Introducing OsmocomGMR

Sylvain Munaut

28C3, December 29th, 2011

Outline

About the speaker

- Linux and free software "geek" since 1999
- M.Sc. in C.S. + some E.E.
- General orientation towards low level
  - Embedded, Kernel, Drivers and such.
  - Hardware (Digital stuff, FPGA or RF more recently)
- Interest in various telecom projects for about 3 years
  - Osmocom projects (OpenBSC, Osmocom-BB, ...)
  - Airprobe, OpenBTS ...
  - In my spare time

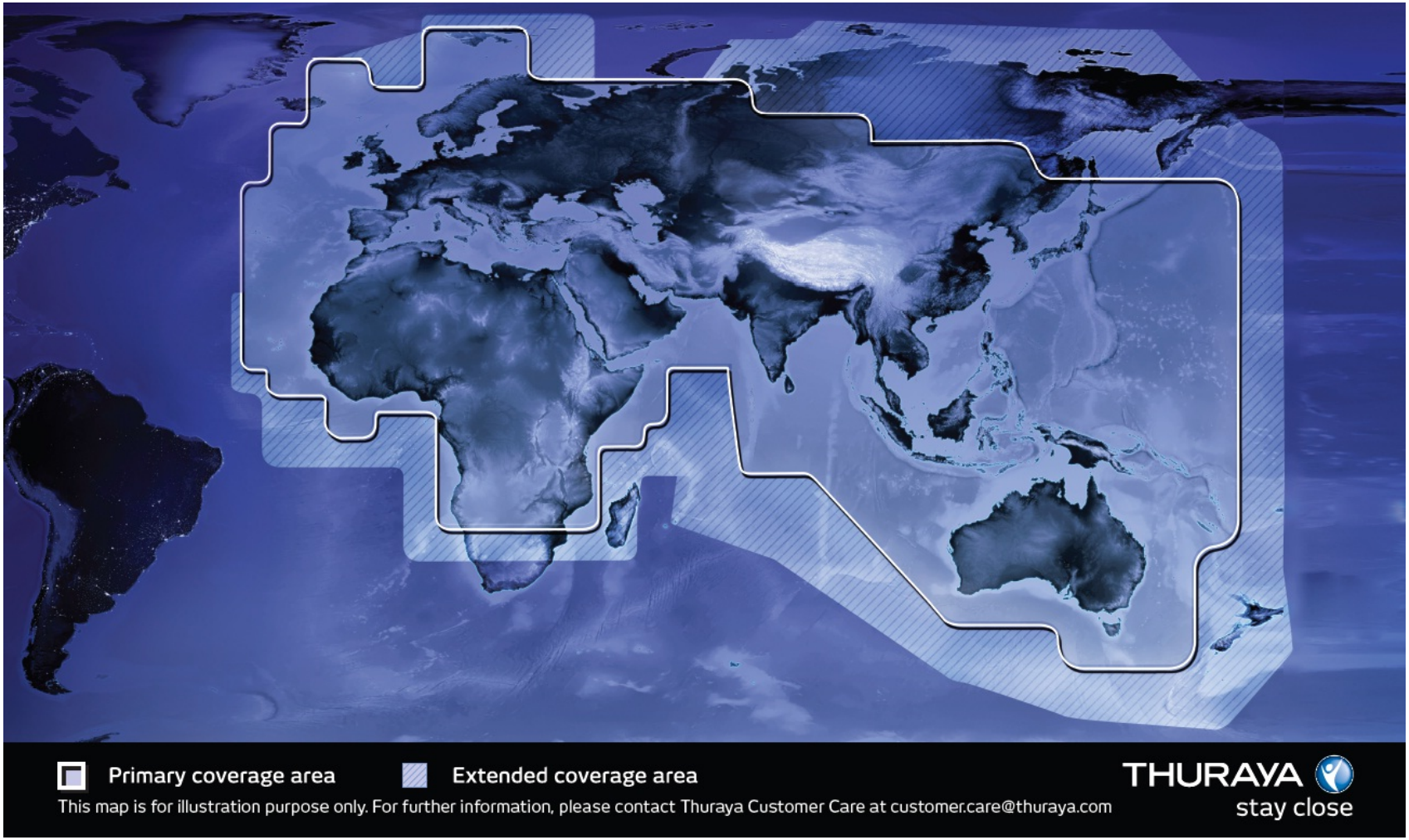
What is GMR ?

- "GEO-Mobile Radio Interface"
  (GEO stands for Geostationary Earth Orbit)
- ETSI standard for satellite phones
- Heavily based on GSM
- Multiple standards :
  - GMR-1 (ETSI TS 101 376)
    - GMR-1 (the one described in this talk)
    - GmPRS
    - GMR-1 3G
  - GMR-2 (ETSI TS 101 377)

Deployment

- GMR-1
  - Thuraya
    - Two satellites : Thuraya 2 (98.5E) and Thuraya 3 (44E)
    - Visible from Europe ⇒ Main focus of our attention so far
  - SkyTerra
  - TerreStar
  - ICO
  - (Inmarsat)
- GMR-2
  - Inmarsat "IsatPhone"
  - ACes

Deployment
Thuraya



Comparison to GSM
Features

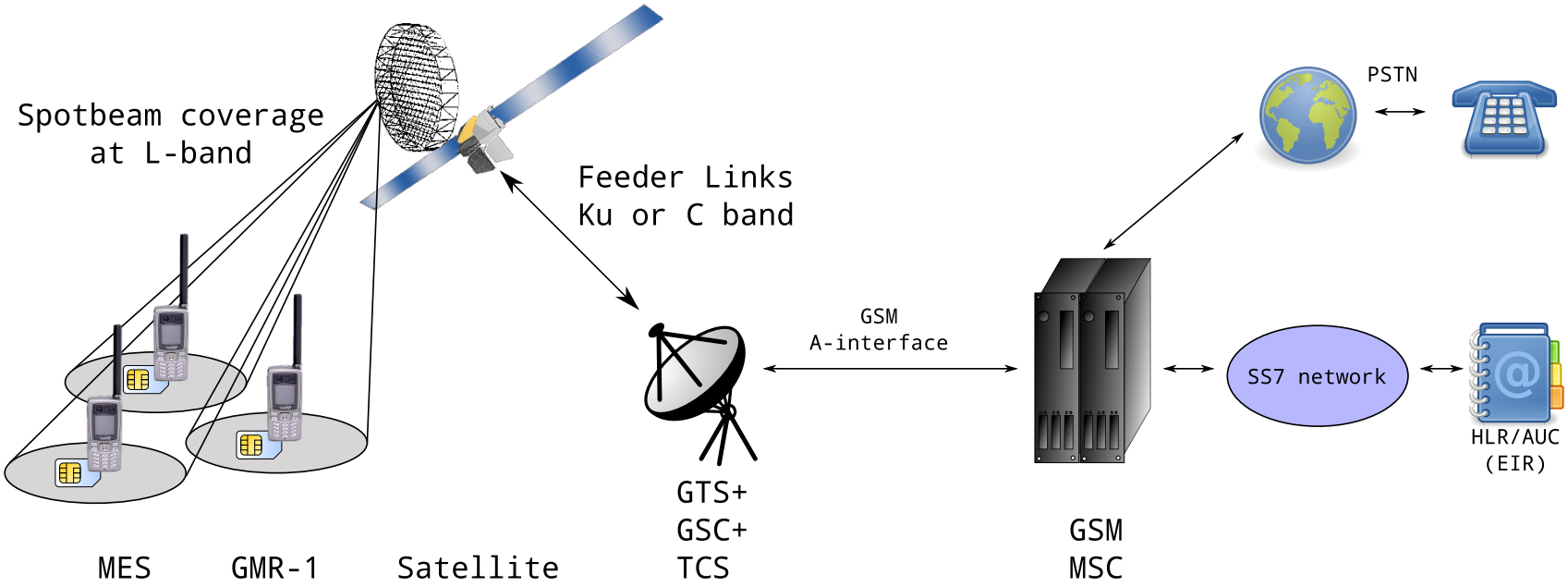
- New names
  - BTS → GTS, BSC → GSC, BSS → GSS, ...
  - MS → MES(-MS)
- New Specialized features
  - Terminal-to-Terminal calls
  - High Penetration Alerting (HPA)
- Tight links to GPS
  - Almanac and Ephemeris sent by the satellite
  - Position reported in RACH (Channel Request)
- New speech codec: AMBE
- New cipher

Comparison to GSM
Protocol Stack

- Layer 0/1: Completely different
  - Different bursts and TDMA multiplex / multi-frame
  - Different modulation
  - More channels types
- Layer 2: LAPSat vs LAPDm
  - Both simplified version of LAPD
  - Shorter header
  - k=16 window size for outstanding unacknowledged segments
- Layer 3:
  - RR different
  - MM/CM common
- Packet Data:
  - RLC/MAC different
  - LLC and above common

Network Overview

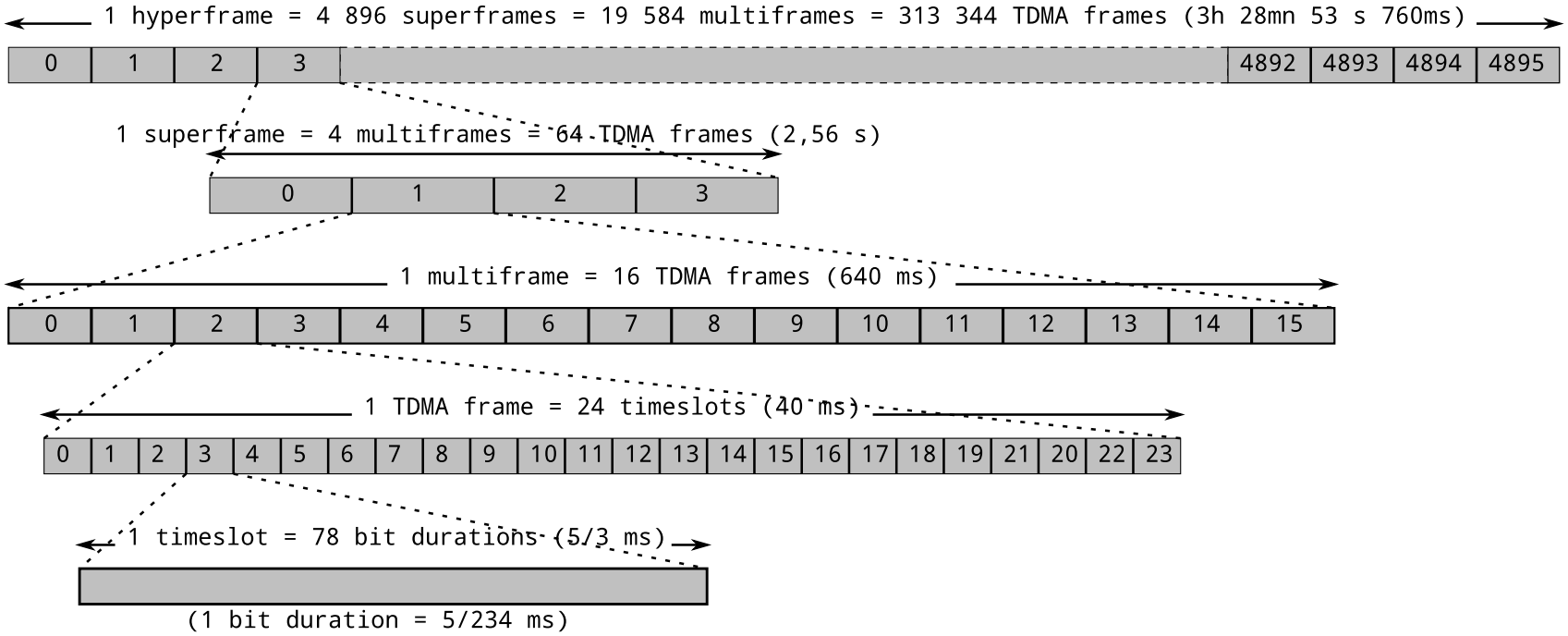
Architecture and Protocol Stack



Physical layer
Frequencies

- Spot beam coverage
  - L-band
  - Left Hand Circular Polarization
  - Downlink: 1525 to 1560 MHz
  - Uplink: 1626.5 to 1660.5 MHz
  - Divided in 1087 ARFCN (channel pairs) of 31.250 kHz
- Feeder Links
  - C-band (DL: 3.400 to 4.200 GHz / UL: 5.850 to 6.725 GHz)
  - Ku-band (12 to 18 GHz)
  - No specifications

Physical layer
TDMA

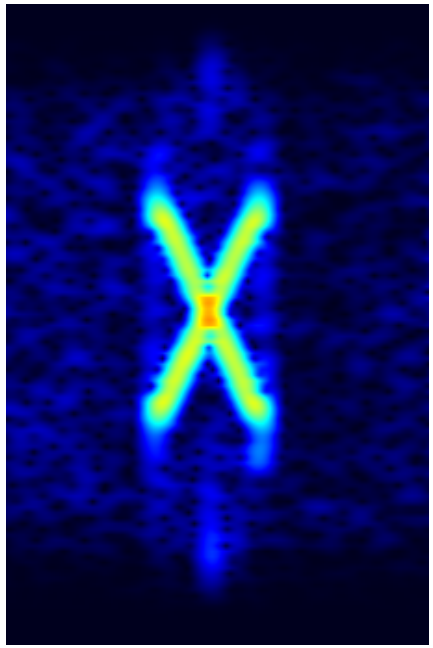


- Fully synchronous
- Base symbol rate: 23.4k
- Bursts occupy several consecutive timeslots (2, 3, 6, 9)

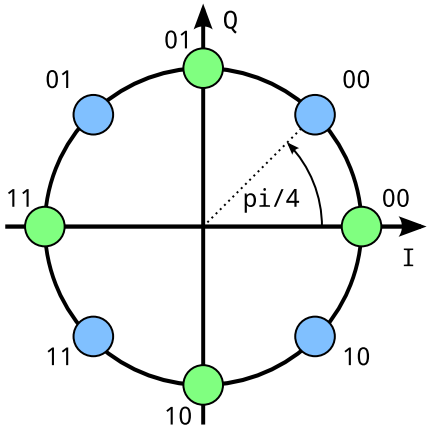
Physical layer

FCCH: "X" marks the spot (beam)

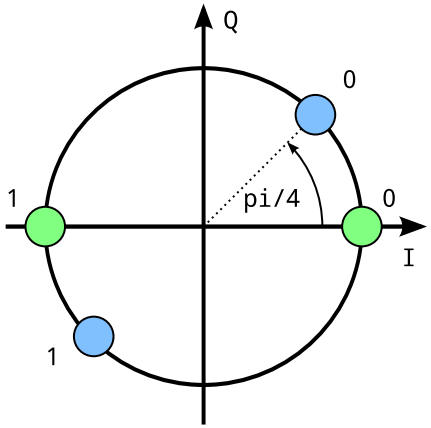
- Dual Chirp waveform over 3 timeslots
- Synchronization steps
  1. Rough position by correlating with reference dual chirp
  2. FFT peak of RX window multiplied by reference up-chirp $\rightarrow f_1$
  3. FFT peak of RX window multiplied by reference down-chirp $\rightarrow f_2$
  4. Derive time alignement error from $f_1 - f_2$
  5. Derive frequency error from $f_1 + f_2$
- More info: `http://goo.gl/Qu4pv`



Physical layer
Normal Bursts



$\pi/4$-CQPSK



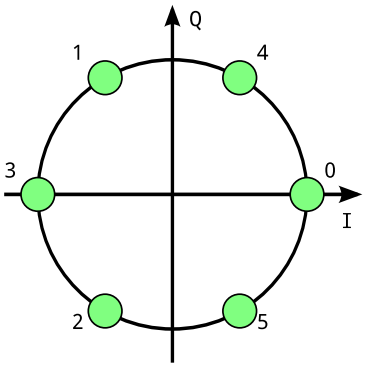
$\pi/4$-CBPSK

- Lots of different burst types, each with its own structure
- BCCH, DC2, DC6, NT3, NT6, NT9, RACH

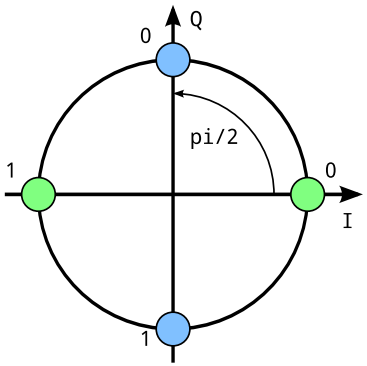
- Used only for FACCH3 and SDCCH

Physical layer
Other Bursts

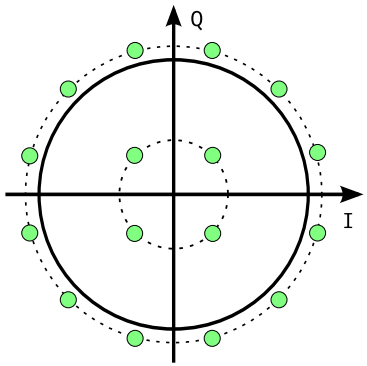
- Other modulations used
  - 6-PSK for BACH (HPA)
  - $\pi/4$-DBPSK for DKAB
- GmPRS and GMR-1 3G packet channels (PNB):
  - New modulations: $\pi/2$-CBPSK, 16-APSK, 32-APSK
  - New symbol rates: 1x, 2x, 4x, 5x



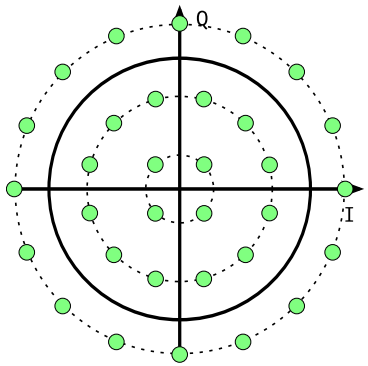
6-PSK



$\pi/2$-CBPSK



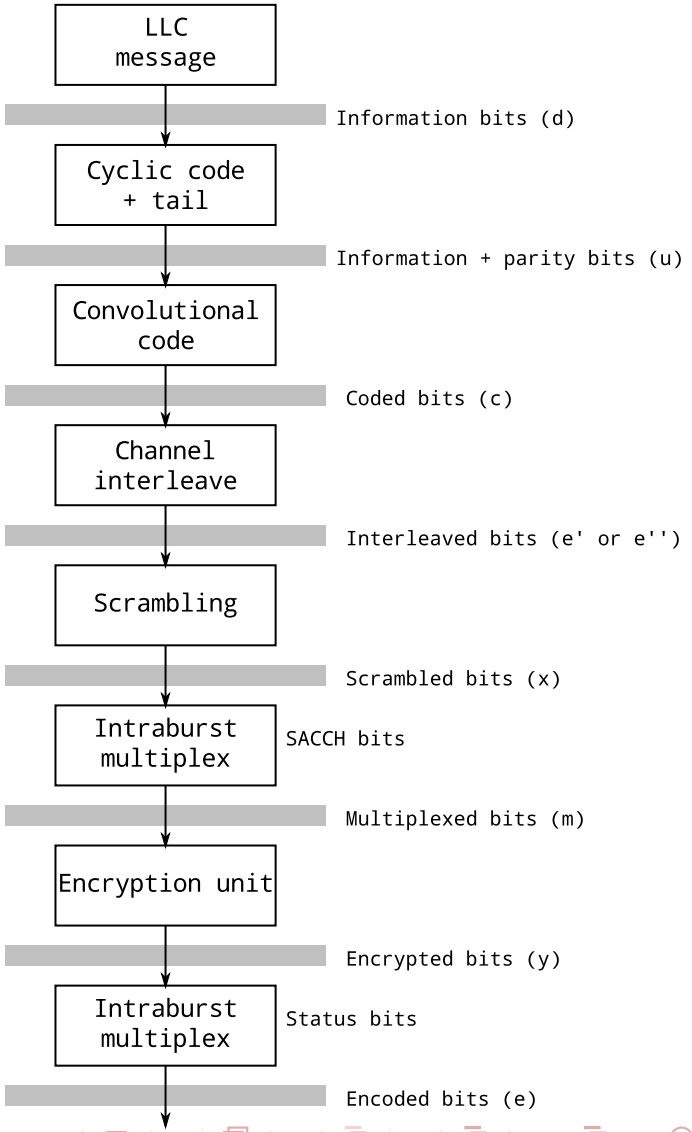
16-APSK



32-APSK

Layer 1
Channel coding

- Depends on channel type ...
- ... but same basic primitives
- Maps L2 frames onto bursts and protects them
  - Error correction
  - Error checking



Layer 2
LAPSat

LAPSat is the data link layer of GMR-1. It mostly handles :

- L3 message segmentation
- Retransmissions
- SAPI multiplexing
- Contention resolution

Layer 3

- Radio Resource (RR)
  - Oversees the establishment of dedicated links
- Mobility Management (MM)
  - Tracks user location
  - Manages authentication and confidentiality
- Connection Management (CM)
  - Call Control (CC)
  - Short Message Service (SMS)
  - Supplementaty Services (SS)

Speech Codec
AMBE

- Advanced Multi Band Excitation
- Low bitrate (4kbps)
- Proprietary (by DVSI inc)
  - No public specification
  - No reference implementation
- Glimmer of Hope:
  - `mbelib`: Implements similar codecs
  - Most likely implemented in phone's DSP
    $\Rightarrow$ Could be extracted

Security

Some good :

- LAPSat contention resolution procedure does **not** send back SABM message content
- Heavy use of DTX should limit known plaintext

And some bad :

- Optional
- Some GSM attacks theoretically applicable "as-is":
  - RACH DoS
  - IMSI Detach DoS
- RACH contains lots of informations in clear
  - Reason for channel request (including dialled number if relevant)
  - GPS position of phone
- Cipher still applied at layer 1

Security
Cipher

- Currently unknown
- Supposedly derived from A5/2
  - It's neither A5/1 or A5/2 as-is, we tried !
- Availability of plain text might be limited:
  - TCH3 channels have less bits per burst
  - No SACCH on TCH3
  - DTX means not empty LAPSat frames
- However:
  - Past experience with A5/1, A5/2, GEA-1, GEA-2 has shown all those to be vulnerable
  - Commercial crackers available

Osmocom-GMR

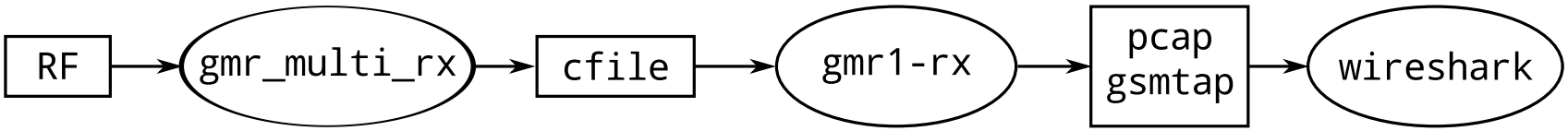
History

- Mid July: Project initiated
- Late July: First signals on FFT
- CCCamp 11: More work on signal reception
- September: First packets demodulated and analyzed
- October: First working code release
- December: TCH3 support

Osmocom-GMR

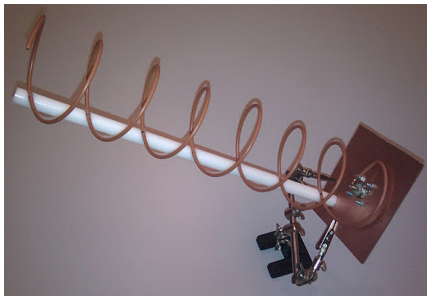
General architecture

- `gmr_multi_rx`: Capture utility
- `libosmo-sdr`: Signal processing utility library
- `osmo-gmr`: Main software stack
  - `sdr/`: Synchronization and demodulation primitives
  - `l1/`: Channel coding
  - `gmr1-rx`: Test software
- `wireshark`: Packet analysis



Reception
Antennas

- Requirements:
  - Good directivity (good gain)
  - Left Hand Circular Polarization (LHCP)
- Tested so far:
  - Offset Dish
  - Helical Antenna
  - Biquad

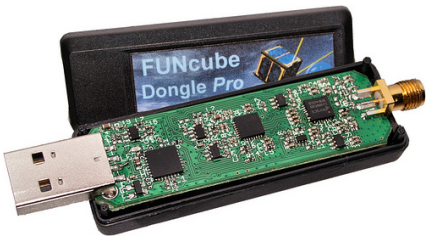


Reception
Filter / LNA

- Both optional
- Low Noise Amplifier:
  - Helps with fainter beams
  - Tested with LNA-23-BP from dg0ve and a modified GPS LNA
- Filter:
  - Prevents out-of-band signals from saturating reception chain

Reception
Capture hardware

- Currently supported:
  - Any ettus hardware (UHD)
    - Large bandwidth ⇒ Multi ARFCN
    - USRP1 could support simultaneous UL/DL
  - FunCube Dongle Pro
    - Low bandwdith ⇒ only a few adjacent channels at a time
  - Soon: OsmoSDR
- But any SDR could be used provided:
  - Sufficient bandwidth (>32 kHz)
  - Tuning to the appropriate frequency range



Reception
Software

Using the `gmr_multi_rx` utility written for this purpose.

- Based on GNURadio
- Simultaneous synchronized captures of several ARFCN
- Optimal center frequency selection
- Channelizing and resampling
- Hardware support:
  - USRP1 using `libusrp`
  - Ettus UHD driver
  - FunCube Dongle Pro

Example usage

```
./gmr_multi_rx --gmr1-dl 267 --gmr1-dl 268
```

Osmo-GMR
libosmo-sdr

Utility library for signal processing

- Complex Vectors (`struct osmo_cxvec`)
- Common operations on them:
  - Scaling
  - Rotation (frequency shift)
  - DC offset removal
  - Correlation
  - Convolution
  - Energy peak finding
- `.cfile` helpers

Osmo-GMR
SDR

Software Defined Radio layer (`src/sdr/*`)

- FCCH acquisition
  - Rough: Correlation
  - Fine: FFT
- $\pi/4$-CxPSK demodulator
- Bursts descriptions
- DKABs
- RX mostly

Osmo-GMR
Layer 1

Channel coding (`src/l1/*`)

- Primitives:
  - Scrambling
  - Convolutional coding
  - Puncturing
  - Cyclic Redundancy Check
  - Interleaving
- Stateless coder / decoders:
  - BCCH
  - CCCH
  - FACCH3
  - TCH3
- TX & RX

Osmo-GMR
Test software

Main receive application (`src/gmr1_rx.c`)

- Acquires synchronization from FCCH
  - Tries to lock to multiple overlapping channels
- Demodulates BCCH and CCCH
- Follows `IMMEDIATE ASSIGNMENT` to TCH3
- Forwards data to GSMTap

Wireshark

- GSMTap extended with GMR-1 support
- LAPSat dissection: complete
- BCCH dissection: partial
- CCCH dissection: All messages seen so far
- RR dissection: All messages seen so far
- CM/MM forwarded to GSM dissector

Demonstration

- GMR signal visualization
- `gmr1-rx`
- Wireshark

Future

- Find the cipher
- Find the speech algorithm
- TDMA framework
- Upper layers implementation
- CSN.1 and 04.008 code generators
- TX side

Help welcome :)

Thanks

Thanks to anyone who contributed to this projects and related ones. Most notably:

- Dimitri "horizon" Stolnikov
- Harald "LaF0rge" Welte
- Steve "steve-m" Markgraf

Further reading

OsmocomGMR `http://gmr.osmocom.org/`

GMR1 Specs `http://pda.etsi.org/pda/queryform.asp`

GSM Specs `http://webapp.etsi.org/key/queryform.asp`