

**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

Inhaltsverzeichnis	v
Listings	1
1 GSM Versuch	1
1.1 Allgemeine Beschreibung der Versuche	1
1.1.1 Versuchsaufbau	1
1.2 Visualisieren von Frequenzen	1
1.2.1 Versuchsdurchführung	3
1.2.2 Versuchsziel	4
1.3 Anruf an die 2600	4
1.3.1 Versuchsziel	5
1.3.2 Versuchsdurchführung	5
1.4 Beschreibung der Verschiedenen Messungen und Ergebnisdarstellung .	6
1.5 Diskussion der Messergebnisse und Ausarbeiten der Aufgaben	6
1.6 Senden einer SMS an die 411	6
1.6.1 Versuchsdurchführung	6
1.6.2 Versuchsziel	6
1.7 Beschreibung der Verschiedenen Messungen und Ergebnisdarstellung .	6
1.8 Diskussion der Messergebnisse und Ausarbeiten der Aufgaben	6
2 BA Versuch	9
2.1 Einleitung	9
2.2 Downlink	9
2.3 Uplink	9
2.4 ARFCN	9
2.5 Untersuchung des Paketflusses mit Wireshark	9
3 RSP Versuch	11
3.1 Einleitung	11
3.2 Downlink	11
3.3 Uplink	11
3.4 ARFCN	11
3.5 Untersuchung des Paketflusses mit Wireshark	11

4	RSC Versuch	13
4.1	Einleitung	13
4.2	Downlink	13
4.3	Uplink	13
4.4	ARFCN	13
4.5	Untersuchung des Paketflusses mit Wireshark	13
5	SDH Versuch	15
5.1	Einleitung	15
5.2	Downlink	15
5.3	Uplink	15
5.4	ARFCN	15
5.5	Untersuchung des Paketflusses mit Wireshark	15
6	RN Versuch	17
6.1	Einleitung	17
6.2	Downlink	17
6.3	Uplink	17
6.4	ARFCN	17
6.5	Untersuchung des Paketflusses mit Wireshark	17

1 GSM Versuch

1.1 Allgemeine Beschreibung der Versuche

Im folgenden handelt es sich um ein Test-Versuch im Global System for Mobile Communications. Es wird an zwei Baugleichen Systemen gearbeitet die jeweils eine Universal Software Radio Peripheral anbieten (USRP). Das System läuft mit dem Programm OpenBTS und implementiert einen GSM-Protokollstack von Layer 1-3 und terminiert die höheren Schichten. Mit dem System ist es möglich die meisten GSM-Signale abzufangen und mit zu schneiden. Ziel des Versuches ist es die Packetdaten via Wireshark, in dem GSM-Netz von einem Anruf auf den Echo-Server sowie eine SMS an die 411 mit dem Text "info", mit zu schneiden und zu analysieren. Um sich mit den Komponenten und GSM vertraut zu machen werden zu Anfang einige Visuelle und Informative Versuche ausgeführt wie z.B. das Visualisieren von Frequenzen und das Erarbeiten der mathematischen Zusammenhänge der Frequenzen.

1.1.1 Versuchsaufbau

Bestandteile des Versuchsaufbaus sind zwei baugleiche Open Base Transceiver Station Systeme bestehend aus Computer und der USRP. Die USRP ist für den Empfang der Funksignale notwendig. OpenBTS läuft in unserem Fall auf einem Rechner mit Ubuntu als Betriebssystem und besteht aus mehreren Programmen. Das System modifiziert den gewöhnlichen GSM-Netzaufbau. USRP, SDR und OpenBTS übernehmen die Aufgaben von der Base Transceiver Station und dem Base Station Controller, die Aufgabe des Mobile Switching Center wird von dem Asterisk übernommen und verbindet das Netz mit dem IP-Backbone. SDR steht für Software Defined Radio und stellt Signalverarbeitungsbibliotheken zur Verfügung. Es wird ein Mobiltelefon das bereits im Netz registriert ist bereit gestellt, es ist jedoch eben so gut möglich sich mit einem anderen GSM-fähigen Telefon in dem Netz anzumelden. Auf dem OpenBTS System laufen verschiedene Dienste wie etwa der Echo-Dienst der unter der Nummer 2600 bzw. eine Reply-Dienste für SMS unter der 411.

1.2 Visualisieren von Frequenzen

Im folgenden Versuch wird mit Hilfe zweier Tools Frequenzen empfangen und diese visualisiert. Das Tool `kal` scannt alle empfangbaren Frequenzen ab, zeigt deren Downlink sowie ARFCN und die Stärke des empfangenden Signals an. ARFCN steht für Absolute Radio Channel Number durch die man die Down- sowie Uplinkfrequenzen

1 GSM Versuch

berechnen kann. Im GSM 1800 sind die ARFCN von 512 bis 885 zugeordnet. Die geringste Downlinkfrequenz bei GSM 1800 ist 1805,2 MHz. Passend dazu sind die Uplinkfrequenzen in einem Abstand von 95 Mhz, beginnend bei 1710,2 bis 1784,8 Mhz. Jedes Down und Uplink-Paar wird durch die ARFCN gekennzeichnet. Durch das Tool baudline ist es möglich die empfangenen Frequenzen zeitlich zu betrachten. Um die Benutzung zu vereinfachen benutzen wir dbusrp.

Auf 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 1.1: Frequenzentabelle der Provider

Die Berechnungen für die Frequenzen ergeben sich aus der folgenden Formeln

$$f_{\text{uplink}} = \text{Startfrequenz} + (\text{ARFCN} - \text{Offset}) * 0,2\text{MHz}$$

$$f_{\text{downlink}} = f_{\text{uplink}} + \text{Abstand}$$

$$f_{\text{uplink}} = f_{\text{downlink}} - \text{Abstand}$$

$$\text{ARFCN} = (f_{\text{uplink}} - \text{Startfrequenz} / 0,2 \text{ MHz}) + \text{Offset}$$

1.2.1 Versuchsdurchführung

Der Versuch zeigt als erstes die empfangbaren Frequenzen mit Hilfe von kal und führt diese auf. Man suche sich eine möglichst stark presente Frequenz um diese sich visualisieren zu lassen.

```

ubuntu@ubuntu: ~
-A      antenna TX/RX (0) or RX2 (1), defaults to RX2
-g      gain as % of range, defaults to 45%
-F      FPGA master clock frequency, defaults to 52MHz
-v      verbose
-D      enable debug messages
-h      help
ubuntu@ubuntu:~$ kal -s DCS
kal: Scanning for DCS-1800 base stations.
DCS-1800:
chan: 555 (1813.8MHz + 14.632kHz)      power: 1007.18
chan: 602 (1823.2MHz - 8.896kHz)      power: 481.48
chan: 619 (1826.6MHz + 572Hz)         power: 1171.37
chan: 620 (1826.8MHz + 347Hz)         power: 727.63
chan: 630 (1828.8MHz + 177Hz)         power: 1421.75
chan: 631 (1829.0MHz + 209Hz)         power: 2495.22
chan: 637 (1830.2MHz + 403Hz)         power: 2876.83
chan: 640 (1830.8MHz + 508Hz)         power: 36384.61
chan: 641 (1831.0MHz + 325Hz)         power: 8809.88
chan: 647 (1832.2MHz - 32.386kHz)     power: 1305.97
chan: 648 (1832.4MHz - 32.470kHz)     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 + 2.954kHz)      power: 1148.92
chan: 713 (1845.4MHz + 621Hz)         power: 6744.54
chan: 715 (1845.8MHz + 388Hz)         power: 20091.07
chan: 755 (1853.8MHz - 20.894kHz)     power: 458.32
chan: 764 (1855.6MHz + 485Hz)         power: 19349.83
chan: 765 (1855.8MHz + 381Hz)         power: 9962.32
chan: 769 (1856.6MHz + 38.177kHz)     power: 3126.76
chan: 798 (1862.4MHz + 498Hz)         power: 994.82
chan: 802 (1863.2MHz + 498Hz)         power: 118213.39
chan: 805 (1863.8MHz + 440Hz)         power: 5597.97
ubuntu@ubuntu:~$

```

Abbildung 1.2: Anzeige der vorhandenen Frequenzen

Mit dem Befehl `dbusrp -f <die gewählte Frequenz>` lässt sich die Frequenz anschaulich darstellen. Die Frequenzen werden in 3 Bereichen angezeigt. Die obere Anzeige zeigt das Signal im Zeitbereich, unten werden die Spektren der Frequenz dargestellt und mittig nach dem Wasserfallmodell. Das Wasserfallmodell zeigt wie sich die Grundfrequenz durch abziehen oder hinzufügen von Frequenzen verändert wird.

1 GSM Versuch

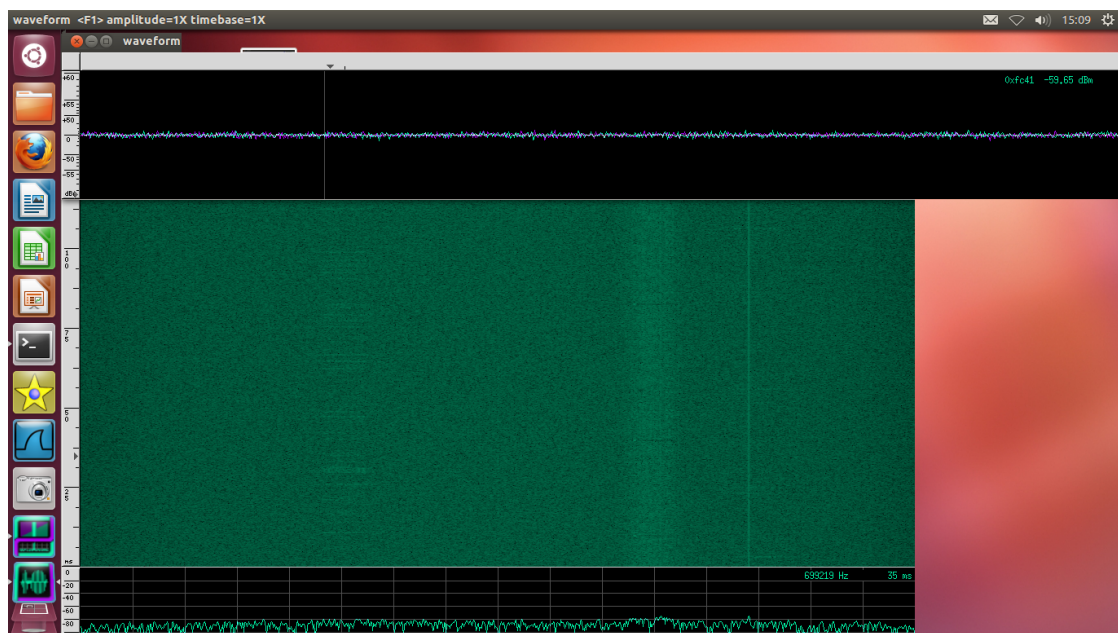


Abbildung 1.3: Eine visualisierte Frequenz

1.2.2 Versuchsziel

Der Versuch gibt einen Allgemeinen Einblick in den Umfang von GSM und veranschaulicht die benutzten Frequenzen. Ausserdem werden die mathematischen Zusammenhänge klarer und GSM an sich verständlicher.

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 Versuchsaufbau 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 Weiterleitung 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.

1.3.1 Versuchsziel

Das Ziel dieses Versuches ist es die mit geschnittenen Daten zu Analysieren und einen Anruf vom Aufbau bis zum Abbau mit zu verfolgen.

1.3.2 Versuchsdurchführung

Nachdem wir uns registriert haben erhalten wir eine SMS mit folgendem Inhalt.

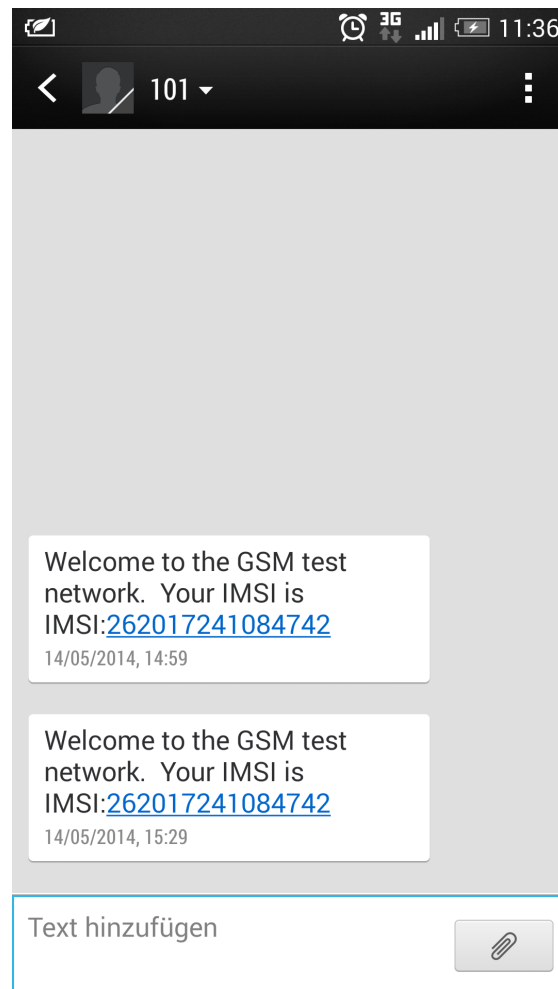


Abbildung 1.4: Einwahl in das GSM Netz

Nun rufen wir die 2600 an und lassen dabei Wireshark mitlaufen um später den Rufaufbau und Datenaustausch mit zu schneiden. Es ertönt eine Stimme und kurz darauf ist der echo-Dienst aktiv und gibt die Sprach-Daten die gesendet werden wieder zurück.

1.4 Beschreibung der Verschiedenen Messungen und Ergebnisdarstellung

1.5 Diskussion der Messergebnisse und Ausarbeiten der Aufgaben

1.6 Senden einer SMS an die 411

Der Selbe Versuch wie mit dem Echo-Dienst wird nun per SMS wiederholt. In diesem Fall sollen die Packetdaten einer SMS mit geschnitten werden und diese Analysiert werden.

1.6.1 Versuchsdurchführung

Da wir bereits im GSM-Netz registriert sind bzw das System gestartet ist, senden wir einfach eine SMS mit dem Inhalt infoän die 411. Als Antwort auf die SMS erhalten wir eine Antwort mit dem Inhalt der gesendeten SMS sowie weitere Informationen wie Zeiten.

1.6.2 Versuchsziel

Der Versuch soll den Ablauf des Senden einer SMS veranschaulichen.

1.7 Beschreibung der Verschiedenen Messungen und Ergebnisdarstellung

Das erste Bild zeigt das Packet das gesendet wird bei dem verschicken 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.

1.7 Beschreibung der Verschiedenen Messungen und Ergebnisdarstellung

No.	Time	Source	Destination	Protocol	Length	Info
265	54.564277	127.0.0.1	127.0.0.1	LAPDM	87 S	func=RR, N(R)=1
266	54.611896	127.0.0.1	127.0.0.1	GSMTAP	87 (CCCH) (RR)	System Information Type 4
267	54.656874	127.0.0.1	127.0.0.1	LAPDM	81 U	func=UI (DTAP) (RR) Measurement Report
268	54.799273	127.0.0.1	127.0.0.1	GSM SMS	81 I, N(R)=0, N(S)=1 (DTAP) (SMS)	CP-DATA (RP) RP-DATA (MS to Netw

GSM SMS TPDU (GSM 03.40) SMS-SUBMIT

- 0... .. = TP-RR: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
- .0... .. = TP-UDHI: The TP UD field contains only the short message
- .0... .. = TP-SRR: A status report is not requested
- ...1 0... = TP-VPF: TP-VP field present - relative format (2)
- 0... = TP-RD: Instruct SC to accept duplicates
-01 = TP-MTI: SMS-SUBMIT (1)
- TP-MR: 27
- TP-Destination-Address - (411)
 - Length: 3 address digits
 - 1... .. : No extension
 - .000 : Type of number: (0) Unknown
 - 0001 : Numbering plan: (1) ISDN/telephone (E.164/E.163)
 - TP-DA Digits: 411
- TP-PID: 0
- TP-DCS: 0
 - TP-Validity-Period: 63 week(s)
 - TP-User-Data-Length: (4) depends on Data-Coding-Scheme
- TP-User-Data
 - SMS text: High

0000 39 01 16 00 01 00 03 81 14 f1 0e 11 1b 03 81 14 9.....
 0010 f1 00 ff 04 c8 f4 19 0d ..

Frame (81 bytes) Reassembled LAPDM (25 bytes)

TP-Data-Coding-Scheme (gsm0340) Packets: 731 · Displayed: 731 (100.0%) · Load time: 0:00:182 Profile: Default

Abbildung 1.5: SMS von Mobilstation an Netzwerk

No.	Time	Source	Destination	Protocol	Length	Info
635	81.706854	127.0.0.1	127.0.0.1	DNS	82	Standard query 0x790a A videosearch.ubuntu.com
636	81.706927	127.0.0.1	127.0.0.1	DNS	82	Standard query 0x790a A videosearch.ubuntu.com
268	54.799273	127.0.0.1	127.0.0.1	GSM SMS	81	I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Netw
379	60.468309	127.0.0.1	127.0.0.1	GSM SMS	87	I, N(R)=0, N(S)=5(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to

RDPD (not displayed)

▶ GSM A-I/F RP - RP-DATA (Network to MS)

▼ GSM SMS TPDU (GSM 03.40) SMS-DELIVER

- 0... .. = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
- .0... .. = TP-UDHI: The TP UD field contains only the short message
- .0... .. = TP-SRI: A status report shall not be returned to the SME
- ...0... = TP-MMS: More messages are waiting for the MS in this SC
- ...00 = TP-MTI: SMS-DELIVER (0)

▼ TP-Originating-Address - (411)

- Length: 3 address digits
- 1... .. : No extension
- .010 ... : Type of number: (2) National
- ...0001 : Numbering plan: (1) ISDN/telephone (E.164/E.163)
- TP-OA Digits: 411

▶ TP-PID: 0

▶ TP-DCS: 0

▶ TP-Service-Centre-Time-Stamp

TP-User-Data-Length: (86) depends on Data-Coding-Scheme

▼ TP-User-Data

SMS text: 1 queued, cell 0.1, IMSI001011832121286, phonenum 10001000, at Aug 21 12:58:44, 'High'

```

0030 00 00 00 25 7e dc 07 00 01 00 0f 09 3e 01 2b ...%...>.+
0040 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b ++++++ ++++++
0050 2b 72 5d c5 07 16 00 +r]....

```

Frame (87 bytes) | Reassembled LAPDm (102 bytes)

N(S) (lapdm.control.n.s), 1 ... Packets: 731 (100.0%) · Load time: 0:00:182

Profile: Default

Abbildung 1.6: 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 Downlink

3.3 Uplink

3.4 ARFCN

3.5 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

Kolophon

Dieses Dokument wurde mit der L^AT_EX-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).