ingenieur
wissenschaften
htw saar

Hochschule für
Technik und Wirtschaft
des Saarlandes
University of
Applied Sciences

Zusammenfassung des TK-Praktikum des sechsten Semesters Kommunikationsinformatik

Praktikum

Deniz Kadiogullari und Christoph Drost

Erstgutachter: Harald Krauss

Zusammenfassung

Kurze Zusammenfassung des Inhaltes in deutscher Sprache, der Umfang beträgt zwischen einer halben und einer ganzen DIN A4-Seite.

Orientieren Sie sich bei der Aufteilung bzw. dem Inhalt Ihrer Zusammenfassung an Kent Becks Artikel: http://plg.uwaterloo.ca/~migod/research/beckOOPSLA.html.

Inhaltsverzeichnis

1 GSM Versuch

1.1 Allgemeine Beschreibung der Versuche

Im folgenden handelt es sich um ein Test-Versuch GSM. GSM ist die Abkürzung für Global System for Mobile Communications und ein Standard für die volldigitale Mobilfunknetze. Wir haben ihn bereits kennen gelernt, da alle unsere Handys darauf beruhen. GSM ermöglicht die eigentliche Telefonie, eine Datenübertragung und das Versenden und Empfangen von SMS, Short Message Services. Mittlerweile wurden für die Datenübertragung leistungsfähigere Standards, wie UMTS und LTE entwickelt, jedoch ist GSM noch nicht wegzudenken.

Der Versuch soll das Verständnis für die Technik vertiefen, die den reibungslosen Ablauf unserer Handygespräche ermöglicht. Zu diesem Zweck steht uns ein System zur Verfügung, das aus einer Antenne, der Technik zur Signalverarbeitung und einem Computer mit entsprechender Software besteht.

1.1.1 Versuchsaufbau

Der Aufbau des Versuchs ist auf den ersten Blick leicht beschrieben: Unser System besteht aus einer Antenne **??**, einem USPR **??** und einem Computer **??**.

1.1.2 Die einzelnen Bauteile im Überblick

1.1.2.1 Antenne

Dieses Bauteil wandelt die elektromagnetischen Signale in elektrische Signale um. Antennen sind in prinzipiell in allen Geräten enthalten, die etwas mit Funktechnik zu tun haben. Dazu zählen beispielsweise Radios oder auch Handys. Die Umwandlung hat den Hintergrund, dass die elektromagnetischen Single aus der Luft nicht direkt weiterverarbeitet werden können.

1.1.2.2 USPR

Das USPR, Universal Radio Peripheral, ist eine geschlossene Einheit, die das Verarbeiten der Empfangenen Signale ermöglicht. Es ist modular aufgebaut, sodass ein breites Frequenzspektrum abgedeckt werden kann. Für unseren Versuch interessieren aber nur die Frequenzen des GSM. Das USPR wird im folgenden nicht weiter betrachtet, da es nicht der Gegenstand des Versuchs war, sondern diesen nur ermöglicht hat.

Abbildung 1.1: USPR mit Antenne

1.1.2.3 Computer

Der Computer mit seiner entsprechenden Software ist die für den Versuch am interessanteste Komponente. Er ermöglicht es, die empfangenen Funksignale grafisch darzustellen und auszuwerten. Weiterhin stellt der Computer die Protokolle für den reibungslosen Ablauf und eine vollwertige U_m Schnittstelle zur Verfügung.

Zur Bereitstellung dieser Schnittstelle und der Protokolle wird das Softwarepaket OpenBTS genutzt.

Das Ziel des Versuchs ist es, die Paketdaten mitzuschneiden, die in einem GSM Netz auftreten. Vor dem Mitschnitt soll ein Grundverständnis über die Physik hinter dem GSM Netz geschaffen werden.

1.2 Visualisieren von Frequenzen

1.2.1 Frequenzen auflisten

1.2.1.1 Aufbau des Versuchs

Für die Visualisierung der Frequenzen werden die in **??** beschriebenen Komponenten benötigt. Aus der Softwarepaket OpenBTS werden die Tools lsursp, baudline und kal benötigt.

Neben der vorhandenen Hardware werden keine weiteren Geräte benötigt. Das Vorhandensein von Sendern in der Reichweite des Systems ist dennoch eine Vorraussetzung.

1.2.1.2 Versuchsdurchführung

Mit dem Tool lsursp wird überprüft, ob die USPR **??** vom System erkannt wird.

Nachdem festgestellt wurde, dass die USRP angeschlossen und vom System erkannt wurde, kann der eigentliche Versuch beginnen. Hierzu wird das Tool kal mit dem Kommando „kal -s -DCS“aufgerufen. Kal führt einen Umgebungsscan durch, das bedeutet, dass alle Frequenzen, die im DCS 1800 Band liegen und empfangen werden können, aufgelistet werden können.

1.2.1.3 Auswertung des Versuchs

Zur Erklärung, das DCS 1800 Band ist ein Frequenzband, das den Frequenzbereich um 1800 MHz nutzt. In Deutschland wurde dieser Bereich ursprünglich von den E-Netzen, also dien Anbietern E-Plus und O_2 genutzt. Aus Kapazitätsmangel haben 1999 auch die großen D-Netz Betreiber DCS 1800 Frequenzen erworben. Der Umgebungsscan gibt also die Frequenzen aus, die mit GSM zu tun haben, auf einen Anbieter ist der Scan aber nicht beschränkt. Das Ergebnis der Umgebungsscans ist in Tabelle **??** aufgelistet. Jede Zeile dieser Auflistung besteht aus chan mit Frequenzen und power mit einem Wert.

Quellen finden

chan Chan steht in diesem Fall für channel oder channel number. Dieser Wert wird auch als ARFCN, Absolute Radio Frequency Channel Number, bezeichnet. Der Hintergrund ist, dass ein Teilnehmer des GSM Netzes nicht das gesamte Frequenzband benötigt. Bzw. auch, dass andere Kommunikationsteilnehmer einer Base Station ausgeschlossen werden, wenn ein Teilnehmer exklusiv das gesamte Frequenzband nutzt. Deswegen werden die Frequenzbänder in Kanäle (channels), bzw. Kanalpaare, unterteilt. Das Kanalpaar hat den Hintergrund, dass GSM für den Down- und des Uplink unterschiedliche Frequenzen nutzt. Anhand der ARFCN kann die absolute Frequenz berechnet werden, die für die tatsächliche Kommunikation genutzt wird. Die Formel

chan:	555 (1813.8 MHz + 14.632kHz)	power: 1007.18
chan:	602 (1823.2MHz - 8.896kHz)	power 481.48
chan:	619 (1826.6MHz + 572Hz)	power: 1171.37
chan:	620 (1826.8 + 347Hz)	power: 727.63
chan:	630 (1828.8MHz + 177Hz)	power: 1421.75
chan:	631 (1820.0MHz + 209Hz)	power: 2495.22
chan:	637 (1830.2MHz + 403Hz)	power: 2876.83
chan:	640 (1830.8MHz + 508Hz)	power: 36384.61
chan:	641 (1831.0MHz + 508Hz)	power: 8809.88
chan:	647 (1832.2MHz - 32.386Hz)	power: 1305.97
chan:	648 (1832.4MHz - 32470Hz)	power: 10507.76
chan:	700 (1842.8MHz + 386Hz)	power: 21662.59
chan:	701 (1843.0MHz + 455Hz)	power: 4220.36
chan:	706 (1844.0MHz + 387Hz)	power: 27836.79
chan:	709 (1844.6MHz + 2.954Hz)	power: 1148.92
chan:	713 (1845.4MHz + 621Hz)	power: 6744.54
chan:	715 (1845.8MHz + 388Hz)	power: 20091.07
chan:	755 (1853.8MHz - 20.894Hz)	power: 458.32
chan:	764 (1855.6MHz + 485Hz)	power: 19349.83
chan:	765 (1855.8MHz + 381Hz)	power: 9962.32
chan:	769 (1856.6MHz + 38.177Hz)	power: 3226.76
chan:	798 (1862.4MHz + 498Hz)	power: 994.82
chan:	802 (1863.2MHz + 498Hz)	power: 118213.39
chan:	805 (1863.8MHz + 440Hz)	power: 5598.97

Tabelle 1.1: Auflistung der empfangenen Frequenzen

dazu ist in der Abbildung **??** beschrieben. Auf diese Thematik wird aber im weiteren Verlauf des Versuchs weiter eingegangen.

Den Scheiß habe ich mir quasi ausgedacht. Stimmt das annähernd?

power Power ist die Stärke, mit der das Signal empfangen wurde. Keine Ahnung welche Einheit.

Berechnung der Frequenzen Wie schon erwähnt, anhand dieser Auflistung ist es möglich, den Frequenzbereichs von DCS 1800 zu errechnen. Zur Berechnung eines Frequenzbereichs gibt es einige Formeln. Welche genutzt wird, hängt davon ab, welche Werte bereits bekannt sind.

Dazu was richtiges schreiben

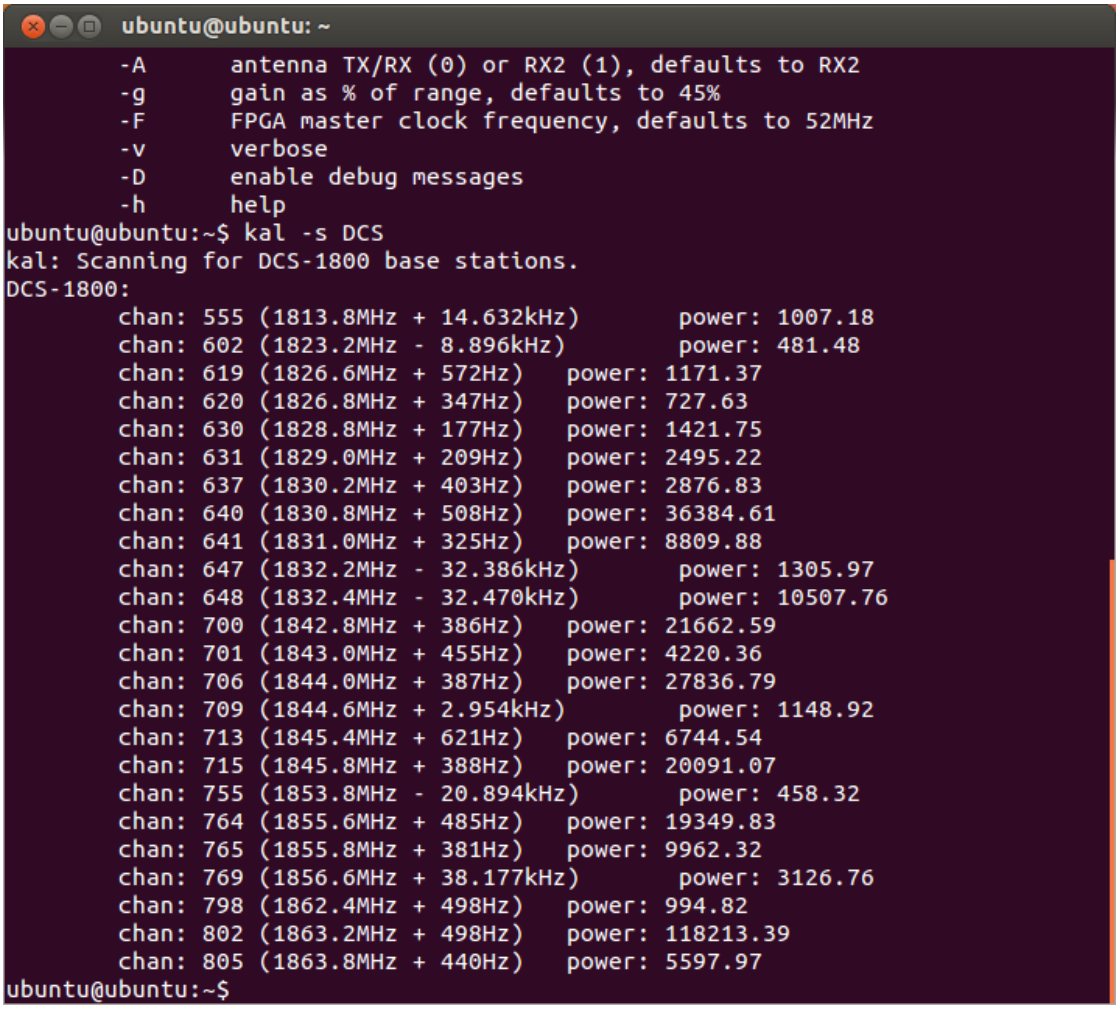

Abbildung 1.2: Screenshot des Umgebungsscans

fuplink = Startfrequenz + (ARFCN -Offset) * 0,2MHz
fdownlink = fuplink + Abstand
fuplink = fdownlink - Abstand
ARFCN = (fuplink - Startfrequenz/0,2 MHZ) + Offset

Tabelle 1.2: Formel zur Berechnung des Frequenzbereichs

Da in unserem Versuch die Antenne als reiner Empfänger gearbeitet hat, haben wir nur Frequenzen empfangen, die von den Sendern als Uplink Frequenzen genutzt werden.

Die empfangenen Frequenzen lassen sich auch einzelnen Providern zuordnen. Für diese Zuordnungen gibt es Pläne, welche Frequenzen an wen vergeben wurden. Auf

Was zur Berechnung schreiben

der folgenden Abbildung ist zu sehen welche Frequenzen in Deutschland von welchem Providern benutzt werden.

	von (MHz)	bis (MHz)	Kurzzeichen	Sendeleistung	Reichweite	Modulation	Gepulst	Betreiber	Sonstiges	Beschreibung
	1.710,0	1.725,0	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	Militär	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.725,2	1.730,0	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	T-Mobile	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.730,2	1.752,4	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	O 2	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.752,8	1.758,0	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	Vodafone	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.758,2	1.780,4	GSM 1800 (UL)	1W ERP (Peak)	16km	GMSK	JA	E Plus	Pulsung mit 217Hz. Leistung schwankt von 25mW-1W (Peak)	Mobilfunk (E-Netz)
	1.805,0	1.820,0	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	Militär	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)
	1.820,2	1.825,0	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	T-Mobile	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)
	1.825,0	1.847,4	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	O 2	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)
	1.847,8	1.853,0	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	Vodafone	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)
	1.853,2	1.875,4	GSM 1800 (DL)	300W ERP	16km	GMSK	JA	E Plus	Pulsungen mit 217Hz. Organisationskanal mit 1.736Hz. Leistungen von 0,5-300W ERP möglich	Mobilfunk (E-Netz)

Militär
T-Mobile
O2
Vodafone
e-plus

Abbildung 1.3: Frequenzentabelle der Provider [1]

Wenn man die Tabelle **??** und die Grafik **??** vergleicht, ergibt sich Tabelle **??**. Auffällig ist, dass keine Signale des Anbieters Vodafone empfangen werden, dafür aber mehrere militärische Kanäle.

1.2.2 Frequenzen darstellen

Der Versuch **??** hat ergeben, dass im GSM Standard verschiedene Frequenzen genutzt werden. Die Tatsache, dass Kanäle mit einer Breite genutzt werden, wirft die Frage auf, was es mit diesen Breiten auf sich hat und wie Informationen übertragen werden.

1.2.2.1 Aufbau des Versuchs

Der Aufbau des Versuchs entspricht grob dem Aufbau des Versuchs **??**. Anstelle des Tools kal wird DSP-Buttler-Tool dsusrp genutzt.

1.2.2.2 Versuchsdurchführung

Vor Beginn des Versuchs muss der Umgebungsscan aus **??** wiederholt werden. Dadurch kann sicher gestellt werden, dass die Messung mit einer aktiven, bzw. gerade gesendeten Frequenz durchgeführt wird. Nachdem eine Frequenz gefunden wurde, beginnt

chan:	555 1813.8 MHz	Militär
chan:	602 1823.2MHz	T-Mobile
chan:	619 1826.6MHz	O_2
chan:	620 1826.8 + 347Hz	O_2
chan:	630 1828.8MHz	O_2
chan:	631 1820.0MHz	Militär
chan:	637 1830.2MHz	O_2
chan:	640 1830.8MHz	O_2
chan:	641 1831.0MHz	O_2
chan:	647 1832.2MHz	O_2
chan:	648 1832.4MHz	O_2
chan:	700 1842.8MHz	O_2
chan:	701 1843.0MHz	O_2
chan:	706 1844.0MHz	O_2
chan:	709 1844.6MHz	O_2
chan:	713 1845.4MHz	O_2
chan:	715 1845.8MHz	O_2
chan:	755 1853.8MHz	E-Plus
chan:	764 1855.6MHz	E-Plus
chan:	765 1855.8MHz	E-Plus
chan:	769 1856.6MHz	E-Plus
chan:	798 1862.4MHz	E-Plus
chan:	802 1863.2MHz	E-Plus
chan:	805 1863.8MHz	E-Plus

Tabelle 1.3: Auflistung der empfangenen Frequenzen

der eigentliche Versuch mit dem Kommando *dbusrp-f 699219*. Dieses Kommando startet ein Analysetool, das sowohl den Frequenz- als auch den Amplitudenbereich ausgibt.

1.2.2.3 Auswertung des Versuchs

Das Ergebnis dieses Versuchs kann in der Grafik **??** betrachtet werden. Die Wellen im oberen Bereich der Darstellung sind die Darstellung im Zeitbereich, die unteren Wellen sind die Darstellung im Frequenzbereich. In der Mitte wird das Signal im Wasserfallmodell darstellt. Das Wasserfallmodell zeigt wie sich die Grundfrequenz durch abziehen oder hinzufügen von Frequenzen verändert wird. Die Darstellung des Signal erinnert stark an weißes Rauschen

Wat han mir wei davon?

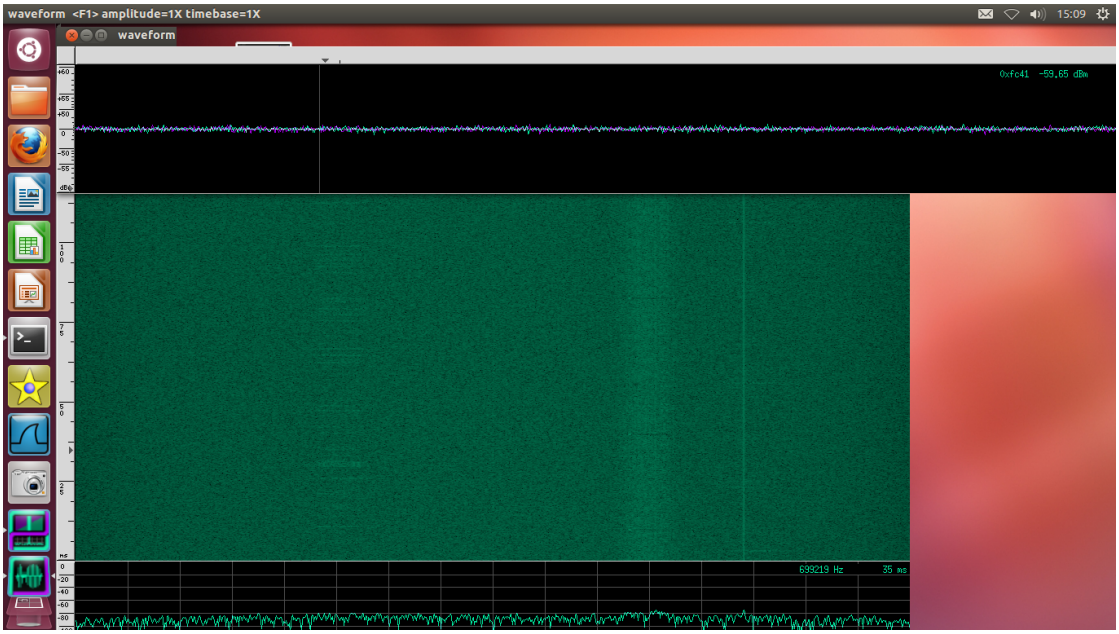

Abbildung 1.4: Eine visualisierte Frequenz

1.3 Anruf an die 2600

Es soll ein Anruf auf die 2600 was dem echo-Dienst entspricht durchgeführt werden. Dazu benötigen wir den am Anfang beschriebenen Versusaufbau sowie ein GSM-Fähiges Mobiltelefon das in dem Netz registriert ist. Als erstes muss das OpenBTS system gestartet werden dies erfolgt über mehrere Konsolen Befehle, da OpenBTS aus mehreren Komponenten besteht. Zuerst muss der Authentication-Service gestartet werden dies erfolgt durch den Befehl sipauthserve. Dannach muss die SMqueue gestartet werden die für die Weiterlietung der SMS verantwortlich ist, mit dem Befehl smqueue wird der Service gestartet. Der eigentliche OpenBTS Service muss ebenfalls gestartet werden. Dieser Dienst stellt den Kern des Systems dar, alle anderen Prozesse agieren mit diesem Prozess. Ausserdem brauchen wir noch den Asterisk Service der bereits in diesem Dokument erklärt worden ist. Diesen starten wir in einer neuen Konsole mit dem Befehl asterisk -r. Alle Befehle müssen als Superuser ausgeführt werden, sonst würden die Berechtigungen dazu fehlen. Um sich in dem Netz mit seinem eigenen Mobiltelefon registrieren zu können wählen wir das entsprechende Netz aus und erhalten unsere IMSI. Nun kann die 2600 angerufen werden und der Versuch durchgeführt werden.

1.4 Datenmitschnitte

Der vorangegangene Versuch sollte die physikalischen Eigenschaften des GSM Standards vermitteln. Der folgende Versuch beschäftigt sich mit den Protokolleigenschaften des GSM. Daher werden Situationen simuliert, die täglich millionenfach in den deutschen GSM Netzen stattfinden. Den Datenverkehr, den diese Situationen verursachen werden wir mitschneiden und analysieren.

1.4.1 Anruf mitschneiden

1.4.1.1 Versuchsaufbau

Die Hardware entspricht der des Versuchs **??**. Der Unterschied liegt in der Software. Diese simuliert ein eigenes GSM Netz. Als Softwarepaket wird Open BTS genutzt, was wieder mit mehreren Softwarekomponenten interagiert. Die für uns relevanten Teile des Open BTS sind im wesentlichen:

- Sipauthserve - Ist für die Authentifizierung verantwortlich
- Smqueue - Ein store-and-forward SIP Server, dient der Weiterleitung von SMS
- Asterisk - Stellt die Telefonanlage zur Verfügung

Diese Software erlaubt in Verbindung mit der Hardware den Betrieb eines eigenen GSM Netzes. Zum Mittschnitt der Daten steht das Tool Wireshark zur Verfügung. Wireshark ist ein Protocol Analyzer, damit ist es möglich einzelne Datenpakete mitzuschneiden.

Die Hardware wird um ein Mobiltelefon erweitert. Dieses ist bereits konfiguriert und registriert. Dieses Mobiltelefon ermöglicht die Kommunikation und Interaktion mit dem GSM Netz.

1.4.1.2 Versuchsdurchführung

Zu Beginn des Versuchs muss die Software gestartet werden. Da die einzelnen Programme untereinander Abhängigkeiten haben, müssen sie in einem Befehl gestartet werden. Der Befehl *sudo sipauthserve & sudo smqueue & sudo OpenBTS & sudo OpenBTSCLI* startet die grundsätzliche Funktionalität des GSM Netzes. Mit dem Befehl *sudo asterisk -r* startet die Vermittlungenlage.

Stimmt das denn auch? Das mit den Abhängigkeiten und gleichzeitigg starten

Nachdem die die Vorbereitungen abgeschlossen sind, steht ein GSM Netz zur Verfügung. Für den Mitschnitt der Daten muss noch Wireshark konfiguriert werden. Hierzu wird das Filter *!(udp port 5700 || udp port 5702 || icmp)* gesetzt. Ein Filter in Wireshark hat den Vorteil, dass beim Datenmitschnitt die umrelevanten Daten herausgefiltert werden können und damit die doch sehr umfangreiche Datenmenge reduziert werden kann.

Der Anruf wird auf die Telefonnummer 2600 getätigt. Diese Telefonnummer ist als echo Kanal konfiguriert, das heißt, dass das Gespräch vom Netz wieder zurück zum Teilnehmer geschickt wird.

Nachdem der Versuch vorbereitet ist, wird über das Mobiltelefon die Nummer 2600 angerufen.

1.4.1.3 Auswertung des Versuchs

Der Echo Kanal funktioniert, wie beschrieben. Die Sprachdaten, die ans Netz gesendet werden, werden wieder vom Netz zurück geschickt.

Hier die Datenpakete, bzw. deren Analyse rein

Wird der Versuch mit einem eigenen Mobiltelefon ausgeführt, muss sich dieses erst an am Netz anmelden. Diese Anmeldung wird vom Netz mit einer SMS bestätigt.

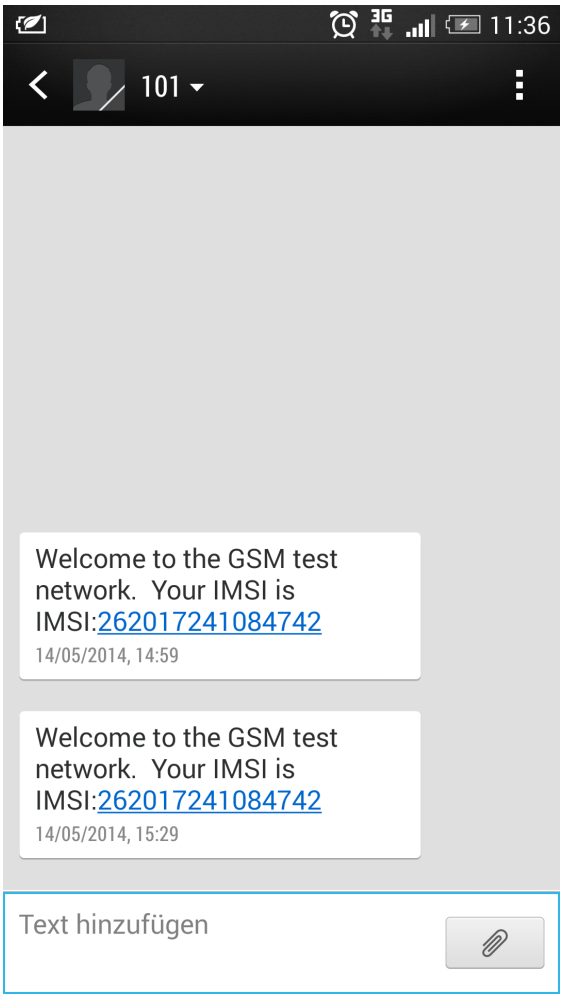

Abbildung 1.5: Quittierung der Einwahl in das GSM Netz

1.5 Mitschnitt einer SMS

1.5.1 Versuchsaufbau

Der Aufbau des Versuchs entspricht dem Aufbau **??**.

1.5.2 Versuchsdurchführung

Die Durchführung entspricht der Durchführung **??**. Anstatt des Anrufs an die Nummer 2600 wird eine SMS mit dem Inhaltt „info “an die Telefonnummer 411 geschickt.

1.5.2.1 Auswertung des Versuchs

Als Antwort auf die SMS erhalten wir eine Antwort mit dem Inhalt der gesendeten SMS sowie weitere Informationen wie Zeiten.

was stand den da noch drin

In der Protokollanalyse sieht man, welche Datenpakete für den Versand einer SMS nötig sind. Die Grafik **??** zeigt das Packet das gesendet wird bei dem Veschicken einer SMS. Wie man schon in der Informationsspalte sehen kann wird die SMS von dem Mobiltelefon(MS) an das Netzwerk(NW) geschickt. In dem Feld TP-USER-DATA kann man sich den geschickten Inhalt ansehen. Was in diesem Fall high ist.

Die Grafik **??** zeigt die gleiche SMS. Der Unterschied ist, dass die SMS vom Netzwerk zum Mobiltelefon geschickt wird.

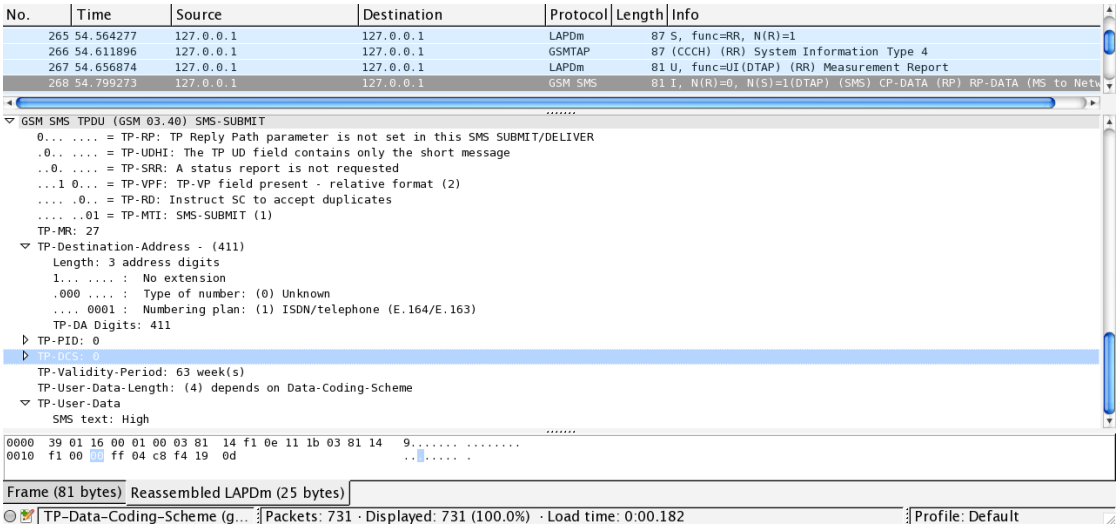

Abbildung 1.6: SMS von Mobilstation an Netzwerk

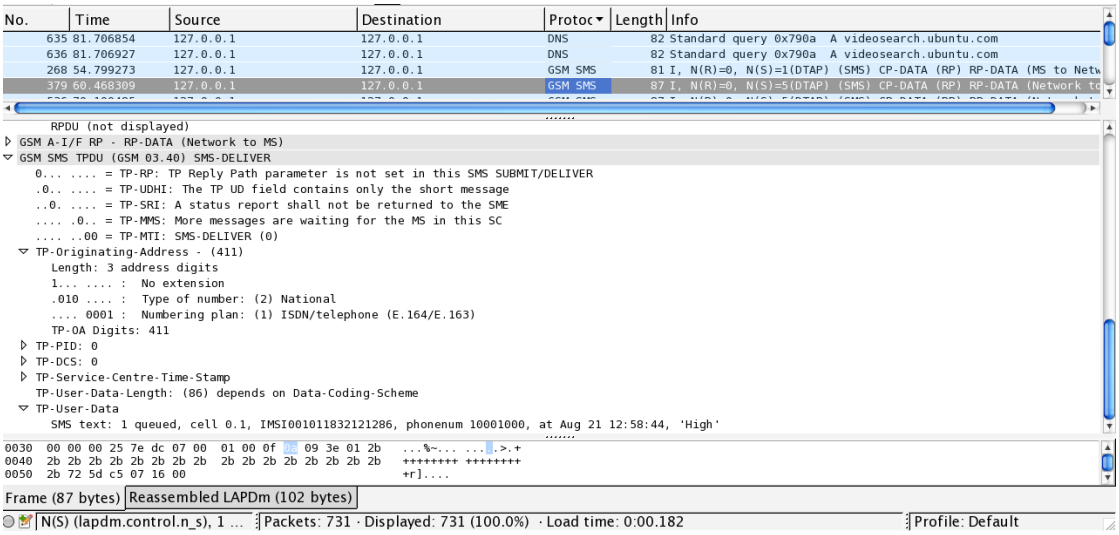

Abbildung 1.7: SMS von Netzwerk an Mobilestation

2 BA Versuch

2.1 Einleitung

2.2 Downlink

2.3 Uplink

2.4 ARFCN

2.5 Untersuchung des Paketflusses mit Wireshark

3 RSP Versuch

3.1 Einleitung

3.2 Switch und Router Konfiguration

3.2.1 Router start up running config

3.3 Packet Tracer

Mit Packet Tracer lassen sich verschiedene Hardware-Szenarien nach spielen und virtuell aufbauen. Es stehen verschiedene Hardware-Produkte zur Verfügung die sich konfigurieren lassen und beliebig verkabeln lassen. Das Folgende Szenario soll erstellt und damit gearbeitet werden.

Abbildung 3.1: SMS von Netzwerk an Mobilestation

3.3.1 Versuchsaufbau

3.3.2 Messungen

3.3.3 Simmulation Echo-Request/-Reply

3.4 Untersuchung des Paketflusses mit Wireshark

4 RSC Versuch

4.1 Einleitung

4.2 Downlink

4.3 Uplink

4.4 ARFCN

4.5 Untersuchung des Paketflusses mit Wireshark

5 SDH Versuch

5.1 Einleitung

5.2 Downlink

5.3 Uplink

5.4 ARFCN

5.5 Untersuchung des Paketflusses mit Wireshark

6 RN Versuch

6.1 Einleitung

6.2 Downlink

6.3 Uplink

6.4 ARFCN

6.5 Untersuchung des Paketflusses mit Wireshark

Literatur

[1] Aaronia AG. *Frequenznutzungsplan GSM 1800*. http://www.aaronia.de/grundlagen/frequenzplaene/fre
gsm1800-de/.

Kolophon

Dieses Dokument wurde mit der LaTeX-Vorlage für Abschlussarbeiten an der htw saar im Bereich Informatik/Mechatronik-Sensortechnik erstellt (Version 1.0). Die Vorlage wurde von Yves Hary und André Miede entwickelt (mit freundlicher Unterstützung von Thomas Kretschmer und Helmut G. Folz).