy-280201.html>. [Online; letzter Aufruf 19.4.2010].
- [12] DANIEL LUIK: *Blacklisted, Blocked or Barred Handsets*. WWW-Dokument, <http://www.unlockme.co.uk/blacklist.html>. [Online; letzter Aufruf 26.3.2010].
- [13] JÖRG EBERSPÄCHER, HAND-JÖRG VÖGEL, CHRISTIAN BETTSTETTER und CHRISTIAN HARTMANN: *GSM – Architecture, Protocols and Services*. Wiley, 3. Auflage, 2009.
- [14] FEDERAL COMMUNICATIONS COMMISSION: *Enhanced 9-1-1 - Wireless Services*. WWW-Dokument, <http://www.fcc.gov/pshs/services/911-services/enhanced911>Welcome.html>. [Online; letzter Aufruf 11.3.2010].

- [15] CARSTEN SCHULTE und CHRISTOFFER RIEMER: *Handy-Ortung und GPS-Ortung*. WWW-Dokument, http://www.iwi.uni-hannover.de/lv/ucc_ws04_05/riemer/frame_haupt.htm. [Online; letzter Aufruf 23.3.2010].
- [16] H. INGENSAND und P. BITZI: *Technologien der GSM-Positionierungsverfahren*. Wichmann Verlag.
- [17] ETSI EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE: *Digital cellular telecommunications system (phase 2+); radio subsystem synchronization (gsm 05.10 version 8.4.0 release 1999) Technical Report ETSI TS 100 912 V8.4.0 (2000-08)*. PDF-Dokument, <http://www.etsi.com>, August 2000.
- [18] GNU RADIO: *USRP2 General FAQ*. WWW-Dokument, <http://gnuradio.org/redmine/wiki/gnuradio/USRP2GenFAQ>. [Online; letzter Aufruf 11.2.2010].
- [19] WAYNE PEACOCK: *A Introduction to Nokia F-Bus*. WWW-Dokument, <http://www.embedtronics.com/nokia/fbus.html>. [Online; letzter Aufruf 24.3.2010].
- [20] MARCIN WIACEK: *Netmonitor in Nokia Phones*. WWW-Dokument, http://www.mwiacek.com/gsm/netmon/faq_net0.htm. [Online; letzter Aufruf 5.2.2010].
- [21] ANTHONY LAMARCA, YATIN CHAWATHE, SUNNY CONSOLVO, JEFFREY HIGHTOWER, IAN SMITH, JAMES SCOTT, TIMOTHY SOHN, JAMES HOWARD, JEFF HUGHES, FRED POTTER, JASON TABERT, PAULINE POWLEDGE, GAETANO BORRIELLO und BILL SCHILIT: *Place Lab: Device Positioning Using Radio Beacons in the Wild*. In: *Proceedings of the Third International Conference on Pervasive Computing*, May 2005.
- [22] PARAMVIR BAHL und VENKATA N. PADMANABHAN: *RADAR: an in-building RF-based user location and tracking system*. Seiten 775–784, 2000.

Abkürzungsverzeichnis

Abkürzung	Beschreibung
ADC	Analog-to-Digital-Converter
AGCH	Access Grant Channel
AOA	Angle of Arrival
ARFCN	Absolute Radio Frequency Channel Number
AUC	Authentication Center
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CCCH	Common Control Channel
CID	Cell ID
COO	Cell of Origin
DAC	Digital-to-Analog-Converter
DCCH	Dedicated Control Channel
EIR	Equipment Identity Register
FACCH	Fast Associated Control Channel
FCCH	Frequency Correction Channel
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
FPGA	Field Programmable Gate Array
GMSC	Gateway Mobile Switching Center
GPS	Global Positioning System
GPSDO	GPS Disciplined Oscillator
GSM	Global System for Mobile Communications
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
LA	Location Area
LAC	Location Area Code
LBS	Location Based Services

Abkürzungsverzeichnis

Abkürzung	Beschreibung
MCC	Mobile Country Code
MNC	Mobile Network Code
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
MSPS	Mega-Samples Per Second
NCH	Notification Channel
NSS	Network Subsystem
PCH	Paging Channel
PDA	Personal Digital Assistant
RACH	Random Access Channel
RSS	Received Signal Strength
SACCH	Slow Associated Control Channel
SCH	Synchronization Channel
SDCCH	Stand-alone Dedicated Control Channel
SDR	Software Defined Radio
SIM	Subscriber Identity Module
SMS	Short Message Service
SNR	Signal to Noise Ratio
TCH	Traffic Channel
TCH/F	Traffic Channel Fullrate
TCH/H	Traffic Channel Halfrate
TDMA	Time Division Multiple Access
TOA	Time of Arrival
TRAU	Transcoder and Rate Adaptation Unit
USRP	Universal Software Radio Peripheral
VLR	Visitor Location Register
WLAN	Wireless Local Area Network

Abbildungsverzeichnis

2.1.	Überblick über die Systemkomponenten	5
2.2.	Mobilstation aus Nokia 3310 und T-Mobile SIM-Karte	8
2.3.	Frequenzmultiplexing im GSM900 Band	10
2.4.	Kommunikation in Zeitschlitzten	11
2.5.	Frequenzmultiplexing und Zeitmultiplexing im GSM900 Band	11
2.6.	Von GSM-TDMA verwendete Bursts (Vorlage nach [13])	12
2.7.	Von GSM-TDMA verwendete Bursts	16
2.8.	Abbildung von logischen auf physikalische Kanäle	
	Zeitschlitz 0: BCCH + FCCH + SCH + CCCH + SDCCH + FACCH	
	Zeitschlitz 1: SDCCH + SACCH	
	Zeitschlitz 2-7: TCH + SACCH + FACCH	17
3.1.	Aufbau eines Software-Radios	20
3.2.	Universal Software Radio Peripheral Version 1 (links) und Version 2 (rechts) .	21
3.3.	USRP2 mit aufgesteckter DBRX-Receiverkarte	22
3.4.	links: Transceiverkarten RFX900/RFX1800; rechts: Receiverkarte DBRX . .	22
3.5.	Untersuchte GSM-Antennen, von links nach rechts: LP0926, VERT900, MAG2100, SLM155 und SLM17	23
3.6.	Bestimmung der Signalstärke mit der Antenne SLM17	24
3.7.	Links: GPSDO von Trimble; Rechts: Monitor-Programm	26
3.8.	Interner Aufbau GPSDO von Trimble	26
3.9.	Nokia 3310 Netmonitor: Seite 1, 3, 4, 5 und 11	27
4.1.	Zusammenspiel der Softwarekomponenten	29
4.2.	Frequenzspektrum zwischen 925 MHz und 950 MHz	30
4.3.	Frequenzspektrum einer GSM-Basisstation bei 927 MHz	30
4.4.	Empfangenes Signal bei 927 MHz als Wasserfallplot	31
5.1.	Zusammenspiel der verwendeten Softwarekomponenten	35
5.2.	Komplettes GSM900 Frequenzbank als Wasserfallplot; X-Achse: ± 12.5 MHz; Y-Achse 200 ms, Mitte bei 947.5 Mhz	39
5.3.	Aufteilen der Kanäle mit einer Filterbank	39
5.4.	Frequenzspektrum des Rauschens ohne Ausgleich der Nichtlinearität (oben) und mit Ausgleich (unten)	41
5.5.	GSM900 Frequenzspektrum mit Mittelwert (grün) und Rauschwert (blau) . .	42
5.6.	Ergebnis der SNR-Berechnung im EGSM900-Band für 125 GSM-Kanäle . .	42
5.7.	Stabilität des berechneten SNR-Wertes mit Mittelwert.	43
5.8.	Benutzeroberfläche des GSM-Scanners	44
5.9.	Scan-Geschwindigkeit bei verschiedenen SNR-Schwellwerten	46
5.10.	Verhältnis zwischen betrachteten Kanälen und gefundenen BTS bei steigendem SNR	46
5.11.	Anzahl der gefundenen BTS bei verschiedenen SNR-Schwellwerten	47
5.12.	Visualisierung der Nachbarschaftsliste im Vodafone GSM-Netz	49

Abbildungsverzeichnis

6.1. Erweiterte Benutzeroberfläche des GSM-Scanners zum Erstellen der Datensätze	52
6.2. Visualisierung der Datenpunkte der Datenbank über Google Maps	55
6.3. Lookup-Datensatz	55
6.4. Visualisierung der gefundenen Positionen	56
6.5. Links: Anzahl empfangener BTS pro Datenpunkt in der Datenbank Rechts: Anzahl empfangener BTS pro Datenpunkt im Lookup-Datensatz . . .	56
6.6. Links: Anzahl der Referenzierungen auf einen Datenpunkt in der Datenbank Rechts: Anzahl Übereinstimmungen zwischen den Lookup-Datensätzen und dem besten Treffer in der Datenbank	57
6.7. Aufzeichnungsorte im zweiten Versuchsaufbau	59
6.8. Links: Anzahl empfangener BTS pro Datenpunkt in der Datenbank Rechts: Anzahl empfangener BTS pro Datenpunkt im Lookup-Datensatz . . .	60
6.9. Bestimmung der minimalen Abweichung für zehn Lookup-Datenpunkte	60
6.10. Visualisierung der gefundenen Positionen im zweiten Versuchsaufbau	61
6.11. Anzahl der Übereinstimmungen zwischen den Lookup-Datensätzen und dem besten Treffer in der Datenbank	61
6.12. Zuordnung der gefundenen Datenpunkte in der Datenbank	62
B.1. Ergebnis der netzseitigen Lokalisierung über den O ₂ Handy-Finder	75
D.1. Umlöten des Widerstandes beim DBSRX-Daughterboard	77

A. Software Installation

A.1. GNU Radio

Installationsanleitungen für unterschiedliche Betriebssysteme stehen auf der GNU Radio-Projektseite¹ bereit. Im Rahmen dieser Arbeit wurde mit Ubuntu 9.10 gearbeitet.

Installationsanleitung für Ubuntu 9.10:

Abhängigkeiten bereitstellen:

```
sudo apt-get -y install swig g++ automake libtool python-dev libfftw3-dev \
  libcppunit-dev libboost1.38-dev libusb-dev fort77 sdcc sdcc-libraries \
  libsdl1.2-dev python-wxgtk2.8 subversion git-core guile-1.8-dev \
  libqt4-dev python-numpy ccache python-opengl libgs10-dev \
  python-cheetah python-lxml doxygen qt4-dev-tools \
  libqwt5-qt4-dev libqwtplot3d-qt4-dev pyqt4-dev-tools
```

Quellen herunterladen:

Die aktuellen Quellen können hier gefunden werden:

<http://gnuradio.org/redmine/wiki/gnuradio/Download> [Stand 09.02.2010: Version 3.2.2]

Quellen kompilieren und installieren:

```
export LD_LIBRARY_PATH=$BOOST_PREFIX/lib
./bootstrap
./configure --with-boost=$BOOST_PREFIX
make
sudo make install
sudo ldconfig
```

¹ GNU Radio, <http://gnuradio.org> [Online; letzter Aufruf 18.02.2010]

A.2. Airprobe

Achtung: Der original GSM-Receiver von Airprobe wurde durch eine Weiterentwicklung von Piot Krysik ersetzt², da diese beim Decodieren der Rohdaten wesentlich bessere Ergebnisse liefert.

Installation der Airprobe-Programme `gsmdecoder` und `gsm-receiver`:

Abhängigkeiten bereitstellen:

```
sudo apt-get -y install git-core autoconf \
automake libtool g++ python-dev swig libpcap0.8-dev
```

Quellen herunterladen:

```
git clone git://svn.berlin.ccc.de/airprobe
```

gsmdecoder kompilieren:

```
./bootstrap
./configure
make
```

gsm-receiver kompilieren:

Der Quellcode des `gsm-receiver` muss geringfügig angepasst werden. Hierfür kann der Patch `/Patch/gsm-receiver.patch` auf der CD im Anhang verwendet werden. Alternativ muss in folgenden Dateien die Zeile `#include <stdint.h>` hinzugefügt werden:

```
gsm-receiver/src/lib/decoder/openbtsstuff/GSMCommon.h
gsm-receiver/src/lib/decoder/openbtsstuff/Threads.h
gsm-receiver/src/lib/decoder/openbtsstuff/Timeval.h
```

Anschließend kann der `gsm-receiver` kompiliert werden:

```
./bootstrap
./configure
make
```

² GSM-Receiver von Piot Krysik, <http://home.elka.pw.edu.pl/~pkrysik/GSM/gsm-receiver.tar.gz>

A.3. Bluetooth GPS als serieller Port

Um ein bluetooth GPS unter Ubuntu zu installieren müssen die folgenden Schritte vorgenommen werden:

Hardware-Adresse des GPS finden:

```
hcitool scan
```

Die Ausgabe sollte das GPS-Modul mit der Hardware-Adresse anzeigen:

```
00:0B:0D:94:35:20      G-Rays2
```

Serieller Port erstellen:

```
sdptool browse 00:0B:0D:94:35:20
```

In der Datei: `/etc/bluetooth/rfcomm.conf` müssen folgende Zeilen eingetragen werden:

```
rfcomm4 {  
    bind yes;  
    device 00:0B:0D:94:35:20;  
    channel 1;  
    comment "Serial Port";  
}
```

Um die Verbindung zum GPS aufzubauen, wird folgender Befehl verwendet:

```
rfcomm connect 4
```

Der serielle Port steht nun unter `/dev/rfcomm4` bereit.

A.4. gpsd

Installieren

```
sudo apt-get install gpsd libgps-dev gpsd-dbg gpsd-clients
```

Der serielle Port, auf dem der gpsd Dämon die Daten empfängt, wird wie folgt eingestellt:

```
gpsd -n /dev/rfcomm4
```

Die Konfiguration kann mit dem Programm `xgps` getestet werden.

A.5. GSM-Scanner Installation

Abhängigkeiten bereitstellen:

```
sudo apt-get update
sudo apt-get install autoconf libtool libglib2.0-dev \
                    intltool libglademm-2.4-dev libgps-dev
```

Airprobe installieren:

Die Installationsanleitung von Airprobe ist in Kapitel A.2 gegeben. Es muss darauf geachtet werden, dass der **Airprobe** Ordner im gleichen Verzeichnis liegt wie der **GSM-Scanner**. Von Airprobe muss der **gsm-receiver** erfolgreich kompiliert sein.

USRP2 Scripte ohne Root-Rechte:

Normalerweise werden für die Kommunikation zum USRP2 root-Rechte benötigt, da die USRP2-Software ein Spezielles Ethernet-Protokoll verwendet. Um Programme für den USRP2 ohne root-Rechte lauffähig zu machen, kann dem Programm **usrp2_socket_opener** root-Ausführungsrechte gegeben werden:

```
sudo chmod u+s /usr/local/bin/usrp2_socket_opener
```

Zusätzlich muss real-time scheduling für den USRP aktiviert werden, indem in der Datei **/etc/security/limits.conf** die folgende Zeile hinzugefügt wird:

```
@usrp - rtprio 50
```

Der verwendete Benutzer muss Mitglied der Gruppe **usrp** sein. Die Änderungen werden erst nach einem Aus- und wieder Einloggen aktiv.

GSM-Scanner kompilieren

```
./bootstrap
./configure
make
```

Der **GSM-Scanner** muss auf dem Stammverzeichnis **gsm-scanner/** aufgerufen werden.

Beispiel: **src/gsm_scanner**

B. Ergebnisse der Lokalisierung

Es wurden insgesamt vier Lokalisierungen mit dem O₂ Handy-Finder durchgeführt. Die Ergebnisse sind in Abbildung B.1 als Karten dargestellt. Die Entfernung zum korrekten Aufenthaltsort ist in jedem der Ortungsergebnisse gleich groß und beträgt 270 m. Der Standort des lokализierten Mobilfunktelefons war Hermann-Herder-Str.10 in 79104 Freiburg und ist auf den Karten als roter Punkt eingezeichnet. Der “Handy-Finder” ist für Kunden von O₂ kostenlos zugänglich. Er ermöglicht die Lokalisierung des eigenen Mobilfunktelefons.

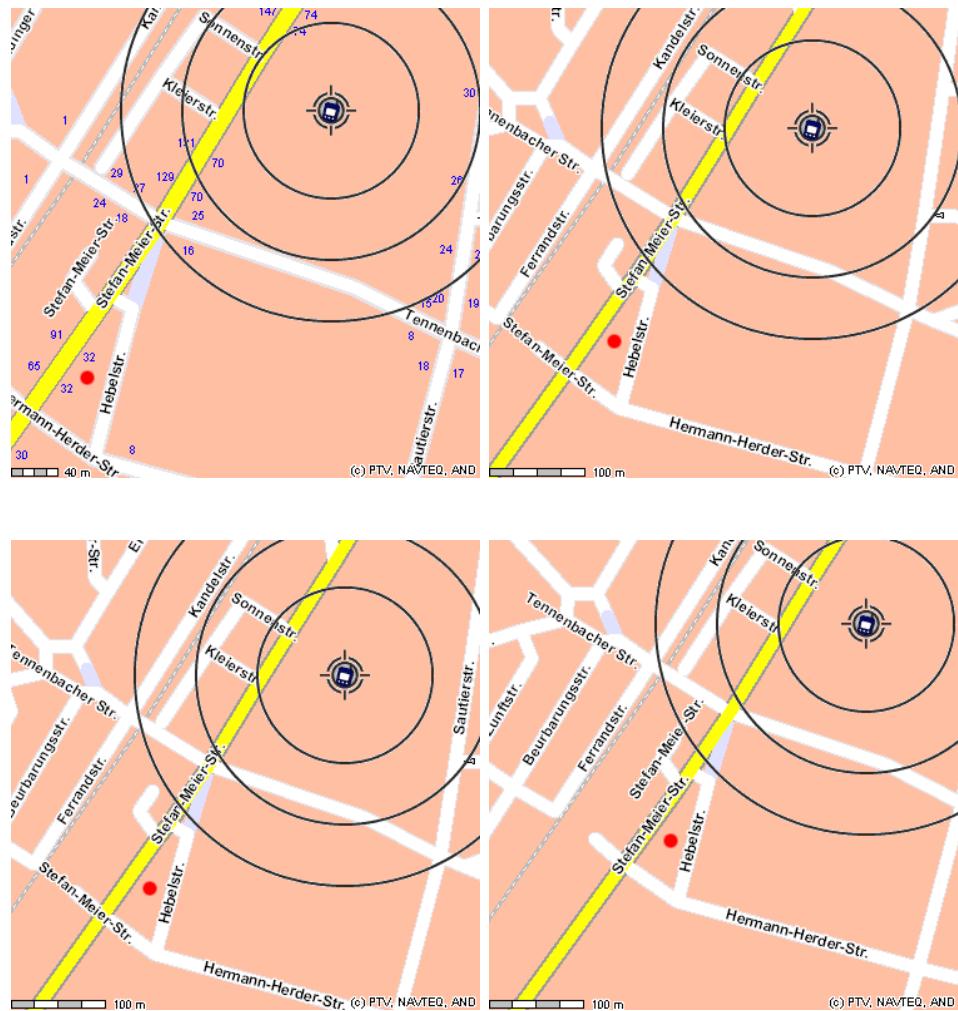


Abbildung B.1.: Ergebnis der netzseitigen Lokalisierung über den O₂ Handy-Finder

C. Beispiel-Snapshot des GSM-Scanners

Die vom **GSM-Scanner** empfangenen BTS können über die Schaltfläche "Save Snapshot" in einer Textdatei im CSV-Format gespeichert werden. Das Trennzeichen zwischen den Spalten ist ein Tabulator. Die folgende Ausgabe wurde in der Hermann-Herder-Str. 10 in 79104 Freiburg augezeichnet:

ARFCN	MCC	MNC	LAC	CID	SNR
1	262	Vodafone	793	15081	12.6076
2	262	Vodafone	793	19232	8.5364
10	262	Vodafone	793	9601	11.5646
18	262	T-Mobile	29191	6326	18.5044
35	262	T-Mobile	29191	8432	10.5497
41	262	T-Mobile	29191	47562	5.22143
60	262	Vodafone	793	15082	13.0892
64	262	Vodafone	793	6913	14.0305
77	262	Vodafone	793	20483	10.3105
78	262	Vodafone	793	19771	10.4384
79	262	Vodafone	793	21783	9.46275
100	262	T-Mobile	29191	16023	12.7119
104	262	Vodafone	793	58641	16.0155
107	262	Vodafone	793	21782	20.6841
109	262	Vodafone	793	21721	8.61312
113	262	Vodafone	793	20482	13.7537
659	262	02	50945	19753	9.06804
665	262	02	50945	39556	15.128
685	262	02	50945	49790	19.8975
686	262	02	50945	39753	28.6561
688	262	02	50945	9790	23.5985
694	262	02	50945	29804	9.04963
789	262	E-Plus	588	11758	28.59
800	262	E-Plus	588	11768	30.3136
830	262	E-Plus	588	55268	10.2142
838	262	E-Plus	588	36658	8.77891
848	262	E-Plus	588	32988	12.9886
852	262	E-Plus	588	32978	5.44955
860	262	E-Plus	588	7108	6.3782
984	262	E-Plus	588	8158	8.34599
997	262	E-Plus	588	55248	21.3123
1012	262	02	50945	41218	9.28821

D. Modifikationen am DBSRX-Daughterboard

Das DBSRX-Daughterboard wurde für den USRP1 entwickelt und muss modifiziert werden, um mit dem USRP2 zu funktionieren. Für die Modifikation wird ein USRP1 benötigt.

Es sind zwei Schritte notwendig:

- Das DBSRX-Daughterboard auf Seite A des USRP1 einbauen. In den GNU Radio Quellen liegt im Verzeichnis `usrp\host\apps\` das Programm `burn-db-eeprom`. Mit folgendem Befehl wird die Firmware des DBSRX geändert:
`./burn-db-eeprom -F -A -t dbsrx_clkmod`
- Im zweiten Schritt wird das Daughterboard ausgebaut und auf der Rückseite der Widerstand R193 entlötet und im freien Platz R194 eingelötet. Der Platz R194 befindet sich links unter R193 und ist frei. Abbildung D.1 verdeutlicht das Umlöten des Widerstandes.

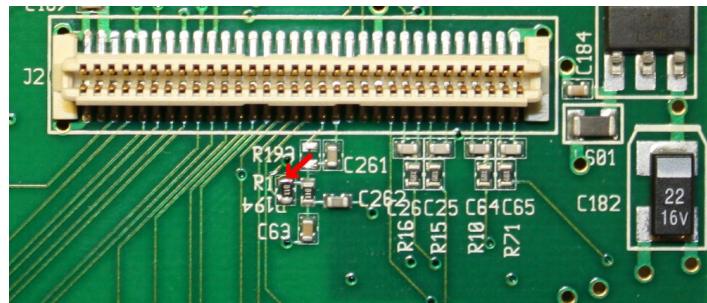


Abbildung D.1.: Umlöten des Widerstandes beim DBSRX-Daughterboard

E. EGSM900 BTS Kanäle und Frequenzen

ARFCN	Frequenz	ARFCN	Frequenz	ARFCN	Frequenz	ARFCN	Frequenz
1	935.2	32	941.4	63	947.6	94	953.8
2	935.4	33	941.6	64	947.8	95	954.0
3	935.6	34	941.8	65	948.0	96	954.2
4	935.8	35	942.0	66	948.2	97	954.4
5	936.0	36	942.2	67	948.4	98	954.6
6	936.2	37	942.4	68	948.6	99	954.8
7	936.4	38	942.6	69	948.8	100	955.0
8	936.6	39	942.8	70	949.0	101	955.2
9	936.8	40	943.0	71	949.2	102	955.4
10	937.0	41	943.2	72	949.4	103	955.6
11	937.2	42	943.4	73	949.6	104	955.8
12	937.4	43	943.6	74	949.8	105	956.0
13	937.6	44	943.8	75	950.0	106	956.2
14	937.8	45	944.0	76	950.2	107	956.4
15	938.0	46	944.2	77	950.4	108	956.6
16	938.2	47	944.4	78	950.6	109	956.8
17	938.4	48	944.6	79	950.8	110	957.0
18	938.6	49	944.8	80	951.0	111	957.2
19	938.8	50	945.0	81	951.2	112	957.4
20	939.0	51	945.2	82	951.4	113	957.6
21	939.2	52	945.4	83	951.6	114	957.8
22	939.4	53	945.6	84	951.8	115	958.0
23	939.6	54	945.8	85	952.0	116	958.2
24	939.8	55	946.0	86	952.2	117	958.4
25	940.0	56	946.2	87	952.4	118	958.6
26	940.2	57	946.4	88	952.6	119	958.8
27	940.4	58	946.6	89	952.8	120	959.0
28	940.6	59	946.8	90	953.0	121	959.2
29	940.8	60	947.0	91	953.2	122	959.4
30	941.0	61	947.2	92	953.4	123	959.6
31	941.2	62	947.4	93	953.6	124	959.8
975	925.2	988	927.8	1000	930.2	1012	932.6
976	925.4	989	928.0	1001	930.4	1013	932.8
977	925.6	990	928.2	1002	930.6	1014	933.0
978	925.8	991	928.4	1003	930.8	1015	933.2
979	926.0	992	928.6	1004	931.0	1016	933.4
980	926.2	993	928.8	1005	931.2	1017	933.6
981	926.4	994	929.0	1006	931.4	1018	933.8
982	926.6	995	929.2	1007	931.6	1019	934.0
983	926.8	996	929.4	1008	931.8	1020	934.2
984	927.0	997	929.6	1009	932.0	1021	934.4
985	927.2	998	929.8	1010	932.2	1022	934.6
986	927.4	999	930.0	1011	932.4	1023	934.8
987	927.6						

F. GSM1800 BTS Kanäle und Frequenzen

ARFCN	Frequenz	ARFCN	Frequenz	ARFCN	Frequenz	ARFCN	Frequenz
512	1805.2	606	1824.0	700	1842.8	793	1861.4
513	1805.4	607	1824.2	701	1843.0	794	1861.6
514	1805.6	608	1824.4	702	1843.2	795	1861.8
515	1805.8	609	1824.6	703	1843.4	796	1862.0
516	1806.0	610	1824.8	704	1843.6	797	1862.2
517	1806.2	611	1825.0	705	1843.8	798	1862.4
518	1806.4	612	1825.2	706	1844.0	799	1862.6
519	1806.6	613	1825.4	707	1844.2	800	1862.8
520	1806.8	614	1825.6	708	1844.4	801	1863.0
521	1807.0	615	1825.8	709	1844.6	802	1863.2
522	1807.2	616	1826.0	710	1844.8	803	1863.4
523	1807.4	617	1826.2	711	1845.0	804	1863.6
524	1807.6	618	1826.4	712	1845.2	805	1863.8
525	1807.8	619	1826.6	713	1845.4	806	1864.0
526	1808.0	620	1826.8	714	1845.6	807	1864.2
527	1808.2	621	1827.0	715	1845.8	808	1864.4
528	1808.4	622	1827.2	716	1846.0	809	1864.6
529	1808.6	623	1827.4	717	1846.2	810	1864.8
530	1808.8	624	1827.6	718	1846.4	811	1865.0
531	1809.0	625	1827.8	719	1846.6	812	1865.2
532	1809.2	626	1828.0	720	1846.8	813	1865.4
533	1809.4	627	1828.2	721	1847.0	814	1865.6
534	1809.6	628	1828.4	722	1847.2	815	1865.8
535	1809.8	629	1828.6	723	1847.4	816	1866.0
536	1810.0	630	1828.8	724	1847.6	817	1866.2
537	1810.2	631	1829.0	725	1847.8	818	1866.4
538	1810.4	632	1829.2	726	1848.0	819	1866.6
539	1810.6	633	1829.4	727	1848.2	820	1866.8
540	1810.8	634	1829.6	728	1848.4	821	1867.0
541	1811.0	635	1829.8	729	1848.6	822	1867.2
542	1811.2	636	1830.0	730	1848.8	823	1867.4
543	1811.4	637	1830.2	731	1849.0	824	1867.6
544	1811.6	638	1830.4	732	1849.2	825	1867.8
545	1811.8	639	1830.6	733	1849.4	826	1868.0
546	1812.0	640	1830.8	734	1849.6	827	1868.2
547	1812.2	641	1831.0	735	1849.8	828	1868.4
548	1812.4	642	1831.2	736	1850.0	829	1868.6
549	1812.6	643	1831.4	737	1850.2	830	1868.8
550	1812.8	644	1831.6	738	1850.4	831	1869.0
551	1813.0	645	1831.8	739	1850.6	832	1869.2
552	1813.2	646	1832.0	740	1850.8	833	1869.4
553	1813.4	647	1832.2	741	1851.0	834	1869.6
554	1813.6	648	1832.4	742	1851.2	835	1869.8
555	1813.8	649	1832.6	743	1851.4	836	1870.0
556	1814.0	650	1832.8	744	1851.6	837	1870.2
557	1814.2	651	1833.0	745	1851.8	838	1870.4
558	1814.4	652	1833.2	746	1852.0	839	1870.6

F. GSM1800 BTS Kanäle und Frequenzen

ARFCN	Frequenz	ARFCN	Frequenz	ARFCN	Frequenz	ARFCN	Frequenz
559	1814.6	653	1833.4	747	1852.2	840	1870.8
560	1814.8	654	1833.6	748	1852.4	841	1871.0
561	1815.0	655	1833.8	749	1852.6	842	1871.2
562	1815.2	656	1834.0	750	1852.8	843	1871.4
563	1815.4	657	1834.2	751	1853.0	844	1871.6
564	1815.6	658	1834.4	752	1853.2	845	1871.8
565	1815.8	659	1834.6	753	1853.4	846	1872.0
566	1816.0	660	1834.8	754	1853.6	847	1872.2
567	1816.2	661	1835.0	755	1853.8	848	1872.4
568	1816.4	662	1835.2	756	1854.0	849	1872.6
569	1816.6	663	1835.4	757	1854.2	850	1872.8
570	1816.8	664	1835.6	758	1854.4	851	1873.0
571	1817.0	665	1835.8	759	1854.6	852	1873.2
572	1817.2	666	1836.0	760	1854.8	853	1873.4
573	1817.4	667	1836.2	761	1855.0	854	1873.6
574	1817.6	668	1836.4	762	1855.2	855	1873.8
575	1817.8	669	1836.6	763	1855.4	856	1874.0
576	1818.0	670	1836.8	764	1855.6	857	1874.2
577	1818.2	671	1837.0	765	1855.8	858	1874.4
578	1818.4	672	1837.2	766	1856.0	859	1874.6
579	1818.6	673	1837.4	767	1856.2	860	1874.8
580	1818.8	674	1837.6	768	1856.4	861	1875.0
581	1819.0	675	1837.8	769	1856.6	862	1875.2
582	1819.2	676	1838.0	770	1856.8	863	1875.4
583	1819.4	677	1838.2	771	1857.0	864	1875.6
584	1819.6	678	1838.4	772	1857.2	865	1875.8
585	1819.8	679	1838.6	773	1857.4	866	1876.0
586	1820.0	680	1838.8	774	1857.6	867	1876.2
587	1820.2	681	1839.0	775	1857.8	868	1876.4
588	1820.4	682	1839.2	776	1858.0	869	1876.6
589	1820.6	683	1839.4	777	1858.2	870	1876.8
590	1820.8	684	1839.6	778	1858.4	871	1877.0
591	1821.0	685	1839.8	779	1858.6	872	1877.2
592	1821.2	686	1840.0	780	1858.8	873	1877.4
593	1821.4	687	1840.2	781	1859.0	874	1877.6
594	1821.6	688	1840.4	782	1859.2	875	1877.8
595	1821.8	689	1840.6	783	1859.4	876	1878.0
596	1822.0	690	1840.8	784	1859.6	877	1878.2
597	1822.2	691	1841.0	785	1859.8	878	1878.4
598	1822.4	692	1841.2	786	1860.0	879	1878.6
599	1822.6	693	1841.4	787	1860.2	880	1878.8
600	1822.8	694	1841.6	788	1860.4	881	1879.0
601	1823.0	695	1841.8	789	1860.6	882	1879.2
602	1823.2	696	1842.0	790	1860.8	883	1879.4
603	1823.4	697	1842.2	791	1861.0	884	1879.6
604	1823.6	698	1842.4	792	1861.2	885	1879.8
605	1823.8	699	1842.6				

G. CD-Inhalt

Auf der CD befinden sich die folgenden Ordner:

airprobe
gsm-scanner
masterarbeit
patch

Der Ordner **airprobe** enthält die beiden Programme **gsm-receiver** und **gsmdecoder** aus dem Airprobe-Projekt. Der hier gespeicherte **gsm-receiver** ist die verbesserte Version von Piot Krysik. Die im Ordner **patch** abgelegten Patches für den **gsm-receiver** sind bereits angewendet.

Im Ordner **gsm-scanner** ist das entwickelte Programm abgelegt.

Zur Installation der Programme bitte die Installationsanleitungen im Anhang A beachten.

Die Masterarbeit im PDF-Format ist im Ordner **masterarbeit** zu finden. Die für die Arbeit erstellten Bilder sind im gleichen Verzeichnis abgelegt.