OsmocomTETRA

Researching TETRA and its security

Harald Welte

gnumonks.org
gpl-violations.org
OpenBSC
OsmocomBB
hmw-consulting.de

SRLabs, January 2011, Berlin/Germany

Outline

About the speaker

- Using + playing with Linux since 1994
- Kernel / bootloader / driver / firmware development since 1999
- IT security expert, focus on network protocol security
- Core developer of Linux packet filter netfilter/iptables
- Board-level Electrical Engineering
- Always looking for interesting protocols (RFID, DECT, GSM)

Introducing TETRA

TErrestrial Trunked RAdio

- Digital PMR (Professional Mobile Radio) standard
- Standardization Body ETSI started work in 1990
- First specified in 1995, endorsed by EU Radiocomms Committee
- Commercial Vendors: Motorola, EADS/Nokia, Arteva/Simoco/Pye/Philips, Rohde & Schwarz
- Chinese vendors are expected to appear on the market soon

TETRA vs GSM

- Longer range due to lower frequency (but not vs. GSM 410/450!)
- Higher spectral efficiency (4 speech channels in 25kHz vs. 16 speech channels in 270kHz)
- Specified to work at speeds above 400 km/h
- one-to-one, one-to-many and many-to-many (but: GSM-R ASCI)
- offers direct mode between handsets in case base station is out of range
- separate infrastructure from public networks (but: GSM-R)
- de-central fall-back, i.e. base stations switching local calls

TETRA vs GSM

Summary

- Most of the TETRA advantages could be achieved using GSM-R in a lower frequency band
- Local call switching can be implemented in GSM (think of OpenBSC)
- GSM requires modifications on the air interface for direct mode, but even in TETRA, direct mode is *very* different from trunked mode

It seems, the industry rather re-invented an entirely different system to ensure the resulting equipment can be sold at multiples of the commercial-grade GSM equipment.

TETRA deployments

- In 2009, TETRA was deployed in 114 countries (every continent except North America)
- Typical users: Police, Transportation, Army, Fire Service, Ambulance, Customs, Coast Guard
- But also: Private company networks (industrial plants)
- In Germany there are 63 registered networks (only 5 are BOS)

TETRA deployments

- Follow TETRA Newsletter released by TETRA MoU organization
- Majority of recent deployments seems to be in Asia, specifically China.

TETRA Frequencies

- European Emergency Services
  - 380-383 MHz and 390-393 MHz
  - 383-385 MHz and 393-395 MHz (optional)
- European Private/Commercial Systems
  - 410-430 MHz
  - 450-470 MHz
- Other Countries
  - Depending on local regulatory requirements

TETRA Frequency plan

- Single TETRA carrier normally 25kHz wide, no guard bands
- Channel grid can align on 6.25, 12.5 and 25kHz offset
- This allows seamless migration / co-existence with analog FM PMR in same band
- Uplink/Downlink spacing can depend on band, typically 10MHz
- Advanced TETRA-2 modes can operate at 50, 75 or 100kHz bandwidth

TETRA Modulation

- pi/4 DQPSK (Differential Quaternary Phase Shift Keying)
- 2 bits per symbol
- Phase *difference* encodes information
- 8 phase constellations, 4 possible transitions
- Requires very linear amplifier as it is not constant envelope
- Used within TETRA at 36 kbits/sec (18 kSymbols/sec)

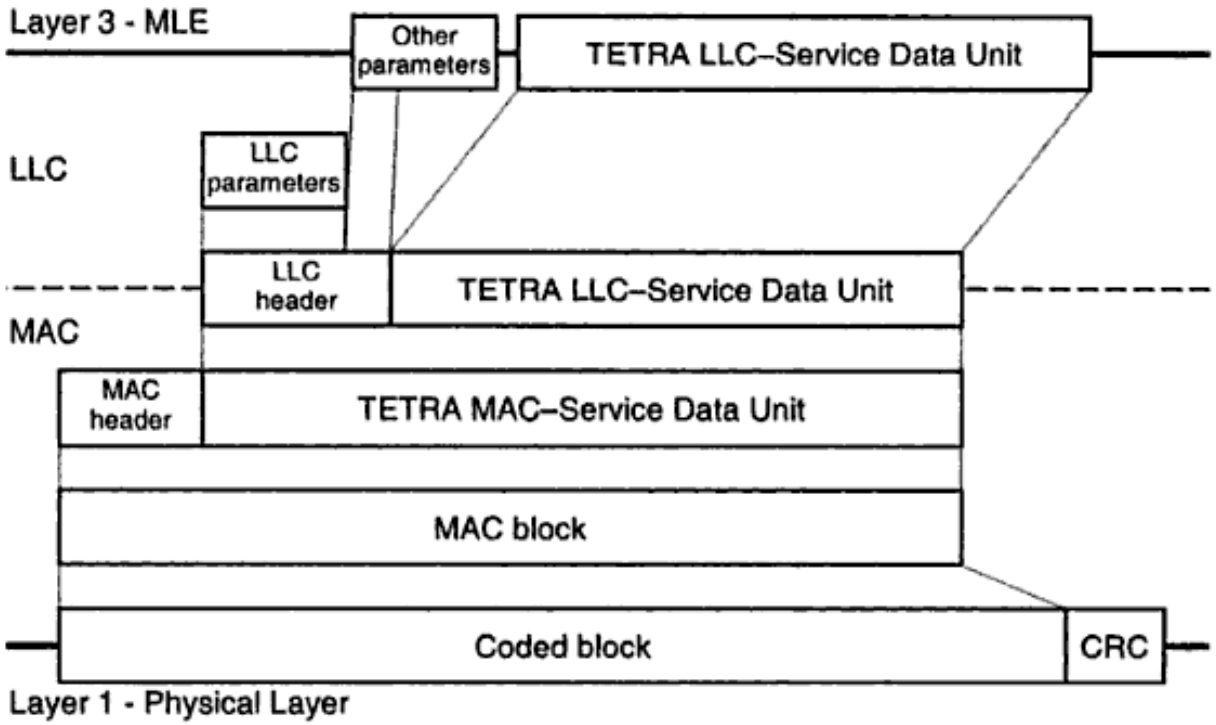
TETRA TDMA Frame structure

- Each time-slot contains 510 bits (GSM: 156)
- TDMA frame with 4 time-slots (GSM: 8)
- Duration of TDMA frame: 56.67 ms (GSM: FIXME)
- Multiframe: 18 TDMA frames (GSM: 26/51)
- Hyperframe: 60 Multiframes (GSM: FIXME)

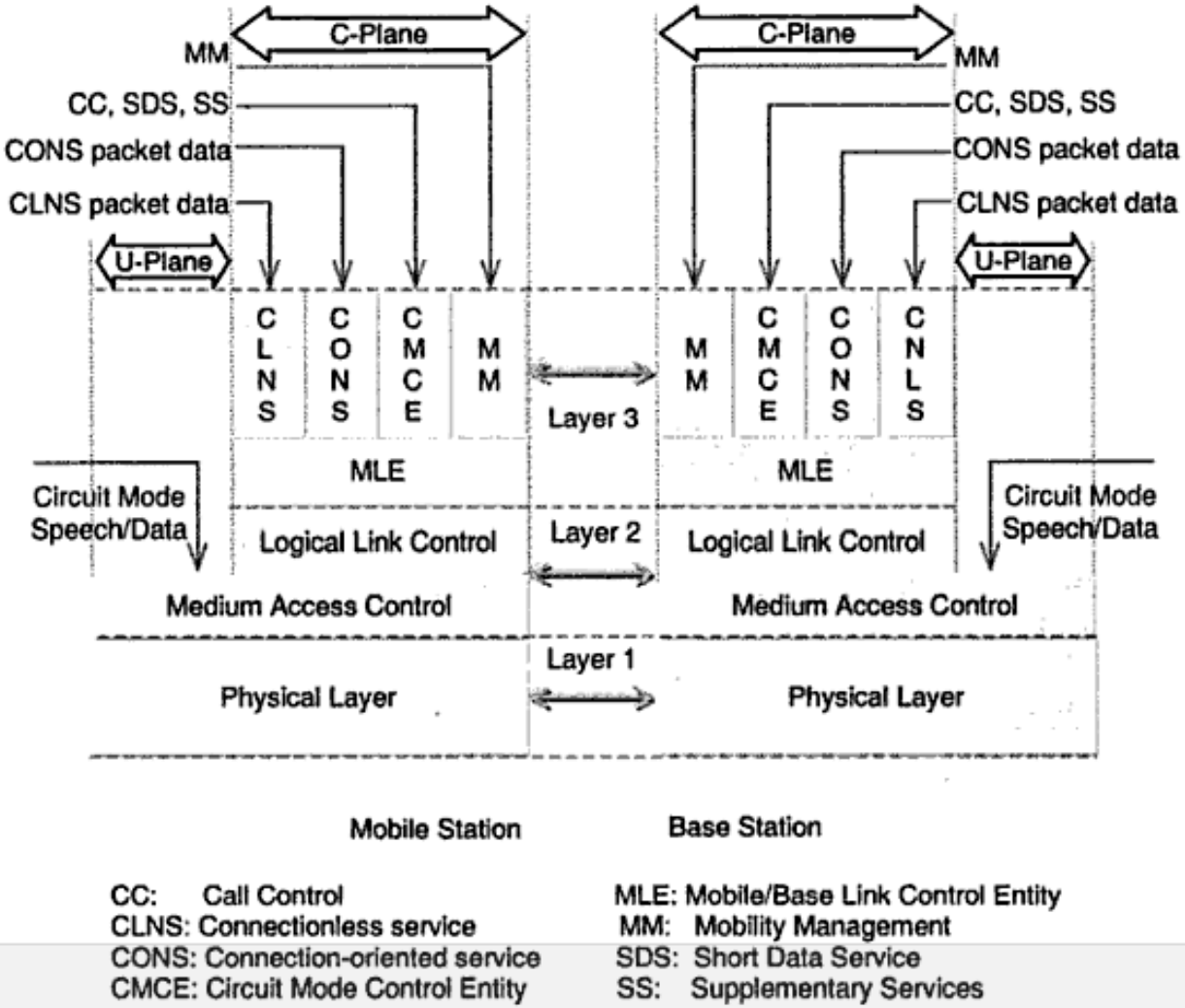
TETRA Protocol Stack

- The TETRA protocol stack is more complex than GSM
- Shared Stacking: PHY/lowerMAC/upperMAC/LLC
- Above LLC there is MLE (resembles GSM RR), on top:
  - MM (Mobility Management)
  - CMCE (Circuit Mode Control Entity)
  - CONS (Connection Oriented Service)
  - CNLS (Connectionless Service)
- Call Control, Supplementary services on top of CMCE
- Packet data on top of CNLS and CONS

TETRA Protocol Stack



TETRA Protocol Stack



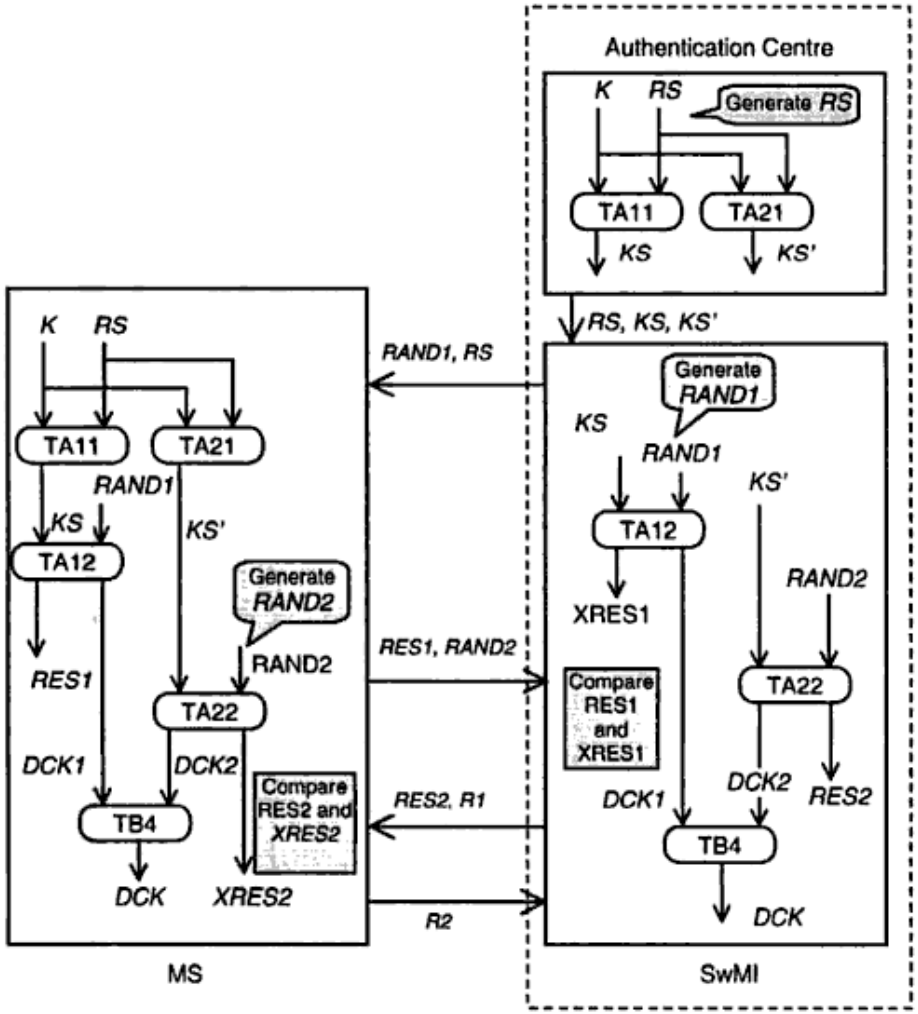
TETRA Security

- Once again all security features optional, like in GSM
- Security features include
  - Authentication
  - Air interface encryption
  - End-to-End encryption
  - Over-the-air re-keying (OTAR)
  - Remote locking of stolen devices
- Not all handsets support all features
- Key material can be stored in handset flash or in SIM

TETRA Authentication

- Authentication messages part of Mobility Management (MM)
- Based on secret User Authentication Key (UAK) in SIM, generating Authentication key K by use of Algorithms TB1, TB2 or TB3
- Supports three modes
  - Authentication of user by infrastructure (TA11, TA12)
  - Authentication of infrastructure by user (TA21, TA22)
  - Mutual authentication (four-pass, TA11, TA12, TA21, TA22)

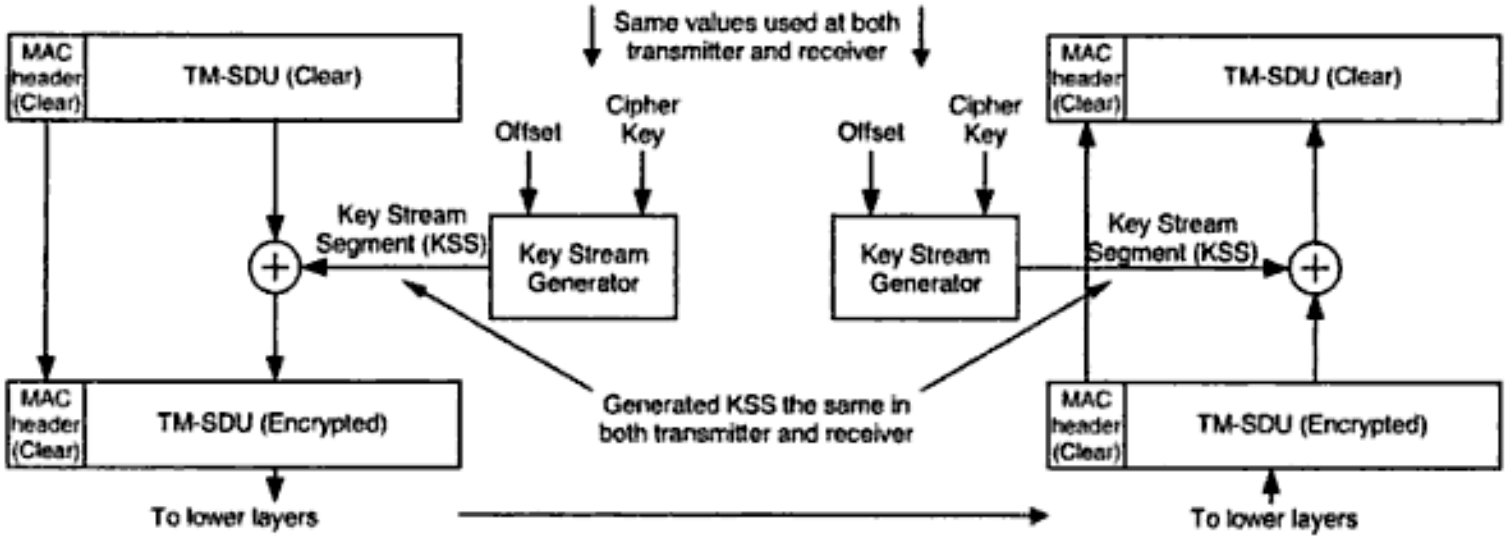
TETRA Authentication



TETRA Air Interface Encryption

- Like GSM: Encrypts only the air interface, not the core network
- Unlike GSM: Not between L1 and L0 but inside the upper MAC layer
  - Thus, no idle frames with known plaintext
  - Thus, no redundant information due to FEC before crypto
- Encryption happens with different keys (SCK, DCK, CCK, GCK, MGCK)
- IV is concatenation of hyperframe, multiframe, frame and slot number

TETRA Air Interface Encryption



TETRA Encryption Keys

- SCK (Static Cipher Key)
  - pre-shared key, used in networks without authentication
  - up to 32 possible keys, selected by SYSINFO.
- DCK (Derived Cipher Key)
  - Generated by authentication procedure (like GSM A3/A8)
  - different for each user
- CCK (Common Cipher Key)
  - Generated by infrastructure and distributed to MS through DCK-encrypted connection using OTAR
  - Used for group calls within one location area
- GCK (Group Cipher Key)
  - Generated by infrastructure and distributed to MS through DCK-encrypted connection using OTAR
  - Used for specific protected groups
- MGCK (Modified GCK)
  - GCK modified by CCK

TETRA Encryption Algorithms

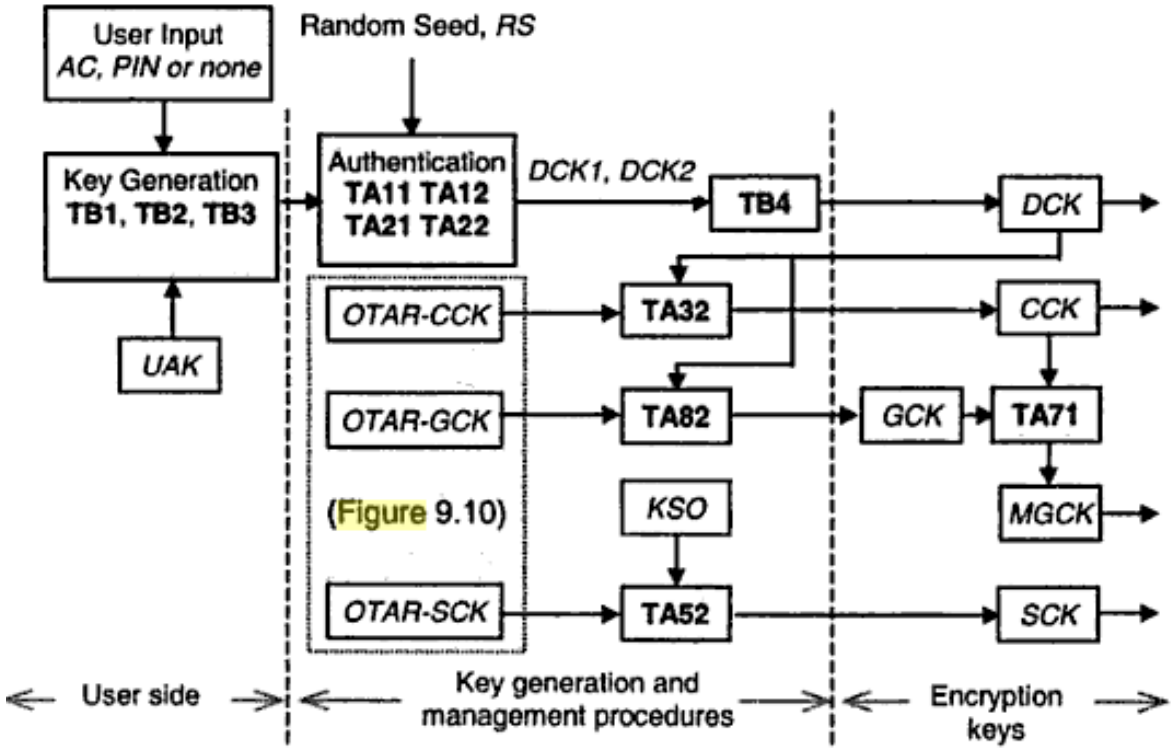
There are 4 specified TETRA Encryption Algorithms (TEA):

- TEA1 generally available, original algorithm, relaxed export
- TEA2 for public safety users in Schengen + EU countries
- TEA3 for public safety users elsewhere
- TEA4 generally available, reflects relaxed 1998 Wassenaar arrangement

It is assumed that at least original ciphers are 80-bit stream ciphers. None of them have ever leaked publicly!

TETRA Air Interface Encryption

Keys and Algorithms



OTAR-CCK	*CCK* sealed with *DCK* and received over the air interface
OTAR-GCK	*GCK* sealed with *DCK* and received over the air interface
OTAR-SCK	*SCK* sealed with *KSO* and received over the air interface
KSO	a session key for OTAR, derived from a key securely distributed to MSs.

Note: Algorithm names are shown in **bold**, e.g., **TB1, TA31, TA52,** etc.

Osmocom TETRA Demodulator

- 1:1 code re-use from APCO-25 Software receiver project
- Hierarchical block fully based on gnuradio blocks
  - Root-raised cosine filter
  - M-PSK receiver block
  - Costas Loop for carrier tracking
  - Muller&Muller synchronizer
  - output: Float value between -3 and 3 in units of pi/4

Osmocom TETRA PHY

The burst synchronizer (`tetra_burst_sync.c`)

- First acquires the Sync Burst training sequence by correlation
- Later locks on Normal Burst (NB) training sequences
- Splits actual payload sections out of training sequences,

The burst generator (`tetra_burst.c`)

- puts together various bursts such as NB, SB and others
- calculates phase alignment bits
- used to test receiver code

Osmocom TETRA lower MAC

Receive Side

- Receives bursts from PHY layer
- Applies the following operations depending on burst type
  - De-scrambling
  - De-Interleaving
  - De-Puncturing (RCPC code)
  - Viterbi decoder (RCPC code)
  - Compute + Verify CRC-16
- Recover TETRA Time (frame number) from SYNC burst
- Hands decoded payload data to upper MAC

Osmocom TETRA lower MAC

Transmit Side

- Receives payload from upper MAC
- Applies the following operations depending on burst type
  - Append tail bits
  - Compute CRC-16
  - Convolutional encoder (RCPC code)
  - Puncturing (RCPC code)
  - Interleaving
  - Scrambling
- Hands decoded payload data to PHY

Tx is currently only used in testing the Rx code

Osmocom TETRA upper MAC

- Rx-only
- Not a complete implementation, just to decode SYSINFO, ACCESS-ASSIGN and some other bits.
- Mainly a proof-of-concept to ensure PHY and lower MAC work

Osmocom TETRA via GSMTAP

- The GSMTAP pseudo-header has been extended for TETRA
- Change is backward-compatible with existing GSMTAP
- current version of libosmocore supports extended GSMTAP
- OsmocomTETRA `tetra-rx` contains GSMTAP output support

wireshark TETRA integration

- TETRA messages are unaligned bit-fields, full of variable-length and optional parts
- Writing manual decoding/encoding routines is tiresome and error-prone
- Beijing Institute of Technology has developed wireshark dissectors based on describing TETRA messages as ASN.1 PER (described in IEEE paper)
- We contacted them and they were willing to release their code under GNU GPL
- Zecke has extended it with GSMTAP support and is in the process of submitting it to wireshark mainline

Transmitting TETRA

- The lower MAC and PHY code exists and is proven
- OP25 project contains modulator for pi/4 DQPSK
- Combining the two should render simplistic TETRA transmitter
- Sending continuous sequence of BSCH in SB and BNCH in NB comprises valid beacon and should allow handsets to lock on the signal
- So far no time to experiment with it
- Could be first step in SDR TETRA Base Station

Thanks

Thanks to

- Dieter Spaar for discovering the APCO25 demodulator and his work on speech decoding
- Sylvain Munaut for implementing our own Viterbi decoder
- Holger Freyther for his work on CRC, Shortened Reed-Muller and wireshark
- horiz0n for providing sample captures of TETRA radio traffic

Further Reading

- http://tetra.osmocm.org/
- http://www.tetramou.com/
- http://www.etsi.org/website/Technologies/TETRA.aspx
- http://www.tetramou.com/uploadedFiles/About_TETRA/TETRA%20Security%20pdf.pdf
- http://www.tetrawatch.net/
- *Digital Mobile Communications and the TETRA System* by John Dunlop, Demessie Girma, James Irvine - Wiley