OpenBTS Overview

مهند مصطفى أشرير

OpenBTS Layers

The OpenBTS application contains:

- L1 TDM functions (GSM 05.02)
- L1 FEC functions (GSM 05.03)
- L1 closed loop power and timing controls (GSM 05.08 and 05.10)
- L2 LAPDm (GSM 04.06)
- L3 radio resource management functions (GSM 04.08)
- L3 GSM-SIP gateway for mobility management
- L3 GSM-SIP gateway for call control
- L4 GSM-SIP gateway for text messaging

SIPAuthServe

- An application that implements Subscriber Registry, the database of subscriber information that replaces both the Asterisk SIP registry and the GSM Home Location Register (HLR) found in a conventional GSM network.

Accessing the System

- All Range installations of OpenBTS Release 4.0 run Ubuntu Linux v12.04 operating system.
- the default IP address of \192.168.0.21".
- Login: openbts &Password: openbts
- The account is super-user (sudo) enabled.
- From a Windows machine an SSH client (like PuTTY) can be used.

Physical Measurements

- Handset Distance. Round-trip propagation delay is directly proportional to handset's distance from the BTS.

- That distance is approximately 535 meters per symbol period of round-tip delay. The round-trip delay reported in the Channel table is in two parts:

  - Timing Advance { This is a clock oset inside the handset controlled by the BTS.
  - Timing Error { This is a timing error measured by the BTS on the arriving signal.

Uplink Power (Solved Problem)

Maximum output power levels for GSM MSs.

Power Class	GSM850 GSM900 Max. Ouput	DCS1800 Max. Output	PCS1900 Max. Output
1	N/A	1 W (30 dBm)	1 W (30 dBm)
2	8 W (39 dBm)	0.25 W (24 dBm)	0.25 W (30 dBm)
3	5 W (33 dBm)	4 W (36 dBm)	2 W (33 dBm)
4	2 W (33 dBm)	N/A	N/A
5	0.8 W (29 dBm)	N/A	N/A

Location Area Code

- GSM.Identity.LAC: 16 bits, values 0xFFxx are reserved. For multi-BTS networks.

- assign a unique LAC to each BTS unit. (This is not the normal procedure in conventional GSM networks, but is the correct procedure in OpenBTS networks.)

Handover in openBTS

- In conventional GSM networks, handover is coordinated by a BSC or MSC that the two BTS units have in common.
- In OpenBTS networks, handover is coordinated by the BTS units themselves using the Range Peering Protocol (RPP).
- Handover is a complex process that aects every aspect and element of the OpenBTS software.
- A list of IP addresses of neighbour BTSs available for handover. By default handover is disabled.

Authentication

- SIPAuthServe Authentication Interface.
- SIPAuthServe supports direct SIP authentication on the Subscriber Registry, but using:
  - the RAND value as the nonce.
  - an operator-specied A3/A8 instead of MD5 as the hash function.
- The SIP username is always \IMSI" followed by the digits of the IMSI.

Creating New Subscribers

- New SIMs : requires Ki and A3/A5, and can be modified.

- Using Pre-existing SIMs: OpenBTS systems can use pre-existing SIMs even in the absence of a carrier roaming agreement, although full RAND-SRES authentication cannot be used because Ki is not known.

Manually register users

- Interactive via SMS:
  - In SMQueue: The \SC.Register.*" parameter
  - In OpenBTS: { \Control.LUR.OpenRegistration" parameter must be defined to accept the intended handsets and the \Control.LUR.OpenRegistration.*" parameters must be defined.

Open Registration

- Open registration is a mode where all MSs are accepted for registration.

- This parameter can be used to reject/accept IMSIs depends on the IMSI:

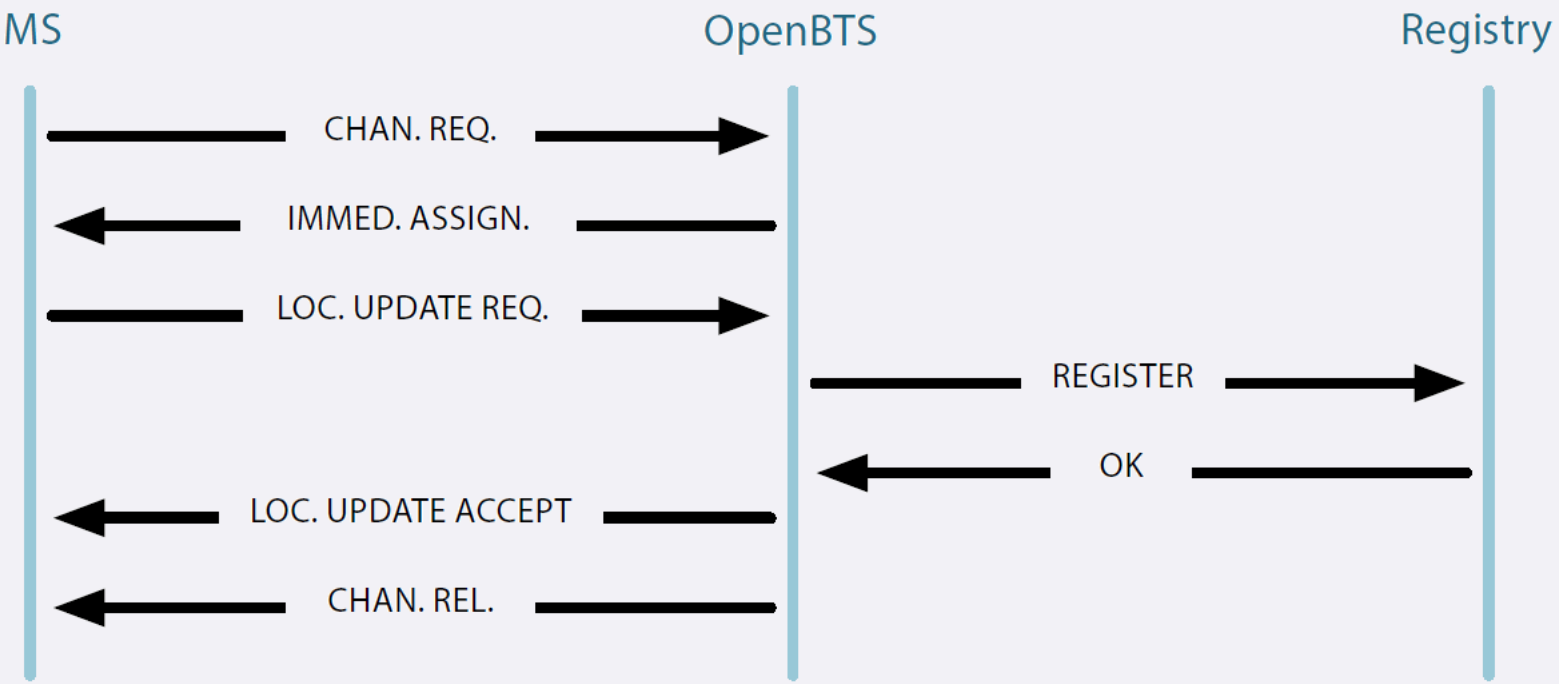
  - ^001 Match any IMSI starting with \001", the MCC for test networks.
  - ^00105 Match any IMSI from the test network with MCC=001 and MNC=05
  - 00105000000042 Match only IMSI \00105000000042"
  - 0 Match any IMSI containing a \0"
  - 1 Match any IMSI containing a \1"
  - 1024$ Match any IMSI ending in \1024"

COMP128v1 and SIM Cloning

- The GSM specifications do not dene specic algorithms for A3 & A8.
- A3/A8 algorithm uses called COMP128.
- So, Design SIMs to shut down or self-destruct if too many A3/A8 calculations are requested too quickly.

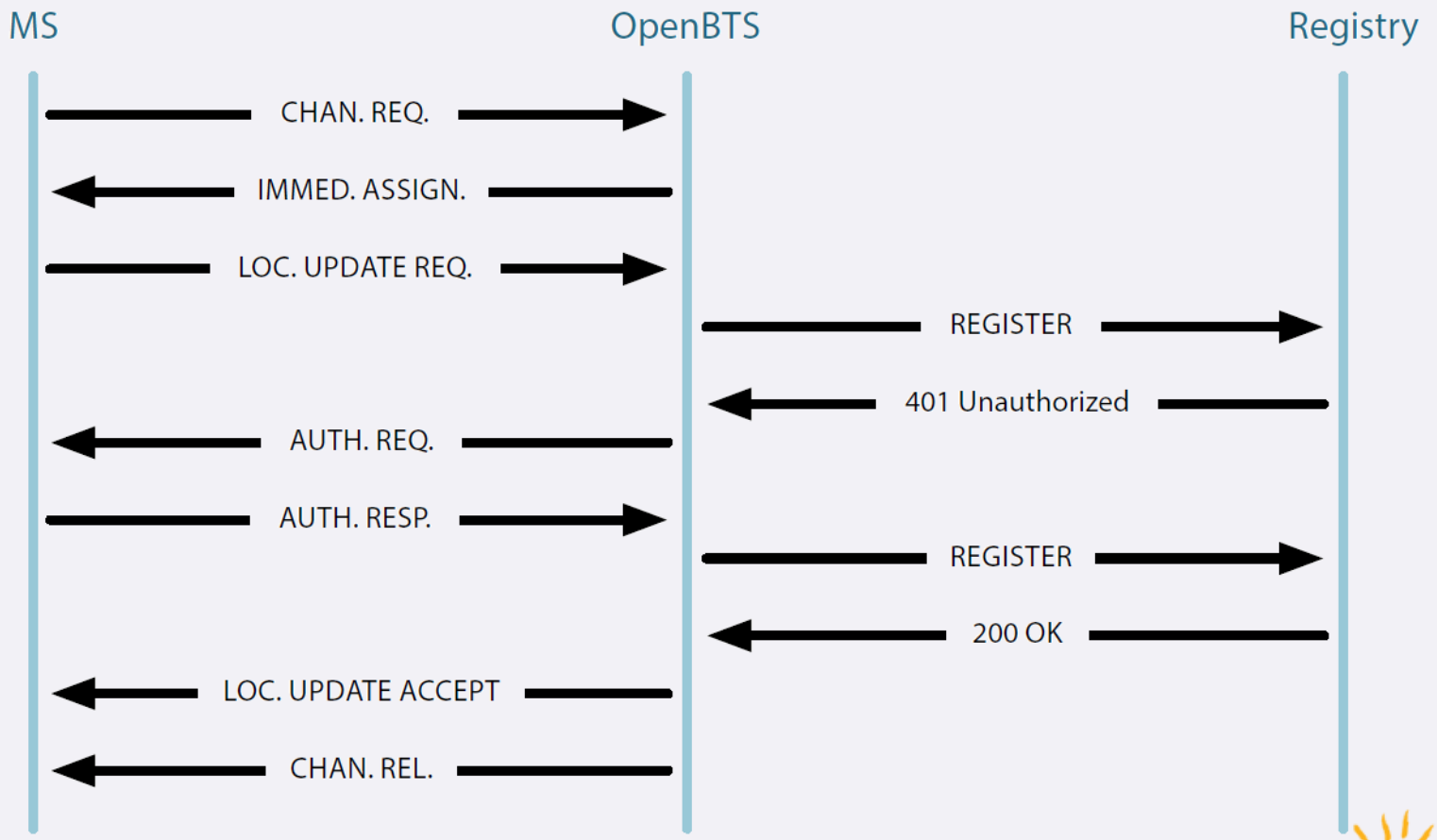
Registration & Location Update

GSM location update mapped to a SIP REGISTER (non-authenticating case).



Registration & Location Update

GSM location update mapped to a SIP REGISTER (with authentication).



Speech coding

- Currently, OpenBTS only supports the GSM full rate codec (GSM-FR).
- The other codecs supported by Asterisk and of potential interest to OpenBTS operators are:
  - G.711 (a-law or mu-law) { This 64 kbit/sec codec oers very good speech quality and is the most widely used in the PSTN and supported by nearly all VoIP carriers.
  - G.729 { This is an 8 kbit/sec codec with fair speech quality and reasonably well-supported by VoIP carriers. The main drawbacks of G.729 are high computational complexity and a licensing fee of about $10/line/year.
  - Speex { This codec can operate at rates as low as 4 kbit/sec and has speech quality and computational complexity similar to G.729 at 8 kbit/sec. The advantages of Speex are greater configuration flexibility and freedom from licensing fees. Support for Speex is growing among VoIP carriers.
  - LPC-10 { This is a low-complexity 2.4 kbit/sec codec. The speech is understandable, but often unnatural sounding.

Overhead problem

- The media protocol most commonly used with SIP is RTP (IETF RFC-3550).
- When any codec is run over RTP, there is an additional overhead.
- For most codecs, the overhead of RTP is greater than the bandwidth requirement of the codec itself.

Overhead solved

- Asterisk also supports a combined signaling-and-media protocol called IAX.
- IAX has an overhead of roughly 20 kbit/sec with a codec frame size of 20 ms, but unlike RTP, IAX can distribute this overhead over many calls through a technique called \IAX trunking".

Codec	per call raw rate	per call over RTP	7 calls over RTP	7 calls IAX trunking	speech quality
G.711	64	81	567	468	toll-quality
GSM-FR	13	30	210	124	toll-quality
G.729	8	25	175	97	near-toll-quality
Speex	8	25	175	97	near-toll-quality
Speex	4	21	147	60	not toll-quality
LPC-10	2.4	20	136	37	not toll-quality