Report of OpenBSC GSM field test August 2009, HAR2009 Vierhouten, The Netherlands

Harald Welte <laforge@gnumonks.org>

June 7, 2011

Abstract

HAR2009 is a gathering and conference of technology enthusiasts and *hackers* in a broad sense: Individuals who are interested in understanding and tinkering with technology.

For the first time at such a hacker conference, a GSM test network was operated under approval of the regulatory authority. The network was operated on a novel *Open Source* implementation of the GSM network side protocol stack called *OpenBSC*.

This is a report on the experience and result of the field test.

Contents

1 Description of test setup

The test setup consisted of two Siemens BS-11 microBTS with each two TRX, connected over a E1 line to a standard PC running the Debian GNU/Linux Operating System and the OpenBSC software.

1.1 Siemens BS-11 microBTS

Siemens BS-11 microBTS are > 10 year old 2G-only GSM BTS intended for small cells, to get more coverage and capacity to locations at which it is needed in a GSM network.

As opposed to traditional BTS, the BS-11 are not based on a rack full of TRX, power combiner, etc. The BS-11 is a single compact unit containing all components from A-bis (E1) link to the Air interface. They're meant for pole or wall mount. They include flat patch antenna that are typically attached directly to the BTS case. Each BTS has one integrated Antenna panel, including both Rx and Tx for the two TRX of the BTS. The maximum transmit power for each TRX in the GSM 900 band is 2W.

All transceivers of both BS-11 have been configured by the use of local maintenance terminal to limit the transmit power to conform with the limit imposed by the test license: 100mW.

The BTS were placed at the bottom of a tree on top of a hill on the test site. The antenna had been detached, extended by 2m RG-58 antenna cable and mounted with duct tape at about 2.5 meters height to the trunk of the tree.

The antenna were mounted back-to-back (offset by about 40cm in height), each antenna facing to half of the test site, at a slight downwards angle. The physical setup can be seen in Figure 1.

(a) Picture of the BTS + Antenna installed on a tree

(b) Picture of the two antennae mounted back-to-back

Figure 1: Physical installation of the two BTS

1.2 A-bis Link

Both BS-11 were connected by a multi-drop E1 link of about 48m length, terminated in a Linux PC running the new open source OpenBSC software. The E1 line card was a "HFC-E1 evaluation board" as sold by Colognechip GmbH in Cologne, Germany. This E1 line card is operating in NT mode, i.e. acting as clock master for the E1 line.

Since the crystal clock of the E1 card is not accurate enough for the high accuracy requirements of the GSM carrier clock, the BS-11 were configured to run in standalone mode, based on their internal OCXO. This internal clock source was pre-calibrated before bringing the BS-11 to the test site.

1.3 PC running the GSM Network

The Linux PC was running the Debian GNU/Linux operating system on a AMD Opteron 64bit x86_64 architecture. A custom, modified HFC-E1 mISDN kernel driver supporting multiple E1 timeslots for signalling was implemented and used.

(a) The tent in which the OpenBSC PC was running

(b) The PC running the OpenBSC software

Figure 2: The core GSM network of the HAR2009 test network

The actual operational OpenBSC can be seen in Figure 2

There was no connection to any other public or private network, neither classic POTS nor VoIP of any sort. As such, only SMS and voice calls could be established between registered subscribers of the test network.

1.4 OpenBSC

OpenBSC is a novel implementation of the minimal required subset of BSC, MSC and HLR. It was developed in a few months, mainly by Harald Welte, the author of this report. During the year 2009, a community of individual enthusiasts with interest in GSM protocols and GSM security has formed around OpenBSC. There is no company or other commercial or non-commercial entity behind its development.

OpenBSC is Open Source software and licensed under GNU General Public License, i.e. the source code is available to anyone, at no charge, with no warranties. However, any modified versions of OpenBSC must also again be released under the same license terms to everyone, ensuring the the source code of all derivative versions is and will always be available to all interested parties.

The goal of OpenBSC is to enable the wider IT security community to perform practical GSM protocol security analysis. The Open Source nature allow any programmer to intentionally violate GSM protocol specs by sending messages at the wrong protocol states, sending invalid messages or testing MS side GSM stacks for implementation weaknesses.

OpenBSC furthermore serves as an inexpensive lab setup where students and other interested parties can set up a very simple GSM network for learning about GSM protocols.

OpenBSC is not intended as a product-quality BSC/MSC/HLR implementation, as it was never written with Telco-grade scalability and reliability in mind.

More information about OpenBSC as well as the full source code can be found at http://openbsc.gnumonks.org/

1.5 Registration procedure

In order to maximize the number of participants for the test, but minimize the impact or implications for regular GSM subscribers in the same area, a special registration procedure was designed and implemented.

To achieve a large number of voluntary test participants, as well as to increase the convenience to participate, it was decided to use the regular SIM cards of commercial operators in roaming mode, rather than to issue our own SIM cards for the test network.

However, to prevent disruption of the commercial GSM networks, we could not simply just accept everyone into the test network.

At the time a LOCATION UPDATE REQUEST from a particular IMSI was first seen in our test network, we sent LOCATION UPDATE ACCEPT, initiated and completed the delivery of a mobile terminated (MT) SMS, and then immediately removed the subscriber from our network by performing a AUTHENTICATION REQUEST followed by an unconditional AUTHENTICATION REJECT.

The SMS content was

```
HAR 2009 GSM. Register at http://har2009.gnumonks.org/ Your IMSI is 012345678901234
auth token is ABCDEFGH, phone no is 12345.
```

The AUTHENTICATION REJECT prevents the phone from performing further LOCATION UPDATE procedures with our network. Even in case the MS is switched off and on again and sends successive LOCATION UPDATE REQUEST to the test network, our network remembers the IMSI and will LOCATION UPDATE REJECT all such attempts.

This ensures that apart from the brief period to deliver the SMS, no phone will ever stay for an extended period of time on our network.

However, if the subscriber has actually visited the website indicated in the SMS and approved the usage terms of the test network by entering his IMSI + Authentication Token, we marked his entry active in our HLR and permit him to perfom successive LOCATION UPDATE and other operations on our test network.

A screenshot of the registration website can be seen in Figure 3

The phone numbers to be used for the subscribers were randomly allocated from a private 5-digit numbering plan.

1.6 No cryptographic authentication or encryption

Since the Ki of the SIM issued by commercial GSM operators is not known to us, no cryptographic (A3/A8) authentication or A5 based encryption was used on the network.

The operators of the test did not consider this a weakness. Confidentiality was not required in an all-public test anyway. Furthermore, other groups present at HAR2009 such as airprobe are developing a software defined radio (SDR) based passive GSM protocol analyzer. Initial development and testing of such software is much simpler in test network that does not implement cryptography.

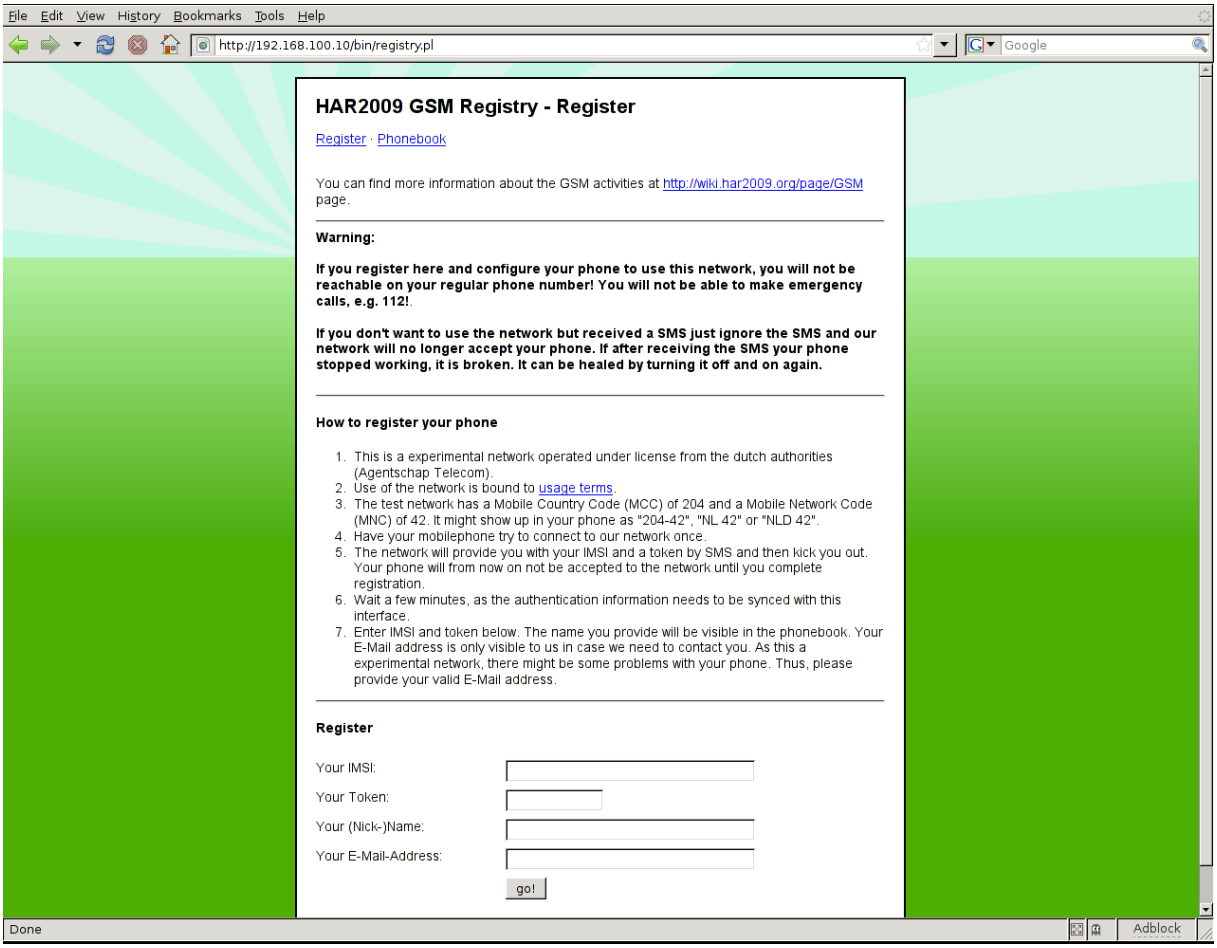

Figure 3: The HAR2009 GSM network registration web form

1.7 No support for emergency calls

Since the test network did not have any support for emergency calls, we ensured that the SYSTEM INFORMATION messages in our BCCH did correctly indicate that no emergency calls are possible in our network. This prevents MS without an active SIM to try to use our network to perform EMERGENCY SETUP.

1.8 No support for Handover

OpenBSC does not yet have support for hand-over of active dedicated channels. If a subscriber moves from one BTS' coverage area into that of another BTS, the call will drop. For the purpose and duration of this test, it has not been a big problem, as the speed of the subscribes is low (walking) and the duration of each call was typically very short.

However, as soon as OpenBSC implements handover, a field test of similar size is recommended for testing and verification of the implementation.

2 Objectives of the field test

2.1 Load Test

The objective of the field test was to do a realistic load test with as many real-world users as possible.

OpenBSC was so far only tested under small lab conditions, using either two single-TRX BTS or one dual TRX BTS with a maximum of 10 MS attached at any given time. The MS equipment was always static,

and the network load was extremely low. Furthermore, the Tx power in those tests was always limited to 30mW or less, i.e. only indoor tests at low distance were performed.

Thus, the much more realistic load of many users on the field test was a very important test.

2.2 Interoperability

The MS used were not issued by the tester. Rather, each participant brought his own personal MS. The intent is to achieve interoperability testing with many different MS-side GSM implementations of both current as well as old equipment.

2.3 Skill building

The programmers of the OpenBSC software did not have much exposure to real-world GSM networks and especially not use/deployment/operation or even development of carrier-grade GSM equipment.

Therfore, operating a network of this relatively large size provided an interesting opportunity to observe a GSM network literally "in the field", adjusting operational parameters on the network side and observing its effects on the actual subscriber base in real time.

3 Results

3.1 Network Load

The network was used a total number of 863 registered subscribers. This is a relatively low quota, given the number of more than 3000 potential users (attendees of the HAR2009 event). Using/testing the OpenBSC GSM network at HAR2009 was of limited attractivity to many users since there was no connection to the on-site DECT network with much more subscribers.

However, to limit the complexity of the network setup and to respect the regulatory requirements, no connection between the private GSM and the private DECT network was implemented.

Furthermore, visitors with only one GSM handset needed to stay on the regular operator networks in order to remain able to make and receive calls to public networks.

The number of users was still sufficient for achieving good test results.

3.2 Network Availability

The network was running throughout the event, within the timeframe authorized by the test license granted by Agenschap Telecom.

Throughout this time, there were unscheduled service interruptions whenever the OpenBSC team has fixed a bug or made some other change to the OpenBSC software which required an OpenBSC restart. Each restart takes about 10 seconds.

3.3 Network coverage

Several site surveys with network monitor enabled Nokia 3310 handsets indicated almost complete coverage of the event site. Slightly higher transmit power would probably have resolved those small network availability issues, but this was not possible due to the limits imposed by the test license.

Figure 4 shows a phone in Nokia Network Monitor mode while being used for coverage testing on the event camp site.

3.4 Network usage

The network usage was surprisingly low. A total of more than 1800 voice calls were established throughout the test, and more than 27,000 SMS were transmitted.

Figure 4: A phone in network monitor mode used on-site

The average call duration was very low, which was expected. Although no conversations were monitored, we assume the average user was simply using the phone to communicate their current location on the site, or set up / coordinate meeting schedule with other people.

The high number of SMS are caused by two reasons: First, there was a full conference programme with several tracks in parallel, i.e. people were likely to have their phones in silent mode and not make phonecalls while attending a seminar or workshop. Secondly, a number of users connected their MS to a laptop computer to send SMS spam to other usesr.

The available TCH and SDCCH timeslots were sufficient for the number of users and the use patterns in the test network. Network overload situations with no available channels were only observed in very short and rare occasions.

3.5 Location Updating between Location Areas

OpenBSC received and parsed the Location Update messages correctly and was able to deliver the paging requests only to the location area in which the particular MS was seen last.

While this is a standard behavior expected of any GSM network, it had so far not been tested with OpenBSC yet.

3.6 RRLP testing

Many modern smartphones with GPS receiver are rumoured to have support of the RRLP protocol. According to its specification, RRLP enables the network (or anyone claiming to be the network) to obtain the current GPS fix of the MS without any form of authentication.

The operators of the test network consider this a dangerous feature of GSM networks and were interested in determining if this protocol is actually implemented in real-world MS.

Therefore, OpenBSC was extended to send a RRLP position request message every time a dedicated channel was established, e.g. at location update, mo/mt sms and mo/mt voice call establishment time.

Although RRLP supports sending GPS aiding data to the MS, this was not implemented in OpenBSC. Not having this data probably increased the TTFF (time to first fix) from several seconds to about a minute, causing some RRLP requests to time out.

Implementation of this feature was only finished on the last day of the test, explaining the relatively little number of successful (and unsuccessful) RRLP requests.

Result: RRLP is not just a theoretical feature specified in the GSM/3GPP specs. It is implemented by numerous high-end smartphones. There is no authentication of the network. There is no notification of the user. There is no way for the user to disable this [mis]feature.

Impact: Public debate about this feature is needed. Operators probably need to consider working on some terms about how they use this feature in their privacy policy.

3.7 SMS interoperability problems

The SMS-CP and SMS-RP protocol implementations as part of OpenBSC have only been added very recently. They have been tested only with a very limited number of MS models. During the field test, many users experienced malbehavior such as unsuccessful SMS transmission and duplicate SMS reception.

On-site analysis of protocol traces have shown that the SMS submission (MS→network) was using invalid transaction identifiers in the network to MS direction, causing the MS of a MO SMS to ignore the acknowledgement of successful reception by the SMSC (also part of OpenBSC).

Thus, the SMSC has stored the SMS multiple times, causing multiple successful deliveries of the same message content to the receiver (MT SMS).

The observed error could not be fully fixed/verified until the end of the test, further investigation is required.

3.8 OpenBSC software stability

OpenBSC software was presumed to be somewhere between alpha and beta level quality. Many implementation shortcuts have been made all over the codebase in order to provide quick results. Focus is on getting things to work, rather than implementing them correctly.

However, OpenBSC has been working quite reliably. Crashes (segmentation faults due to invalid memory accesses) were observed infrequently. The operating environment ensured core dumps were stored at each crash, enabling further analysis and fixing of the respective errors.

One particular timer list corruption bug has been discovered, drastically improving software stability.

4 Summary

OpenBSC has shown that it is more than a simple proof-of-concept implementation for small single-BTS, single-TRX laboratory use. It can well be used in deployments with several hundreds and potentially thousands of MS served by a number of BTX and TRX.

The software is still not at production quality, as it was expected. There are interoperability problems and lack of core features such as in-call handover.