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

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

Abbildungsverzeichnis

Tabellenverzeichnis

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 scnannen. 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

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 Direktversorung 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 angeschlssossenes 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 höhster Displayhelligkeit den GSM Suchlauf durchzuführen. Die Displaybeleuchtung dunkelt sich nach 10 Sekunden ab um diesen Fall auszuschließen. Dies kann in den Einstellungen geändert werden.

BILD DISPLAYHELLIGKEIT

Bedienung über die Desktopoberfläche

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
```

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 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

```
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 Kalibierung 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.

Noch Ein Kapitel

Einige Features

Hier werden einige Features gezeigt.

Ein Unterabschnitt

Die Tabelle 4.1 ist ein Beispiel für eine wissenschaftliche Tabelle (ohne vertikale Trennlinien).

Tabelle 4.1: Beispieltabelle

Apfel	Birne	Katze
200 g	180 g	3.4 kg

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

In Abbildung 4.1 ist eine Kurve dargestellt.

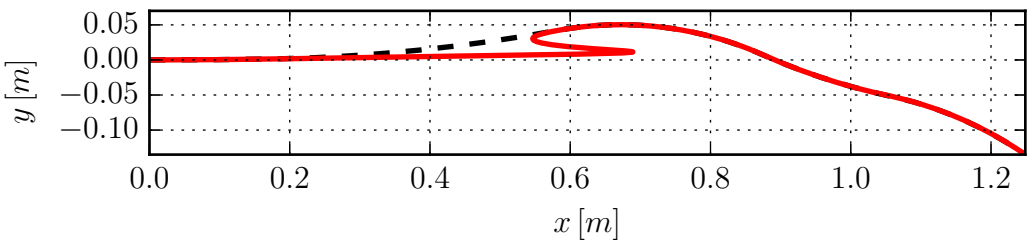

Abbildung 4.1: Beispielbild

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 4.2 dargestellt.

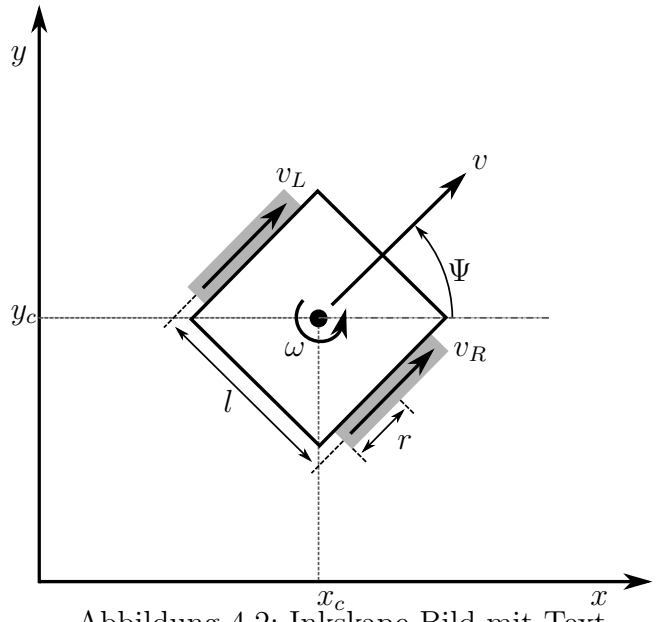

Abbildung 4.2: Inkskape Bild mit Text

Außerdem gibt es eine Umgebung zum Schreiben von Pseudo-Code. Ein Beispiel dazu ist in Algorithmus 4.1 dargestellt.

Algorithm 4.1 Beispielalgorithmus

```
1: procedure AddTwoNumbers(x, y)
2:     sum ← 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