

Projektarbeit im SoSe2017

Konzeption und Aufbau eines Handheld zum Auslesen des BCCH umliegender GSM Basisstationen

von
Dennis Dette und Christian Kobiela



Hochschule Karlsruhe
Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

!!Datum!!

Inhaltsverzeichnis

Abkürzungsverzeichnis	iii
Abbildungsverzeichnis	iv
Tabellenverzeichnis	v
1 Einleitung	1
2 Installationsanleitung	3
2.1 Installation von benötigter Software für gr-gsm	3
2.1.1 Installieren von Kalibrate	3
2.1.2 Zugriff auf USB-Device freischalten	3
2.1.3 Kalibrierung des RTL-SDR Gerätes	4
2.1.4 Installation von GNU Radio	5
2.1.5 Installieren von libosmocore	5
2.2 Installation von gr-gsm	6
3 Bedienung des Handhelds	7
3.1 Stromversorgung	7
3.2 Bedienung über die Desktopoberfläche	8
3.3 Erweitern und Verändern	9

4	Setup des Raspberry PI	12
4.1	Das How To und interdependencies	12
5	Einige Features	14
5.1	Ein Unterabschnitt	14
6	Zusammenfassung	16
7	Ausblick	17

Abkürzungsverzeichnis

UML	Unified Modelling Language
GSM	Global System for Mobile Communications
BTS	Base transceiver station
BCCH	Broadcast control channel

Abbildungsverzeichnis

3.1	Einstellung der automatischen Helligkeitsregelung	8
3.2	Ansicht des Dekstops	9
5.1	Beispielbild	14
5.2	Inkscape Bild mit Text	15

Tabellenverzeichnis

5.1	Beispieltabelle	14
-----	---------------------------	----

Einleitung

Die Aufgabe bestand darin ein Handheld zu konzipieren mit welchem es möglich ist die umgebenden Global System for Mobile Communications (GSM) Base transceiver station (BTS) zu scannen. Durch das Auslesen des Broadcast control channel (BCCH) können die gefundenen Basisstationen beschrieben und charakterisiert werden.

Ein solches System bestand bereits allerdings lief dieses unter Ubunutu und war somit an ein Notebook gebunden. Die Idee war es das Ganze ein wenig mobiler zu gestalten und auch auf den neuesten Stand zu bringen.

Die Verwendung eines DVB-T Sticks sowie der Software Gnuradio wurde vorgeschrieben

Installationsanleitung

Ausführlichere Anleitung und weitere Wiki-Einträge sind hier nachzulesen:
<https://github.com/ptrkrysik/gr-gsm/wiki/Installation-on-RaspberryPi-3>

Installation von benötigter Software für gr-gsm

Installieren von Kalibrate

Als erstes installieren wir Kalibrate:

```
sudo apt-get install libtool autoconf automake libfftw3-dev librtlsdr0 librtlsdr-dev
git clone https://github.com/asdil12/kalibrate-rtl.git
cd kalibrate-rtl
git checkout arm_memory
./bootstrap
./configure
make
sudo make install
```

Zugriff auf USB-Device freischalten

Das RTL-SDR Gerät einstecken und ID mit dem Befehl `lsusb` überprüfen.
Zu sehen sollte etwas wie folgend sein:

```
Bus 001 Device 004: ID **0bda:2832** Realtek Semiconductor Corp. RTL2832U DVB-T
```

2.1. INSTALLATION VON BENÖTIGTER SOFTWARE FÜR GR-GSM3

```
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp. SMSC9512/9514 Fast Ethernet Controller  
Bus 001 Device 002: ID 0424:9514 Standard Microsystems Corp.  
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

In unserem Fall ist die ID **0bda:2832**. Anschließend öffnen wir eine rules-Datei:

```
sudo nano /etc/udev/rules.d/20.rtl-sdr.rules
```

...in welcher dann folgende Zeile hinzugefügt werden muss:

```
SUBSYSTEM=="usb", ATTRS{idVendor}=="0bda", ATTRS{idProduct}=="2832", GROUP="adm"
```

Falls mehrere RTL-SDR Geräte verwendet werden, können mehrere Zeilen hinzugefügt werden. Die ID muss jeweils natürlich entsprechend des Gerätes abgewandelt werden.

Danach sollte der Raspberry Pi neugestartet werden: `sudo reboot`

Kalibrierung des RTL-SDR Gerätes

Jetzt können wir den Befehl ausführen um das RTL-SDR Gerät zu kalibrieren (um genau zu sein um den durchschnittlichen absoluten Fehler in ppm zu berechnen):

```
kal -s GSM900
```

Das Ergebnis sollte ähnlich zu diesem sein:

```
Found 1 device(s):  
 0: Generic RTL2832U
```

```
Using device 0: Generic RTL2832U
```

```
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
kal: Scanning for GSM-900 base stations.
GSM-900:
chan: 1 (935.2MHz - 33.430kHz) power: 55085.23
chan: 3 (935.6MHz - 34.130kHz) power: 63242.36
chan: 5 (936.0MHz - 33.970kHz) power: 41270.82
...
...
chan: 112 (957.4MHz - 32.934kHz) power: 498930.07
chan: 116 (958.2MHz - 31.859kHz) power: 88039.44
chan: 124 (959.8MHz - 32.429kHz) power: 247404.23
```

Das stärkste Signal wäre in diesem Fall Kanal 112. Also führen wir die Kalibrierung auf diesem Kanal durch:

```
kal -c 112
```

...und erhalten ein Ergebnis wie folgt:

```
Found 1 device(s):
  0: Generic RTL2832U

Using device 0: Generic RTL2832U
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
kal: Calculating clock frequency offset.
Using GSM-900 channel 112 (957.4MHz)
average [min, max] (range, stddev)
- 34.368kHz [-34376, -34357] (20, 4.697051)
overruns: 0
not found: 0
average absolute error: 35.897 ppm
```

Unser durchschnittlicher absoluter Fehler wäre hier also 36 ppm (35.897 ppm).

Installation von GNU Radio

Als nächstes installieren wir GNU Radio:

```
sudo apt-get install gnuradio gnuradio-dev
```

Installieren von libosmocore

Libosmocore muss kompiliert werden...

```
sudo apt-get install cmake
sudo apt-get install build-essential libtool shtool autoconf automake git-core
sudo apt-get install libpcsclite-dev libtalloc-dev
git clone git://git.osmocom.org/libosmocore.git
cd libosmocore/
autoreconf -i
./configure
make
sudo make install
sudo ldconfig -i
cd
```

...außerdem benötigen wir noch ein paar andere Dinge.

```
sudo apt-get install gr-osmosdr rtl-sdr
sudo apt-get install libboost-dev
sudo apt-get install osmo-sdr libosmosdr-dev
sudo apt-get install libusb-1.0.0 libusb-dev
sudo apt-get install libboost-all-dev libcppunit-dev swig doxygen liblog4cpp5-dev
```

Installation von gr-gsm

Und nun zum letzten Schritt:

```
git clone https://github.com/ptrkrysik/gr-gsm.git
```

```
cd gr-gsm
mkdir build
cd build
cmake ..
make
sudo make install
sudo ldconfig
```

Zuletzt erstellen wir noch die `/.gnuradio/config.conf` config-Datei, mit `nano /.gnuradio/config.conf`. Und fügen diese zwei Zeilen hinzu (damit GNU Radio die custom Blöcke von gr-gsm finden kann):

```
[grc]
local_blocks_path=/usr/local/share/gnuradio/grc/blocks
```

Bedienung des Handhelds

In diesem Kapitel finden Sie eine Bedienungsanleitung für das Handheld und Tipps für den Umgang mit diesem.

Um einen Betrachtungspunkt zu haben legen wir nun fest, dass man das Tablet im Querformat verwendet und "oben" die Seite beschreibt an der die USB Anschlüsse des Raspberrys zu sehen sind. In diesem Fall finden wir die Ladebuchse rechts, HDMI, AUX und einen Mikro USB Anschluss zur Direktversorgung links. Der ON/OFF Schalter befindet sich auf der Unterseite rechts. Dieser ist leider nicht all zu gut zugänglich, weshalb es empfohlen wird den Schalter mit einem spitzen Gegenstand zu betätigen (Beispielsweise bietet sich hier die Antenne an).

BILD VON DRAUFSICHT MIT BESCHREIBUNGEN DER ANSCHLÜSSE

Stromversorgung

Verbaut ist ein 2,5 Ah LiPo Akku welcher über eine Adafruit Powerboost1000c Ladeelektronik geladen und betrieben wird. Die Elektronik ist sowohl dafür zuständig den Akku aufzuladen als auch im stationären Zustand ein angeschlossenes USB Netzteil als Stromquelle zu Nutzen. Da der Normalstrom der aus dem Akku gezogen wird sich um die 1A bewegt kann es durchaus zu einer Unterversorgung kommen. Aufgrund dessen wird es nicht empfohlen bei höchster Displayhelligkeit den GSM Suchlauf durchzuführen. Die Displaybeleuchtung dunkelt sich nach 10 Sekunden ab um diesen Fall auszuschließen. Dies kann in den Einstellungen geändert werden.

]

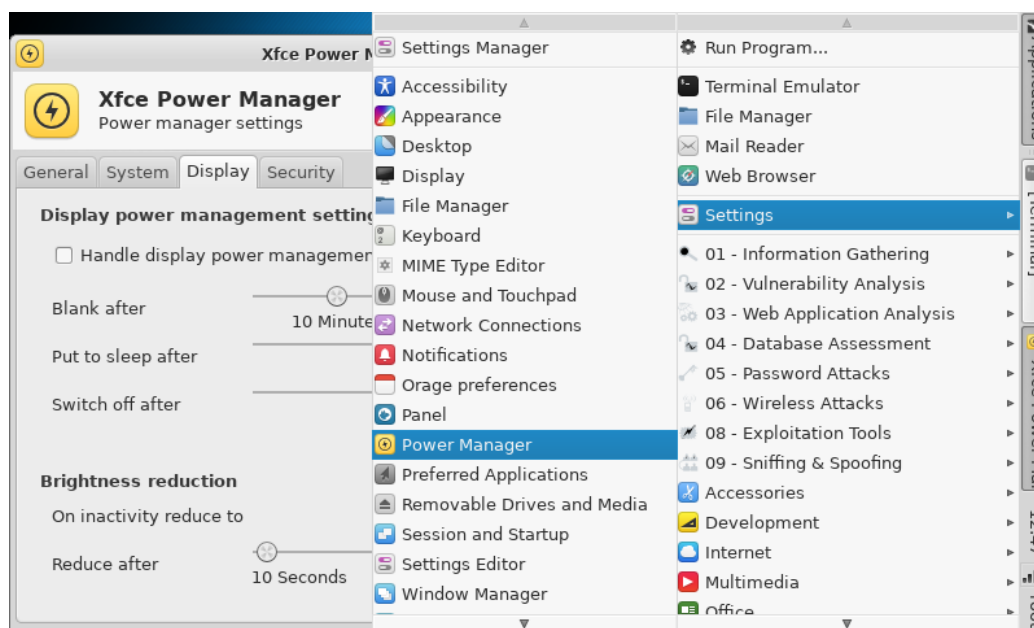


Abbildung 3.1: Einstellung der automatischen Helligkeitsregelung

Bedienung über die Desktopoberfläche

Auf dem Desktop befinden sich die wichtigsten Shortcuts für den Gebrauch des GSM Scanners.

Das Touchscreen ist so eingestellt, dass man nur einmal klicken muss um Programme auszuführen was eine Bedienung mit dem Finger erleichtern sollte. Um eine einfache Einstellbarkeit der Displayhelligkeit zu realisieren haben wir auf dem Desktop Shortcuts hierfür implementiert. Die Stufen 10%, 50% und 100% können ausgewählt werden. Sind andere Stufen gewünscht, so kann man die Displayhelligkeit durch ausführen des Befehls

```
echo XXX > /sys/class/backlight/rpi_backlight/brightness
```

ändern. XXX kann im Bereich von 0 (0%) bis 255 (100%) gewählt werden.

Ferner findet sich ein virtuelles Keyboard auf dem Desktop falls man mobil etwas schreiben möchte. Reboot und Shutdown Shortcuts sind ebenso zu finden. Bitte beachten Sie: Nach dem Shutdown muss die Stromversorgung zusätzlich am ON/OFF Schalter getrennt werden.

Der GSM Scanner hat ebenfalls ein Desktop Shortcut welches mit einem

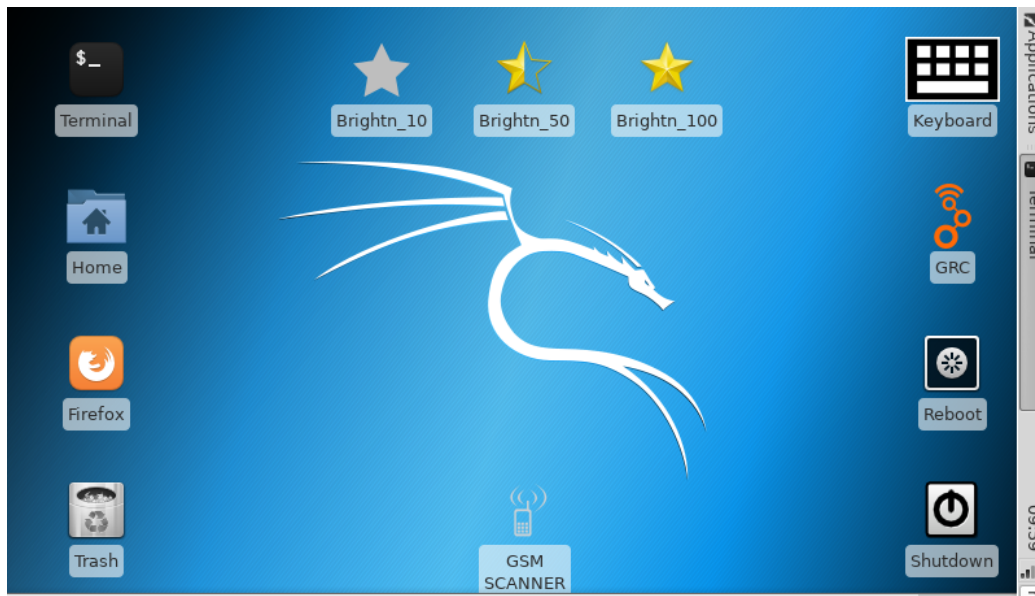


Abbildung 3.2: Ansicht des Dekstops

Klick die Suche nach GSM Basisstationen ermöglicht. Um den Hintergrund zu verstehen erläutere ich hier auf die möglichen Einstellmöglichkeiten mit denen ein Scan gestartet werden kann.

Erweitern und Verändern

Nach dem Anschalten am ON/OFF Schalter auf der Unterseite des Handhelds fährt dieses hoch ohne, dass eine Anmeldung erforderlich ist. Sollte dies geändert werden so müssen müssen zwei Befehle in der Datei `lightdm.conf` auskommentiert werden.

```
cd /etc/lightdm
nano lightdm.conf

*****
autologin-user=root
autologin-user-timeout=0
*****
```

müssen durch voransetzen eines `"#"` auskommentiert werden

Options:

```

-h, --help          show this help message and exit
-b BAND, --band=BAND Specify the GSM band for the frequency. Available
                    bands are: GSM900, DCS1800, GSM850, PCS1900, GSM450,
                    GSM480, GSM-R
-s SAMP_RATE, --samp-rate=SAMP_RATE
                    Set sample rate [default=2000000.0] - allowed values
                    even_number*0.2e6
-p PPM, --ppm=PPM   Set frequency correction in ppm [default=0]
-g GAIN, --gain=GAIN Set gain [default=24.0]
--args=ARGS         Set device arguments [default=]
--speed=SPEED       Scan speed [default=4]. Value range 0-5.
-v, --verbose       If set, verbose information output is printed: ccch
                    configuration, cell ARFCN's, neighbour ARFCN's

```

```
grgsm_scanner -g 50 -p 29 --speed=5
```

Mit diesen Übergabeparametern wird der GSM Scanner aufgerufen und sucht im default BAND das Netz von 925 Mhz bis 960 Mhz ab. Dies entspricht dem E-GSM 900 Netz. Ein Gain von 50 dB ist der maximalwert und ermöglicht somit die größte "Ausbeute" was die Ergebnisliste angeht. Der Offset des Quarzes wurde berechnet durch eine Kalibrierung des DVB-T Sticks und ist immer mit anzugeben.

Das zugehörige Desktop Shortcut, wie auch die zur Helligkeitsregulierung, führen Shell Skripte aus welche unter

`/root/Documents`

hinterlegt sind. Hier kann man eingreifen falls etwas geändert werden soll. Am besten öffnet man diese über das Terminal mit "nano" da sonst kein Textverarbeitungsprogramm installiert ist.

Alle von uns geschriebenen Komponenten sind im Ordner

`/root/GrGsm-Gui`

zu finden. Da es sich hierbei um ein Git Repository handelt kann dieses auch über

```
cd GrGsm-Gui/  
git pull
```

auf den neusten Stand gebracht werden, sollten Veränderungen vorgenommen werden.

Setup des Raspberry PI

Im folgenden wird beschrieben wie wir den Raspberry aufgesetzt haben und welche Probleme uns dabei begegnet sind.

Das How To und interdependencies

GrGsm wird hauptsächlich von Piotr Krysik entwickelt und wird von diesem auch gepflegt. Es gibt auch einen vorgeschlagenen Weg wie man GrGsm auf einem Raspberry Pi 3 zu installieren hat. Dieser Weg hat sich allerdings als Sackgasse erwiesen. Grund dafür war, dass in Zwischenzeit GnuRadio weiterentwickelt aber nicht für Raspbian Jessie und dadurch inkompatibel zu GrGsm wurde.

GrGsm benötigte damals eine Version von GnuRadio $> 3.7.9$. Für Raspbian war allerdings nur die Version 3.7.6 verfügbar. Der Versuch auf unstable Versionen 3.7.10+ auszuweichen erwies sich ebenso als Aussichtslos. Das Installieren von diesen Versionen führte nur dazu, dass wiederum Bibliotheken von denen GnuRadio abhängig war inkompatibel wurden.

Nach einiger Recherche wie man ein funktionierendes Gesamtpaket erhalten könnte sind wir auf das Programm PyBombs gestoßen. Dieses macht genau das, es installiert ein Programm und alle Abhängigkeiten die dieses zur Nutzung benötigt. Im Gegensatz zu apt-get, wie man es von von Ubuntu und sonstigen Linux Distributionen kennt

!!!!!!!!!!!!HIER PYBOMBS ERKLÄREN!!!!!!!!!!!!!!

An diesem Punkt haben wir beschlossen, dass eine zeitnahe Umsetzung mit GrGsm wohl aussichtslos erscheint. Indes standen wir mit Piotr Krysik in Kontakt um einen Weg zu finden wie es doch zu lösen sein könnte. Zu dieser Zeit war dieser dabei seine Anpassungen in einem Raspberry Emulator

zur überprüfen. Wir entschieden uns doch Airprobe zu verwenden. Dafür haben wir uns an einer Jahrealten Anleitung orientiert und sind dabei auf Kali Linux gestoßen, dieses war glücklicherweise auch für Raspberrys verfügbar. Nachdem wir das installiert hatten, war, wer hätte es gedacht Gnuradio mittlerweile zu Neu um mit Airprobe arbeiten zu können. Allerdings war die stabile Version glücklicherweise 3.7.10, somit mit dem neusten GrGsm kompatibel und so konnten wir alle Abhängigkeiten installieren, die Kalibrierung durchführen und GrGsm installieren. Zu der Zeit haben wir schon einen Monat Arbeit in das Projekt stecken und die Grenzen unserer Frustrationstoleranz immer ein Stückchen weiter schieben müssen.

Einige Features

Hier werden einige Features gezeigt.

Ein Unterabschnitt

Die Tabelle 5.1 ist ein Beispiel für eine wissenschaftliche Tabelle (ohne vertikale Trennlinien).

Tabelle 5.1: Beispieltabelle

Apfel	Birne	Katze
200 g	180 g	3.4 kg

So zitiert man [?]. Man kann auch mehrere Quellen auf einmal referieren [?, ?, ?, ?]

In Abbildung 5.1 ist eine Kurve dargestellt.

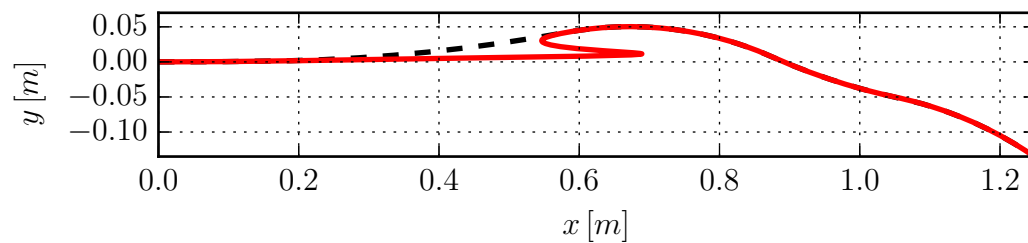


Abbildung 5.1: Beispielbild

Inkscape erlaubt es eps-Files und den Text getrennt zu exportieren, auf diese

Weise kann man die Schrift nachträglich anpassen. Ein Beispiel dazu ist in Abbildung 5.2 dargestellt.

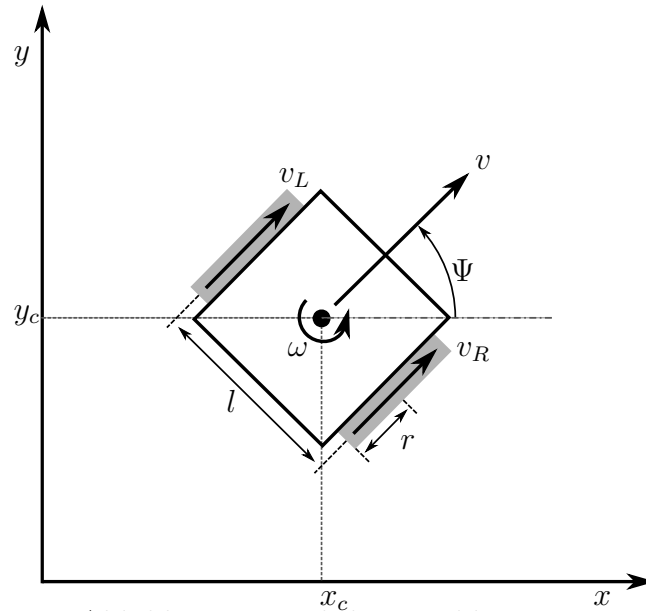


Abbildung 5.2: Inkscape Bild mit Text

Außerdem gibt es eine Umgebung zum Schreiben von Pseudo-Code. Ein Beispiel dazu ist in Algorithmus 5.1 dargestellt.

Algorithm 5.1 Beispielalgorithmus

```

1: procedure ADDTWO NUMBERS( $x, y$ )
2:    $sum \leftarrow x + y$ 
3:   if  $sum = 42$  then
4:     FIXEVERYTHING

```

Das Paket acronym handelt Abkürzungen automatisch. Bei der ersten Verwendung sieht das so aus: Unified Modelling Language (UML). Wenn die Abkürzung nochmal verwendet wird, steht da nur noch UML.

Zusammenfassung

Ausblick