Report of OpenBSC/sysmoBTS field test December 2013, 30C3, Hamburg, Germany

Daniel Willmann
dwillmann@sysmocom.de

Holger Hans Peter Freyther
hfreyther@sysmocom.de

March 20, 2014

Abstract

The 30C3 was the 30th annual Conference of the Chaos Computer Club. A GSM test network using the OpenBSC software suite and the sysmoBTS 1002E was operated and provided voice and short-message service to the attendees that purchased a SIM card for this test network.

Contents

1 Description of Test Setup **2**
1.1 Antennas . . . 2
1.2 SIM Cards . . . 2
1.3 sysmoBTS 1002E . . . 3
1.4 Server running the GSM Network . . . 3
1.5 Networking . . . 3
1.6 TEMS . . . 3

2 Objectives of the field test **3**
2.1 Reliability . . . 3
2.2 Interopability . . . 4

3 Software Defects **4**
3.1 USSD own number query . . . 4
3.2 Filtering by IMSI . . . 4
3.3 Late Replies during Location Updating . . . 4
3.4 Timeouts during SMS on TCH/F . . . 5
3.5 Rogue connects to RSL . . . 5

4 Interopability issues **5**
4.1 Vodafone Germany . . . 5
4.2 Missed Periodic Updates . . . 6
4.3 SS interrogation during Location Updating . . . 6

5 Usage **6**
5.1 Communication . . . 6
5.2 Human to Machine . . . 6
5.3 Spam . . . 6

6 Conclusions and Outlook **7**
TODO? introduction?

1 Description of Test Setup

The test setup consisted of seven installations using the sysmoBTS 1002E and various different antennas that were located throughout the building. Those BTSes connected to a central server that was running the osmo-nitb Software to provide the BSC/MSC functionality of the GSM network. We used Linux-Call-Router (LCR) to connect to the Phone Operation Center (POC) to provide an interconnect to the POTS and Dect network of the conference. The software used on the BTS is the osmo-bts Software and it is the first time we use it at a public event.

1.1 Antennas

In the past we had experimented with inexpensive antennas from China but the performance has been poor. This year we have used antennas from Kathrein and Procom. We have deployed the following models at the venue.

- Procom CXL 1800-1LW
- Procom CXL 1800-3LW
- Kathrein Vpol BiDir
- Kathrein Vpol Indoor (80010465)
- Kathrein Vpol Indoor (80010249)

1.2 SIM Cards

We have provisioned SIM Cards at previous events and these remain working at future events. We have changed the model of the SIM Card from sysmoSIM-GR1 to sysmoSIM-GR2 and produced a dedicated batch with the artwork of the event. The SIM Cards can be provisioned using the pySIM software of the Osmocom project.

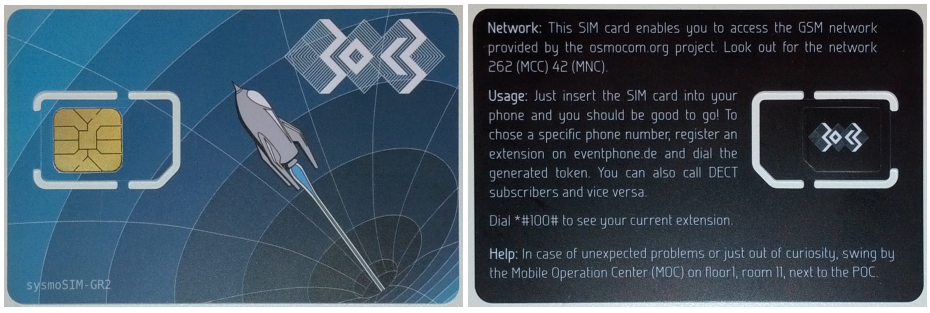

Figure 1: 30c3 SIM card (front and back)

1.3 sysmoBTS 1002E

The sysmoBTS 1002E is a low power GSM Base-Station and we have used seven devices at this event. The BTSes were operated on the DCS1800 band and the current stable version of osmo-bts and other Osmocom components were used.

1.4 Server running the GSM Network

We are using an older 1U system with about 1GB of RAM running Gentoo Linux. The system is using osmo-nitb of OpenBSC and the Linux-Call-Router (LCR) to connect voice calls to the POC. The latest version of OpenBSC and its support libraries has been used.
The osmo-nitb Software is executed from a shell script that enables coredumps and copies the executable to the /space/30c3/core directory. In case of a crash we can use the GNU Debugger (gdb) to generate a backtrace and inspect the datastructures that were used.

1.5 Networking

At the Congres Centrum Hamburg (CCH) we started to use VLANs to connect the BTS with our BSC/NITB system. After a BTS has been physically installed we had to connect it to one of the switches that were placed throughout the venue and record the LLDP message being broadcasted by the switch. After all systems were placed we asked the NOC to forward these ports to our VLAN.

1.6 TEMS

Once the network was up an ad-hoc site survey was carried out. We used TEMS capable phones and walked around the venue. The nice thing about this hardware is that it displays the neighbor cells and their receive level. We were able to locate places without coverage and could deploy another BTS.

TODO: picture?

2 Objectives of the field test

The 30C3 provides the unique opportunity to generate a load that we can not easily simulate with a number of different devices we don't own.

2.1 Reliability

The osmo-nitb software is used in various temporary and permanent deployments throughout the world and there were no known runtime failures or memory leaks before the event. The osmo-bts software has been extensively tested in our development labs using banks of modems and been exposed to RACH DoS

attacks but it is the first time we use it at an event like this so we were excited to see how the software performs.

2.2 Interopability

The main development of OpenBSC/osmo-bts happens with a small number of mobile phones. The attendees bring devices we either don't use or normally do not have access to. This will test our protocol implementation with various phones and might or might not expose issues.

3 Software Defects

During the first and second day we have seen a low number of problems.

3.1 USSD own number query

The USSD own number query encoding was broken. In our support library we introduced proper USSD encoding and *n* overloads of our encoding version. There was a *size_t* to *int* conversion issue when checking how many septets were written. The issue has been resolved by using the right encoding function and migrating to the *n* version.

3.2 Filtering by IMSI

Our libosmocore library supports filtering log messages by IMSI. In theory this should allow to analyze the problems of a specific subscriber. The filtering function was not properly registered when initializing the logging framework sub-system. The issue has been resolved in libosmocore but we didn't want to restart the osmo-nitb Software. We have used the below trick to register the filter function.

```
$ gdb -p ‘pidof osmo-nitb‘
(gdb) p osmo_log_info->filter_fn = filter_fn
(gdb) c
(gdb) q
$
```

3.3 Late Replies during Location Updating

During the Location Updating procedure we collect the IMSI and IMEI of the subscriber using the Identity Request mechanism. We ended with a NULL dereference when the response to our request arrived after the timeout we have for handling identity requests. A NULL check has been added to the code path.

3.4 Timeouts during SMS on TCH/F

We experienced multiple crashes when trying to deliver a Short-Message during an active call. To deliver the short message a link layer connection for SAPI=3 needs to be established. When this timedout the SMS handling code tried to free the transaction and would crash while iterating over the list of transactions. The osmo-nitb code currently has two kind of transactions one for Call-Control (CC) and one for SMS handling. To conserve space the data for SMS and CC were put in an union. The code that deals with the timeout didn't check for the kind of transaction. On AMD64 when interpreting the union as a SMS the pointer to the SMS looked like a valid address and when dereferencing it we would run into a segmentation fault.

3.5 Rogue connects to RSL

The osmo-nitb Software supports TCP/IP based GSM Base-Stations. The software is listening on port 3002 for OML connections and on port 3003 for the RSL connection. When a new RSL connection is made the code attempts to identify the BTS this connection is coming from. Receiving a valid RSL packet before the look-up check completed lead to a crash. We have added a check to see if the data structures for the RSL connection are fully initialized before trying to forward the message.

4 Interopability issues

4.1 Vodafone Germany

We were facing an unexpected issue that certain phones lost the network and didn't reconnect. We first noticed this with iOS devices but various other phones had similar issues. It turned out to be an odd behavior by the German Vodafone network. A mobile phone assumes that there is just one global GSM network and when the home network is not visible a phone will search for other networks and will attempt to roam by starting the Location Updating procedure. We would have expected that the roaming will be rejected with the *PLMN not allowed* reject reason but in the case of Vodafone the phone received *IMSI not in HLR* reject reason. The effect of this reject reason is that the phone will stop communicating with the SIM Card and that no further Location Updating will be attempted. Phones needed to be restarted to re-connect to our network.
We have resolved this issue by adding the German operators to the forbidden PLMN list but this required to program the SIM. We need to forbid other networks the next time we provision SIM cards.

4.2 Missed Periodic Updates

The network was configured to require periodic location updating. When a subscriber leaves the venue we would still try to page him for mobile terminated SMS and Calls. With periodic location updating we can set the subscriber to inactive if an update is missed. Some phones did miss the periodic updating and when asking for a service we rejected it with by saying that the IMSI is not in the VLR. We had hoped that a phone would start a Location Updating Procedure. It didn't happen though. We have modified the code to allow an implicit attach.

4.3 SS interrogation during Location Updating

There is no support for supplementary services in osmo-nitb. Some telephones asked for the state of the Call-Forwarding and this request has not been answered at all. This means that the transaction number remains occupied and a sub-sequent own number query would fail. We have modified the code to reject supplementary service invocations we don't handle.

5 Usage

The usage of the GSM network has increased this year. It is used for personal communication, interaction between attendees to machine and for spamming.

TODO: Add numbers...

5.1 Communication

We have noticed that people start using the system for real communication between attendees. This is specially true for non German subscribers that would like to communicate with other attendees.

5.2 Human to Machine

Multiple installations interacted using SMS. We hope that this trend will increase in the years to come.

5.3 Spam

The amount of mass spammers appears to go up. We don't know if this is considered an issue and if some kind of *credit* system should be built or spam handling.

6 Conclusions and Outlook

The system has been more stable than in previous years and the number of users, calls and SMS have gone up. Our system is using the very early call assignment. This means that for a mobile orginated call we attempt to immediately assign a traffic channel. In case no more traffic channels are available we will not assign any channel. One approach is to use half rate traffic channels to double the number of possible voice calls. Alternatively we can finish the implementation of early/late assignment during call control or even making an early hand over to another reachable BTS.
The A3A8v3 algorithm has been reverse engineered and we should start using it for the next batch of SIM cards. We could start to use A5/3 for the encryption on the air interface as well.
We have not used/implemented cell broadcast services and we would be happy if somebody would start to implement it. We very much look forward to see how phones handle tsunami warnings. For the next year we would like to provide more services that are built on top of SMS, USSD and voice call handling.