

Mobile Netze

Mobile Netze - Man-In-The-Middle

Ausarbeitung
von
Attenberger, Bollenmiller, Schuster, Wilhelm
SS17 IG
27. September 2017

Inhaltsverzeichnis

1. Einleitung	1
2. Architektur des Osmocom Systems	2
3. Architektur des OpenBTS Systems	3
4. Inbetriebnahme eines Osmocom Systems	4
4.1. Vorinstallationen	4
4.1.1. Ubuntu 16.04.3	4
4.1.2. Git	4
4.1.3. Softwarevoraussetzungen	4
4.1.4. Aktivierung der Verbindung zum USRP2	4
4.2. Installation einzelner GSM Komponenten	5
4.2.1. OsmoTRX	5
4.2.2. OsmoBTS	5
4.2.3. OpenBSC	5
4.3. Starten des Systems	6
5. Inbetriebnahme eines OpenBTS Systems	7
5.1. Vorinstallationen	7
5.1.1. Ubuntu 16.04.3	7
5.1.2. Git	7
5.1.3. Softwarevoraussetzungen	7
5.2. Installation einzelner GSM Komponenten	7
5.3. Starten des Systems	7
6. Umsetzung des Projektziels	8
6.1. pcapsipdump	9
6.2. Abspeichern der Daten	9
6.3. pcap2wavgsm	10
6.4. Extrahieren der Daten	10
6.5. Vollautomatisieren aller Schritte	10
6.6. incron	10
6.7. Weiteres Feature	11
7. Ergebnisse	12
8. Projektaufteilung	13
A. openbsc.cfg	14
B. openbsc.cfg	16

1. Einleitung

Was ist GSM? Was ist OpenBTS, OsmoBTS, OpenBSC, Osmo-Nitb etc?

- eigenes weiteres Kapitel – Was ist das Ziel des Projektes - UseCases
- Architektur dann als eigenes Kapitel - Beschreibung einzelner Komponenten sowie deren Funktion
- Systemspezifikation

2. Architektur des Osmocom Systems

Evtl unterteilung in Kapitel: Überblick Beschreibung der einzelnen Komponenten

3. Architektur des OpenBTS Systems

Evtl unterteilung in Kapitel: Überblick Beschreibung der einzelnen Komponenten

4. Inbetriebnahme eines Osmocom Systems

Für Inbetriebnahme des GSM Netzes waren einige Vorinstallationen sowie das Einrichten von Ubuntu 16.04.3 nötig. Im Folgenden wird das Vorgehen zur Einrichtung des Systems sowie die Inbetriebnahme des GSM Netzes beschrieben.

4.1. Vorinstallationen

4.1.1. Ubuntu 16.04.3

Zunächst wurde das Betriebssystem Ubuntu 16.04.3 auf einem Labor-Rechner installiert und eingerichtet.

4.1.2. Git

Da die Open-Source Projekte von OsmocomBB auf Git-Repositories liegen, wurde zunächst Git eingerichtet. Zur Versionskontrolle und Verwaltung des Codes wurde außerdem ein Team-eigenes Git Repository angelegt.

```
1 sudo apt-get install git
```

4.1.3. Softwarevoraussetzungen

Osmocom empfiehlt zunächst die Einrichtung von einigen Bibliotheken und sonstigen, nötigen Abhängigkeiten als Voraussetzung für die Inbetriebnahme der GSM Komponenten. Diese wurden mittels Paketmanagers wie folgt installiert.

```
1 sudo apt-get install libpcsc-lite-dev libtalloc-dev libortp-dev libsctp-dev
2 libmnl-dev libdbi-dev libdbd-sqlite3 libsqlite3-dev sqlite3 libc-ares-dev
3 libdbi0-dev libdbd-sqlite3 build-essentials libtool autoconf automake pkg-
   config
4 libsqlite3-tcl sqlite-autoconf sqlite-autoconf
```

Die die Fehler bezüglich Bumpversion nicht behoben werden konnten, wurden sie ignoriert. Dies zog keinerlei Konsequenzen hinsichtlich der Inbetriebnahme der GSM Komponenten nach sich. Zusätzlich bedarf es der separaten Installation der Software Bibliotheken libosmo-abis, libosmo-core und libosmo-netif. Diese wurden von den entsprechenden Git Repositories heruntergeladen und nach analogem Vorgehen installiert.

```
1 git clone git://git.osmocom.org/<lib-source>
2 cd <lib-source>
3 autoreconf -fi
4 ./configure
5 make
6 make install
7 sudo ldconfig
```

Trotz der sorgfältigen Installation einiger Softwarevoraussetzungen traten zusätzliche Abhängigkeiten bei der Installation einzelner GSM Komponenten auf, welche in 4.2 beschrieben sind.

4.1.4. Aktivierung der Verbindung zum USRP2

Vor Installation des Treibers sollte zunächst die Netzwerkschnittstelle wie folgt aktiviert werden. Die default IP Adresse des Ettus USRP2 ist 192.168.10.2.

```
1 sudo ifconfig enp0s25 192.168.10.3
2 ping 192.168.10.2
```

4.2. Installation einzelner GSM Komponenten

OsmocomBB hält detaillierte Beschreibungen zur Installation der GSM Komponenten bereit, welche zur Inbetriebnahme des in Rahmen dieser Arbeit verwendeten GSM Netzes herangezogen wurden. Im Folgenden wird die Installation und Einrichtung der GSM Komponenten genauer erläutert.

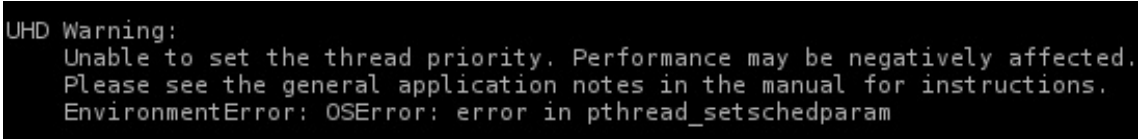
4.2.1. OsmoTRX

Zur Kommunikation mit der Basisstation ist der osmoTRX Treiber nötig. Osmocom bietet diesen - meist wie die anderen Komponenten - im Git Repository an. Die Installation des Treibers erforderte die Bibliotheken *libusb-1.0-0-dev*, *uhd-host*, *libboost-dev* und *libuhd-dev*. Diese bieten die Suchfunktion *uhd_find_devices*. Dadurch lässt sich testen, ob die Basisstation gefunden wird. Mittels *osmo-trx* lässt sich der Treiber nach der Installation starten.

```
1 git clone git://git.osmocom.org/osmo-trx
2 cd osmo-trx/
3 autoreconf -i
4 ./configure
5 sudo make -j8
6 sudo make install
7 osmo-trx
```

Zur Behebung der Warnung, die in Abbildung 1 zu sehen ist, wurde die Priorität in der Datei */etc/security/limits.conf* gesetzt.

```
1 @usrp - rtprio 50
```



```
UHD Warning:
Unable to set the thread priority. Performance may be negatively affected.
Please see the general application notes in the manual for instructions.
EnvironmentError: OSError: error in pthread_setschedparam
```

Abbildung 1: Fehlermeldung bezüglich der Thread Priorität in osmoTRX

4.2.2. OsmoBTS

Die Installation von OsmoBTS erfolgte analog zur Einrichtung der anderen Osmocom Komponenten.

```
1 git clone git://git.osmocom.org/osmo-bts.git
2 autoreconf -fi
3 cd osmo-bts
4 ./configure
5 sudo make -j8
6 sudo make install
```

Zur Konfiguration wurden zunächst die Pfade der folgenden Variablen angepasst.

```
1 PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games"
2 PKG_CONFIG_PATH="/home/netpc06/libosmo-abis/"
3 LIBOSMOTRAU_CFLAGS="/home/netpc06/libosmo-abis/"
4 LIBOSMOTRAU_LIBS="/home/netpc06/libosmo-abis/"
```

4.2.3. OpenBSC

Weiterhin wurde OpenBSC installiert. Dazu wurde die Bibliothek *libssl-dev* (eigentlich unter *lib-crypto* bekannt) vorausgesetzt.

```
1 sudo apt-get install libssl-dev
2 git clone git://git.osmocom.org/openbsc
3 cd openbsc/
4 cd openbsc/openbsc/
5 autoreconf -i
6 ./configure
7 sudo make -j8
8 sudo make install
```

Zur Konfiguration von OpenBSC wurde eine Beispieldatei wie folgt angepasst (siehe Anhang ??).
short name und *long name* beschreiben den Name des Netzwerks und wurden umbenannt.

4.3. Starten des Systems

5. Inbetriebnahme eines OpenBTS Systems

Für Inbetriebnahme des GSM Netzes waren einige Vorinstallationen sowie das Einrichten von Ubuntu 16.04.3 nötig. Im Folgenden wird das Vorgehen zur Einrichtung des Systems sowie die Inbetriebnahme des GSM Netzes beschrieben.

5.1. Vorinstallationen

5.1.1. Ubuntu 16.04.3

Verweis machen, wenn wie bei Osmocom

5.1.2. Git

Verweis machen, wenn wie bei Osmocom

5.1.3. Softwarevoraussetzungen

selbst

5.2. Installation einzelner GSM Komponenten

selbst

5.3. Starten des Systems

6. Umsetzung des Projektziels

Während es sich bei den beiden vorherigen Kapiteln um die Inbetriebnahme des GSM-Netzes selbst gehandelt haben, geht es nun um die konkrete Umsetzung des eigentlichen Projektziels "Man-In-The-Middle". Dabei wird versucht die Gesprächsdaten auf der Strecke zwischen BTS, BSC und PBX abzugreifen.

Zuerst versucht zwischen BTS und BSC?!? -> evtl Screenshot von Daten des ABIS-Interface?!

<https://osmocom.org/projects/osmo-sip-conector/wiki/Osmo-sip-connector> <http://ftp.osmocom.org/docs/latest/osmonusermanual.pdf> -> p.6/7

Abgreifen der Daten zwischen BTS und BSC (ABIS-Interface) schwierig -> Daten weiter analysiert und weitere Angriffspunkte ausmachen. -> Abgreifen der Daten vor der Telefonanlage (Asterisk (OPEN: IAX; Osmo: PBX)) -> dadurch die Daten im VOIP Format (SIP + RTP), welches via PC relativ gut zu handeln ist.

Zunächst eigenes analysieren der Daten. Suche nach praktischem Tool im Internet -> pcapspidump
Für die Installation und Einrichtung der benötigten Tools wurde ein Bash-Skript erstellt, welches die meisten Schritte automatisch durchführt. Die manuell noch auszuführenden Schritte werden in der Komandozeile ausgegeben.

Listing 1: Install and configure Script

```

1  #!/bin/bash
2
3  HOMEPATH=/home/all
4
5  #check if script called with root privileges
6  if [ `id -u` != 0 ];then
7      echo "You have to start this script with root privileges"
8      exit 1
9  fi
10
11
12  echo ">>>creating folder with access of all user"
13  sudo mkdir -p $HOMEPATH/wiresharkCalls
14  sudo mkdir -p $HOMEPATH/wavCalls
15  sudo mkdir -p $HOMEPATH/gsmCalls
16  echo ""
17
18  echo ">>>extending permissions"
19  sudo chmod a=rwx $HOMEPATH
20  sudo chmod a=rwx $HOMEPATH/wiresharkCalls
21  sudo chmod a=rwx $HOMEPATH/wavCalls
22  sudo chmod a=rwx $HOMEPATH/gsmCalls
23  echo ""
24
25  echo ">>>copying conversionScript"
26  cp startPcap2wavgsmConversion.sh $HOMEPATH/.
27  chmod a=rwx $HOMEPATH/startPcap2wavgsmConversion.sh
28  cp pcap2wavgsm.sh $HOMEPATH/.
29  chmod a=rwx $HOMEPATH/pcap2wavgsm.sh
30  echo ""
31
32  echo ">>>checking dependencies "
33  if ! which "tshark" > /dev/null
34  then
35      sudo apt-get install -y tshark sox
36  fi
37  echo ""
38
39  echo ">>>installing pcapspidump"
40  if ! which "svn" > /dev/null
41  then

```

```

42     sudo apt-get install -y subversion
43 fi
44 sudo apt-get install -y libpcap-dev
45 svn checkout https://svn.code.sf.net/p/pcapsipdump/code/trunk pcapsipdump-code
46 cd pcapsipdump-code
47 sudo cp ../calltable.cpp .
48 sudo make
49 sudo make install
50 cd ..
51 echo ""
52
53 sudo chmod +x startingPcapsipdump.sh
54 sudo ./startingPcapsipdump.sh $HOMEPATH
55 echo ""
56
57 echo ">>installing incron if not already installed.."
58 if ! which "incron" > /dev/null
59 then
60     sudo apt-get install -y incron
61 fi
62 echo ""
63 echo ""
64
65 echo ">>YOU have to do that manually:"
66 echo ">>append your username into '/etc/incron.allow'"
67
68 echo ">>starting service with 'systemctl start incron.service'"
69
70 echo ">>add job with 'incrontab -e' and append following line:"
71 echo "/home/all/wiresharkCalls IN_CLOSE_WRITE /home/all/
    startPcap2wavgsmConversion.sh \${@} \${#}"
72 echo ""

```

6.1. pcapsipdump

6.2. Abspeichern der Daten

Mit den beiden Komandozeilenanwendungen tshark und tcpdump können Daten von einem Interface in eine pcap-Datei abgespeichert werden. Hierbei können auch bereits schon beim aufnehmen Filter gesetzt werden, sodass nur die relevanten Daten gespeichert werden.

pcapsipdump ist open-source Tool, welches auf der libpcap basiert. Das Tool hört auf einem Interface die Daten mit und speichert die SIP/RTP sessions als pcap-Datei ab. Diese Datei kann nun in tcpdump, Wireshark oder ähnlichem geöffnet, eingelesen und weiterverarbeitet werden. Das nette Feature dabei ist, dass das Tool selbstständig pro Session eine Datei anlegt. Das Tool läuft als Hintergrundprozess, sodass es nur einmal manuell gestartet werden muss. Alternativ kann das Tool auch mit dem systemd-Init-Prozess automatisch gestartet werden, sofern man es nachträglich selbst konfiguriert. Hören das Loopback-Interface ab -> da all Tools auf dem selben Rechner laufen und die Tools über diese Schnittstelle miteinander kommunizieren.

Abhängigkeiten des Programms installieren

```
1 sudo apt-get install -y libpcap-dev
```

Gestartet wird das Tool mit folgenden Parametern.

```
1 sudo pcapsipdump -i lo -v 10 -d $HOMEPATH/wiresharkCalls/%Y%m%d-%H%M%S-%f-%t-%i
    .pcap -U
```

Im späteren Verlauf Probleme mit dem Tool, sodass letztendlich Source-Code angepasst wurde. Das Problem lag darin, dass das Tool die erstellte Datei lange nicht schließt, obwohl bereits seit längerem die Session beendet ist. Der Übeltäter war ein Timer in der calltable-Klasse, welcher

auf 5 Minute gestellt war. Nach Verändern des Timers auf 5 Sekunden wurde auch die erstellte pcap-Datei kurz nach Ende der Session geschlossen.

```

211     ...
212     if (table[idx].is_used && (
213         (currttime - table[idx].last_packet_time > 5) ||
214         (currttime - table[idx].first_packet_time > opt_absolute_timeout))) {
215     ...

```

6.3. pcap2wavgsm

6.4. Extrahieren der Daten

Zunächst wurden die von pcapsipdump extrahierten Daten mit Wireshark manuell analysiert. Darin sind nun wirklich nur noch die SIP- und RTP-Packet enthalten, wie auf fig XXXXX zu sehen. Mit Wireshark erkennt auch den VOIP-Anruf und kombiniert die RTP-Packages korrekt. Allerdings konnte der Stream nicht direkt im Programm abgespielt werden. Der Grund hierfür ist vermutlich, dass Wireshark gsm nicht dekodieren kann. Jedoch gibt es einen Weg, wie die beiden Streams als .raw-Daten exportiert werden können. Hierfür ein beliebiges RTP-Packet auswählen, über "Telefonie->RTP->Stream Analyse"den Stream analysieren. Nun kann der Hinweg und Rückweg als seperate Datei gespeichert werden. Man muss jedoch als Datei-Typ .raw auswählen. Die .raw-Dateien können nun via folgendem Komandozeilenaufwurf abgespielt werden

```
1 padsp play -t gsm -r 8000 -c 1 example.gsm
```

Mit dem universellen und sehr mächtigen Audiokonverter SoX können die Dateien über folgenden Komandozeilenaufwurf in .wav convertiert werden, sodass diese auch mit jedem herkömmlichen Media Player abgespielt werden können.

```
1 sox -t gsm -r 8000 -c 1 example.raw exampleConverted.wav
```

Mit dem Bash-Skript pcap2wav von <https://gist.github.com/avimar/d2e9d05e082ce273962d742eb9acac16> können genau diese Schritte automatisiert ausgeführt werden.

6.5. Vollautomatisieren aller Schritte

6.6. incron

Das Abspeichern der Daten funktioniert bereits voll automatisiert und jeweils auch in eine extra Datei pro Session. Allerdings muss das Convertierungs-Skript noch automatisch getriggert bzw. ausgeführt werden. Hierfür kann das Linux-Tool "Incron" genutzt werden. Das Tool setzt auf das Kernel-Subsystem Inotify, um auf Dateisystem-Ereignisse zu reagieren. Dadurch kann ein Ordner überwacht werden und bei einer neuen Datei etwas getriggert werden, wie z.B. eben die Ausführung des Konvertierungs-Skriptes. Incron ähnelt dabei in der Handhabung an das Standardwerkzeug "Cron", welches Cron Jobs auf Basis von Zeitpunkten startet.

```

1 echo ">>installing incron if not already installed.."
2 if ! which "incron" > /dev/null
3 then
4     sudo apt-get install -y incron
5 fi
6 echo ""
7 echo ""
8
9 echo ">>YOU have to do that manually:"
10 echo ">>append your username into '/etc/incron.allow'"
11
12 echo ">>starting service with 'systemctl start incron.service'"
13
14 echo ">>add job with 'incrontab -e' and append following line:"

```

```
15 echo "/home/all/wiresharkCalls IN_CLOSE_WRITE /home/all/  
    startPcap2wavgsmConversion.sh \${@} \${#}"  
16 echo ""
```

Nun werden also die Daten direkt von der Schnittstelle abgegriffen, gefiltert und gespeichert. Danach automatisch in .wav konvertiert, sodass die Gespräche lokal auf dem PC angehört werden können. Um nicht an den lokalen PC gebunden zu sein, wäre es möglich die Dateien über einen Webserver global zur Verfügung zu stellen.

6.7. Weiteres Feature

Es soll das letzte oder die letzten Gespräche via einem Telefonanruf wiedergegeben werden können. Dies wurde mit einer/mehreren speziell konfigurierten Nummern ermöglicht.

==> kann auch die Nummer beschränkt werden, sodass nur eine registrierte Nummer die Gespräche abhören kann?!???

7. Ergebnisse

vielleicht unterteilen in: Fazit/ Ergebnisse/ Was wurde umgesetzt, was nicht Probleme Lessons Learned

8. Projektaufteilung

Projekt unterteilt in Aufgaben : dahinter jeweils alle Namen

Dokument unterteilt in Kapitel: dahinter jeweils alle Namen

Appendix

A. openbsc.cfg

```

1 !
2 ! OpenBSC configuration saved from vty
3 ! !
4 password foo
5 !
6 line vty
7 no login
8 !
9 e1\_input
10 e1\_line 0 driver ipa
11 e1\_line 0 port 0
12 network
13 network country code 262
14 mobile network code 99
15 short name mitm2
16 long name mitm2
17 auth policy accept-all
18 location updating reject cause 13
19 encryption a5 0
20 neci 1
21 paging any use tch 0
22 rrlp mode ms-based
23 mm info 1
24 handover 0
25 handover window rxlev averaging 10
26 handover window rxqual averaging 1
27 handover window rxlev neighbor averaging 10
28 handover power budget interval 6
29 handover power budget hysteresis 3
30 handover maximum distance 9999
31 timer t3101 10
32 timer t3113 60
33 timer t3122 10
34 dtx-used 0
35 subscriber-keep-in-ram 0
36 bts 0
37 type sysmobts
38 band PCS1900
39 cell\_identity 0
40 location\_area\_code 1
41 training\_sequence\_code 7
42 base\_station\_id\_code 63
43 ms max power 0
44 cell reselection hysteresis 4
45 rxlev access min 0
46 periodic location update 30
47 channel allocator descending
48 rach tx integer 9
49 rach max transmission 7
50 channel-description attach 1
51 channel-description bs-pa-mfrms 5
52 channel-description bs-ag-blks-res 1
53 ip.access unit\_id 1901 0
54 oml ip.access stream\_id 255 line 0
55 neighbor-list mode automatic
56 trx 0
57 rf\_locked 0
58 arfcn 806

```



```
59 nominal power 0
60 max\_power\_red 0
61 rsl e1 tei 0
62 timeslot 0
63   phys\_chan\_config CCCH+SDCCH4
64   hopping enabled 0
65 timeslot 1
66   phys\_chan\_config TCH/F
67   hopping enabled 0
68 timeslot 2
69   phys\_chan\_config TCH/F
70   hopping enabled 0
71 timeslot 3
72   phys\_chan\_config TCH/F
73   hopping enabled 0
74 timeslot 4
75   phys\_chan\_config TCH/F
76   hopping enabled 0
77 timeslot 5
78   phys\_chan\_config TCH/F
79   hopping enabled 0
80 timeslot 6
81   phys\_chan\_config TCH/F
82   hopping enabled 0
83 timeslot 7
84   phys\_chan\_config TCH/F
85   hopping enabled 0
```

B. openbsc.cfg

```

1 !
2 ! OpenBSC configuration saved from vty
3 ! !
4 password foo
5 !
6 line vty
7 no login
8 !
9 e1\_input
10 e1\_line 0 driver ipa
11 e1\_line 0 port 0
12 network
13 network country code 262
14 mobile network code 99
15 short name mitm2
16 long name mitm2
17 auth policy accept-all
18 location updating reject cause 13
19 encryption a5 0
20 neci 1
21 paging any use tch 0
22 rrlp mode ms-based
23 mm info 1
24 handover 0
25 handover window rxlev averaging 10
26 handover window rxqual averaging 1
27 handover window rxlev neighbor averaging 10
28 handover power budget interval 6
29 handover power budget hysteresis 3
30 handover maximum distance 9999
31 timer t3101 10
32 timer t3113 60
33 timer t3122 10
34 dtx-used 0
35 subscriber-keep-in-ram 0
36 bts 0
37 type sysmobts
38 band PCS1900
39 cell\_identity 0
40 location\_area\_code 1
41 training\_sequence\_code 7
42 base\_station\_id\_code 63
43 ms max power 0
44 cell reselection hysteresis 4
45 rxlev access min 0
46 periodic location update 30
47 channel allocator descending
48 rach tx integer 9
49 rach max transmission 7
50 channel-description attach 1
51 channel-description bs-pa-mfrms 5
52 channel-description bs-ag-blks-res 1
53 ip.access unit\_id 1901 0
54 oml ip.access stream\_id 255 line 0
55 neighbor-list mode automatic
56 trx 0
57 rf\_locked 0
58 arfcn 806
59 nominal power 0
60 max\_power\_red 0
61 rsl e1 tei 0

```

```
62 timeslot 0
63   phys\_chan\_config CCCH+SDCCH4
64   hopping enabled 0
65 timeslot 1
66   phys\_chan\_config TCH/F
67   hopping enabled 0
68 timeslot 2
69   phys\_chan\_config TCH/F
70   hopping enabled 0
71 timeslot 3
72   phys\_chan\_config TCH/F
73   hopping enabled 0
74 timeslot 4
75   phys\_chan\_config TCH/F
76   hopping enabled 0
77 timeslot 5
78   phys\_chan\_config TCH/F
79   hopping enabled 0
80 timeslot 6
81   phys\_chan\_config TCH/F
82   hopping enabled 0
83 timeslot 7
84   phys\_chan\_config TCH/F
85   hopping enabled 0
```