Introduction to TETRA
and its use in amateur radio

Jacek Lipkowski / SQ5BPF

Marcin Brzozowski / SP8MB

Who are we?

Marcin / SP8MB

- work for goverment
- TetraPack advocate in Poland
- interests: R&D of unmanned aerial vehicles, digital radio communication systems
- author of TetraLogger

Jacek / SQ5BPF

- licensed in 1993
  (30+ years!)
- making/breaking networks/unix stuff (25+ years)
- interested in all radio: digital, analog, microwave, VLF... everything really
- author of telive

Agenda

- What is TETRA?
- Can it be used in amateur radio?
- HAMTETRA project
- TETRA-LOGGER and TETRA-GPS
- Telive
- TETRA Security

What is TETRA?

- Terrestrial Trunked Radio
- ETSI “open standard”, many vendors
- Similar to 2G GSM
- Used for critical comms (goverment, commercial)

What is TETRA?

- DQPSK π/4 modulation
- 18k symbols/s, 2 bits per symbol, 36kbit/s
- 25kHz bandwidth (more for TEDS)
- Logically divided into 4 slots, 7.2kbit/s

What is TETRA?

TMO – trunked mode operation

TBS – Tetra base station

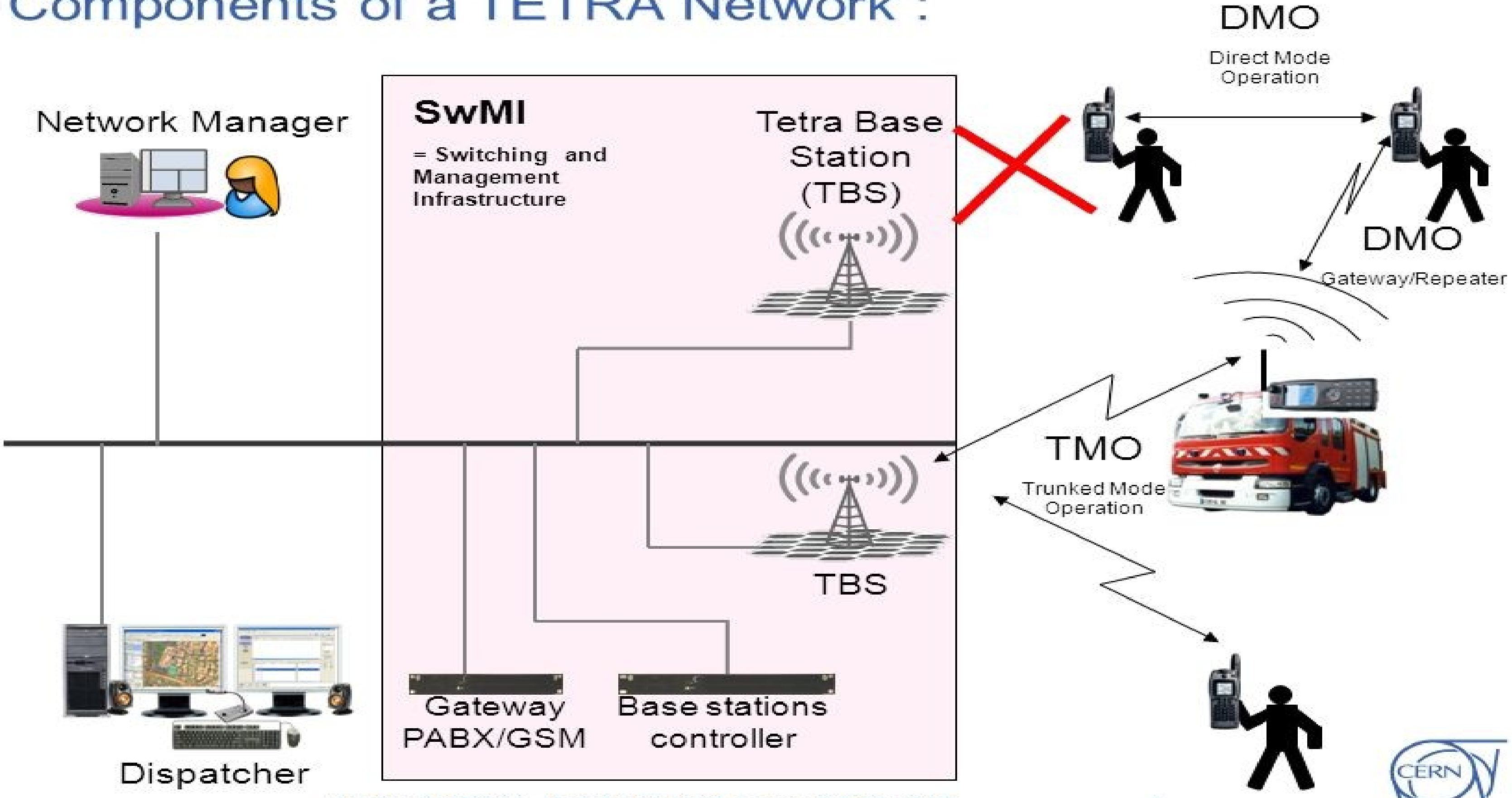
Radio can roam between base stations.

DMO – direct mode operation (radio to radio)

A radio can work as a repeater.

TETRA Infrastructure

Components of a TETRA Network :



What is TETRA?

ETSI “open standard”:

- Most of the protocol is extensively documented
- ACELP: Non-open codec (but source avaliable)
- Proprietary extensions to most things
- Crypto not documented

Not open, but a bit more open than DMR/P25/NXDN etc

TETRA services

- Network management stuff (roaming etc)
- Voice calls: individual (also full duplex), group
- Data transfer: circuit (like CSD), packet (like GPRS)
- Short 2 byte statuses
- Short messages: SDS (like SMS: text, binary)
- Lots of services over SDS: location, proprietary stuff

Can it be used for amateur radio?

- Complicated, but more open than DMR
- Equipment is avaliable
- Opportunity to play around with (old) enterprise stuff

- DMO is easy
- TMO is not :)

HAM TETRA

TETRAPACK

Marcin SP8MB

TetraPack.online

Supported TETRA TMO features

- Group calls
- Simplex and duplex individual calls
- Phone calls (**PBX**) - Ham Telephony - Asterisk
- Short text messaging (**SDS**) and geo-positioning (**LIP report**) - e.g. APRS
- Packet data access (**PD**) max 28.8 kbit, - e.g. WAP application, telemetry system,
- Group scanning at the network controller level, with a priority system,

Bridging with BrandMeister

- Group calls (any talk-group > 90 available across both networks)
- Bridging talk-groups with “classic” ham-radio technologies (D-STAR, System Fusion, etc.)
- Simplex individual calls and SMS bridging
- SMS services via APRS/MQTT/API
- Geo-positioning to APRS/MQTT/API

Bridging with FM-POLAND (svxlink)

- Group calls (TetraPack talk-group 20 = FM-POLAND talk-group 260802)
- services such as weather forecast, time information

TetraPack.online

Bridging with RadioID.net

- radio terminal authentication - Access to the radio layer is limited to active DMR IDs

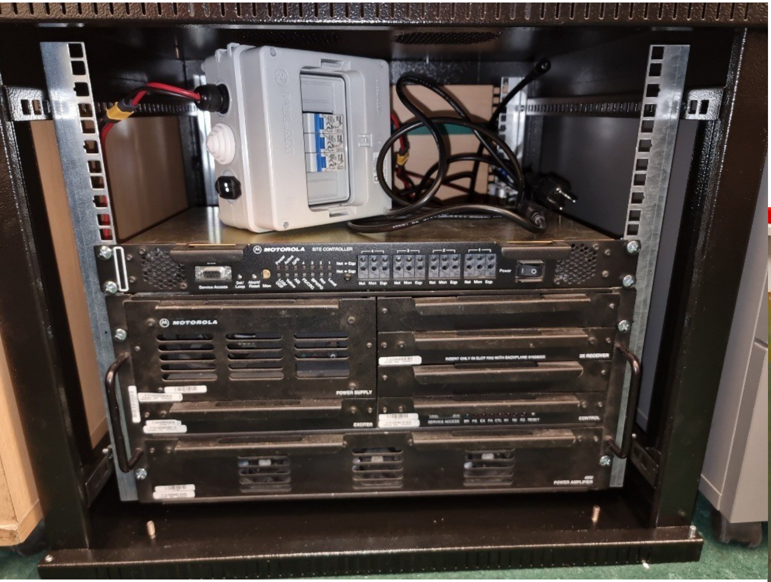
Supported radio-access technologies

- Motorola CompactTETRA (CTS)
- Motorola Dimetra (EBTS/MBTS/MTS) - Dimetra
- Rohill

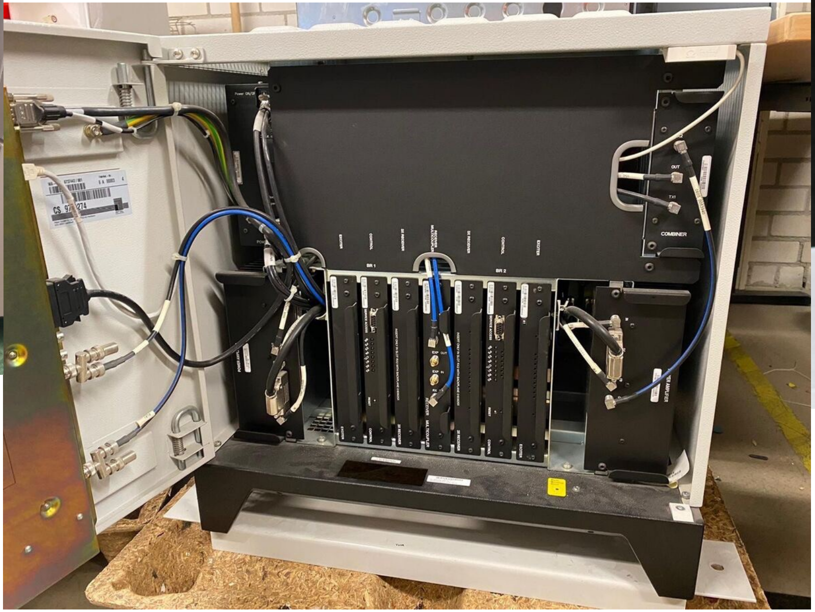
TetraPack base station in Poland (state on 05/08/2025):

- Świdnik/Lublin - Marcin SP8MB
- Olsztyn - Krzysztof M0LWO(SQ4LWO)
- Wrocław - Paweł SQ6POG / Przemek SQ6ODL
- Gdynia - Sebastian SP2FRN
- Biała Podlaska - Kamil SP8KB

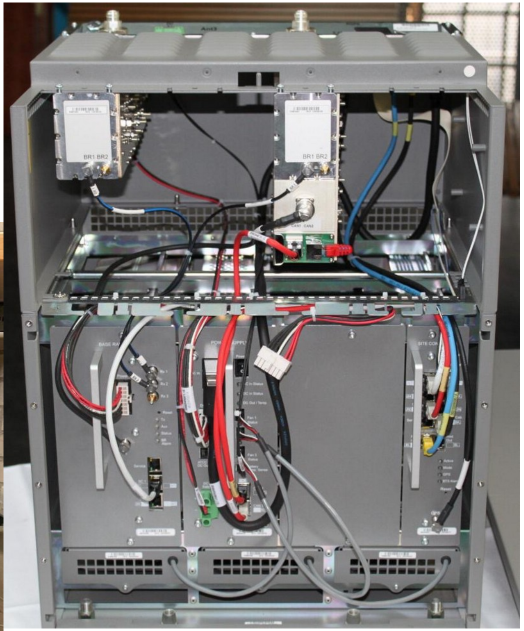
Motorola Dimetra Base Station



EBTS gen. 2



MBTS



MTS 2/4

TetraPack.online

Preferred radio equipment

- Motorola

  MTH, MTP, MXP, MTM, MXM series
- Hytera

  PT, PTC, MT series

Problematic radio equipment

- Sepura - not supported full HAM freq.
- Airbus/Cassidian - programing problem, not supported full HAM freq.
- Teltronic - not supported full HAM freq.
- Rohill - not supported full HAM freq.

TetraPack.online

https://tetrapack.online/

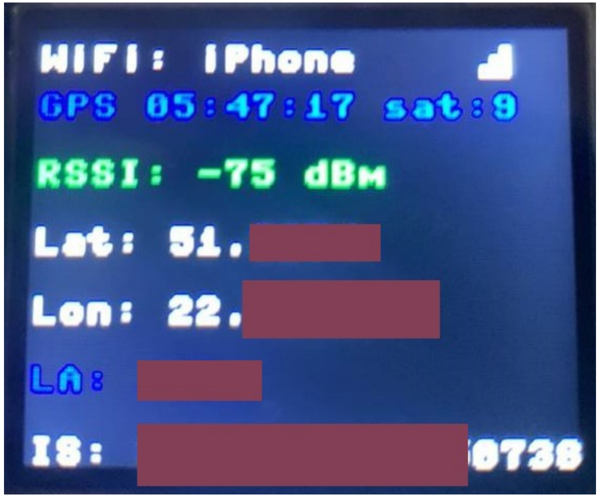
https://tetra-poland.pl

↓

TETRA-LOGGER

System dedicated to recording radio parameters of terminals in TETRA trunking systems.
Data on location and signal strength are an excellent source for estimating the range of base stations.

- built-in OLED screen for viewing current parameters,
- built-in Wi-Fi. Once connected to a Wi-Fi network (e.g., a phone hotspot), it sends data to the database,
- powered by a tetra terminal - it does not require an additional energy source.
- radio can still be used as usual
- the ability to run multiple loggers simultaneously and multiple accounts,
- work in the clear network, TEA1, TEA2, TEA3,
- built-in web based configurator (setup time interval, distance interval, wifi network parameters, database server parameters),
- data export to Excel,
- supported Motorola terminals, tested on: MTM5400, MTP3550, CM5000, MTH800



WIFI: iPhone
GPS 05:47:17 sat:9
RSSI: -75 dBm
Lat: 51.[redacted]
Lon: 22.[redacted]
LA: [redacted]
IS: [redacted]

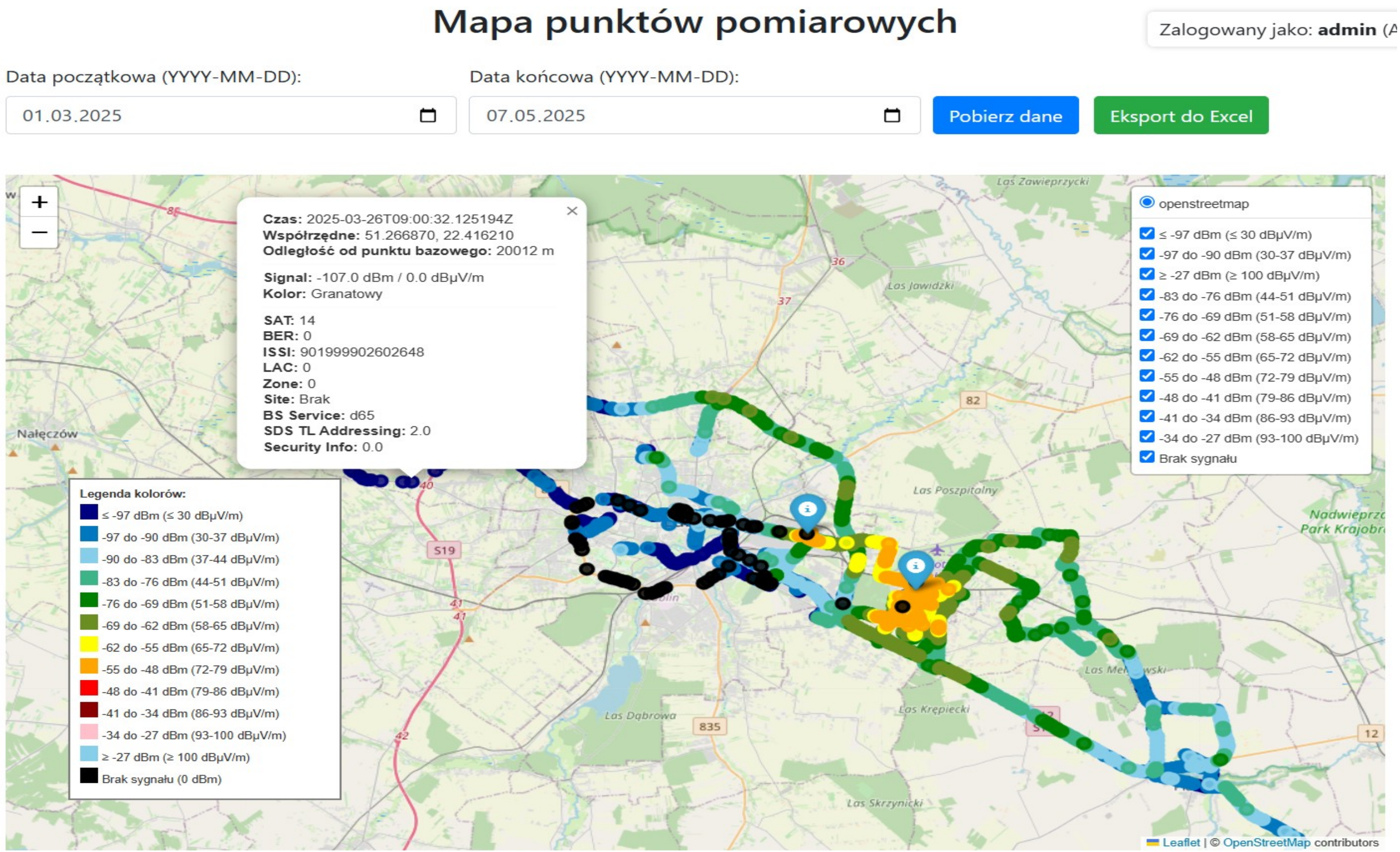
TETRA-LOGGER

Logger component:

- Small device connected to tetra terminal (powered from terminal),
- remote database,
- Web based system for visualizing data on a map and exporting data to Excel,

The device logs basic parameters vehicle and handheld terminals:

- date and time,
- ISSI - Individual Short Subscriber Identity,
- LAT, LON, SAT - latitude, longitude and number of satellites in view,
- LAC, LA - cell info (zone i site),
- SIGNAL - received signal in dBm,
- Security info - information about the type of network security,
- BS Service,
- SDS TL Addressing *,
- BER - bit error rate *,



Mapa punktów pomiarowych

Zalogowany jako: **admin** (A

Data początkowa (YYYY-MM-DD): 01.03.2025

Data końcowa (YYYY-MM-DD): 07.05.2025

Pobierz dane

Eksport do Excel

Czas: 2025-03-26T09:00:32.125194Z
Współrzędne: 51.266870, 22.416210
Odległość od punktu bazowego: 20012 m

Signal: -107.0 dBm / 0.0 dBµV/m
Kolor: Granatowy

SAT: 14
BER: 0
ISSI: 901999902602648
LAC: 0
Zone: 0
Site: Brak
BS Service: d65
SDS TL Addressing: 2.0
Security Info: 0.0

● openstreetmap
- ☑ ≤ -97 dBm (≤ 30 dBµV/m)
- ☑ -97 do -90 dBm (30-37 dBµV/m)
- ☑ ≥ -27 dBm (≥ 100 dBµV/m)
- ☑ -83 do -76 dBm (44-51 dBµV/m)
- ☑ -76 do -69 dBm (51-58 dBµV/m)
- ☑ -69 do -62 dBm (58-65 dBµV/m)
- ☑ -62 do -55 dBm (65-72 dBµV/m)
- ☑ -55 do -48 dBm (72-79 dBµV/m)
- ☑ -48 do -41 dBm (79-86 dBµV/m)
- ☑ -41 do -34 dBm (86-93 dBµV/m)
- ☑ -34 do -27 dBm (93-100 dBµV/m)
- ☑ Brak sygnału

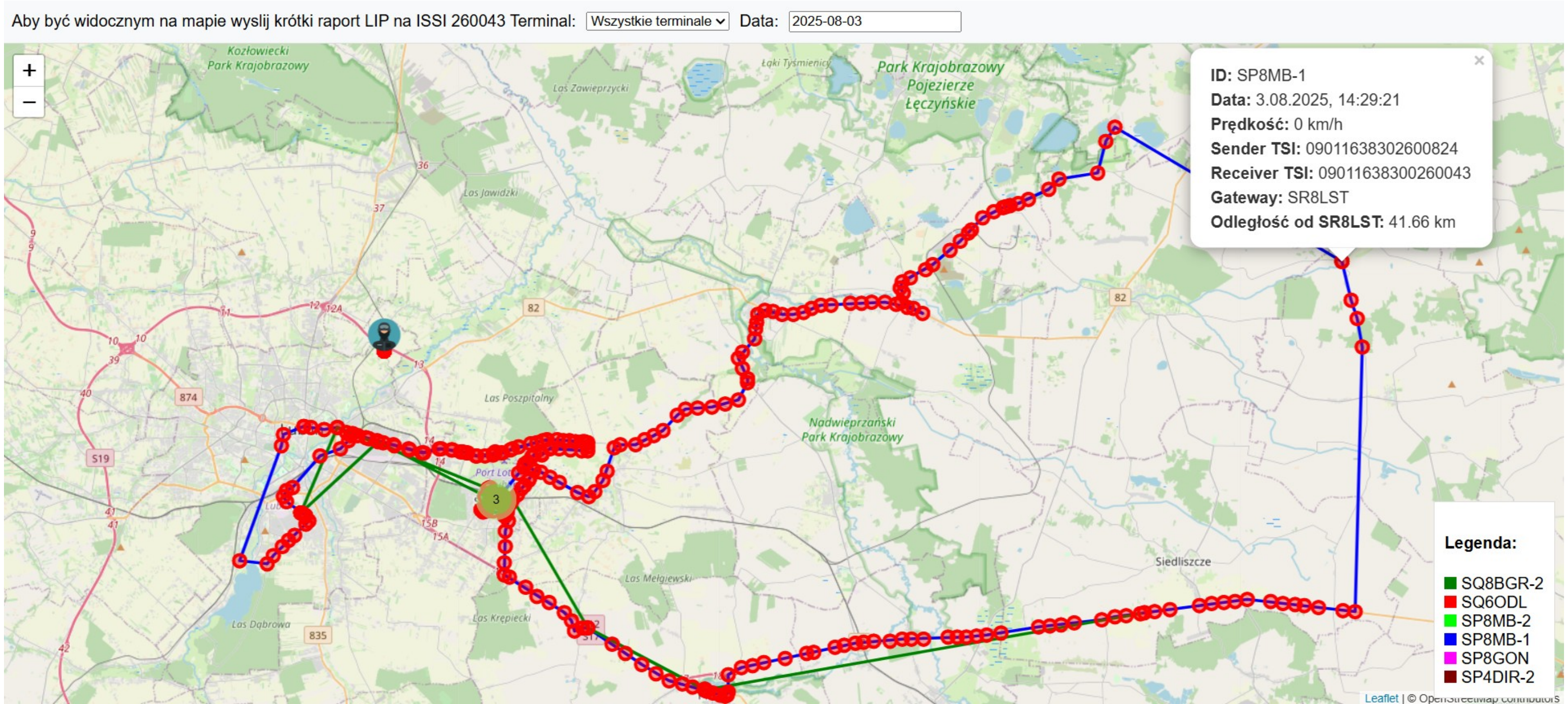
Legenda kolorów:
- ■ ≤ -97 dBm (≤ 30 dBµV/m)
- ■ -97 do -90 dBm (30-37 dBµV/m)
- ■ -90 do -83 dBm (37-44 dBµV/m)
- ■ -83 do -76 dBm (44-51 dBµV/m)
- ■ -76 do -69 dBm (51-58 dBµV/m)
- ■ -69 do -62 dBm (58-65 dBµV/m)
- ■ -62 do -55 dBm (65-72 dBµV/m)
- ■ -55 do -48 dBm (72-79 dBµV/m)
- ■ -48 do -41 dBm (79-86 dBµV/m)
- ■ -41 do -34 dBm (86-93 dBµV/m)
- ■ -34 do -27 dBm (93-100 dBµV/m)
- ■ ≥ -27 dBm (≥ 100 dBµV/m)
- ■ Brak sygnału (0 dBm)

Leaflet | © OpenStreetMap contributors

TETRA-GPS

System for remotely logging and visualization the position of terminals in tetra network.

- web interface for visualizing real time location data with multi-user login,
- dedicated terminal for receiving data from other tetra terminals,
- ability to search historical data by terminals, dates, etc.
- compatible with most hardware manufacturers



Aby być widocznym na mapie wyslij krótki raport LIP na ISSI 260043 Terminal: Wszystkie terminale Data: 2025-08-03

ID: SP8MB-1
Data: 3.08.2025, 14:29:21
Prędkość: 0 km/h
Sender TSI: 09011638302600824
Receiver TSI: 09011638300260043
Gateway: SR8LST
Odległość od SR8LST: 41.66 km

Legenda:

- 🟩 SQ8BGR-2
- 🟥 SQ6ODL
- 🟩 SP8MB-2
- 🟦 SP8MB-1
- 🟪 SP8GON
- 🟫 SP4DIR-2

+
−
Kozłowiecki Park Krajobrazowy
Las Zawieprzycki
Łąki Tyśmienicy
Park Krajobrazowy Pojezierze Łęczyńskie
Las Jawidzki
Las Poszpitalny
Nadwieprzański Park Krajobrazowy
Port Lot
Siedliszcze
Las Melgiewski
Las Krępiecki
Las Dąbrowa
3
82
874
S19
835
Leaflet | © OpenStreetMap contributors

TELIVE

Tetra live monitor

TETRA

Jacek Lipkowski   SQ5BPF

OSMO-TETRA

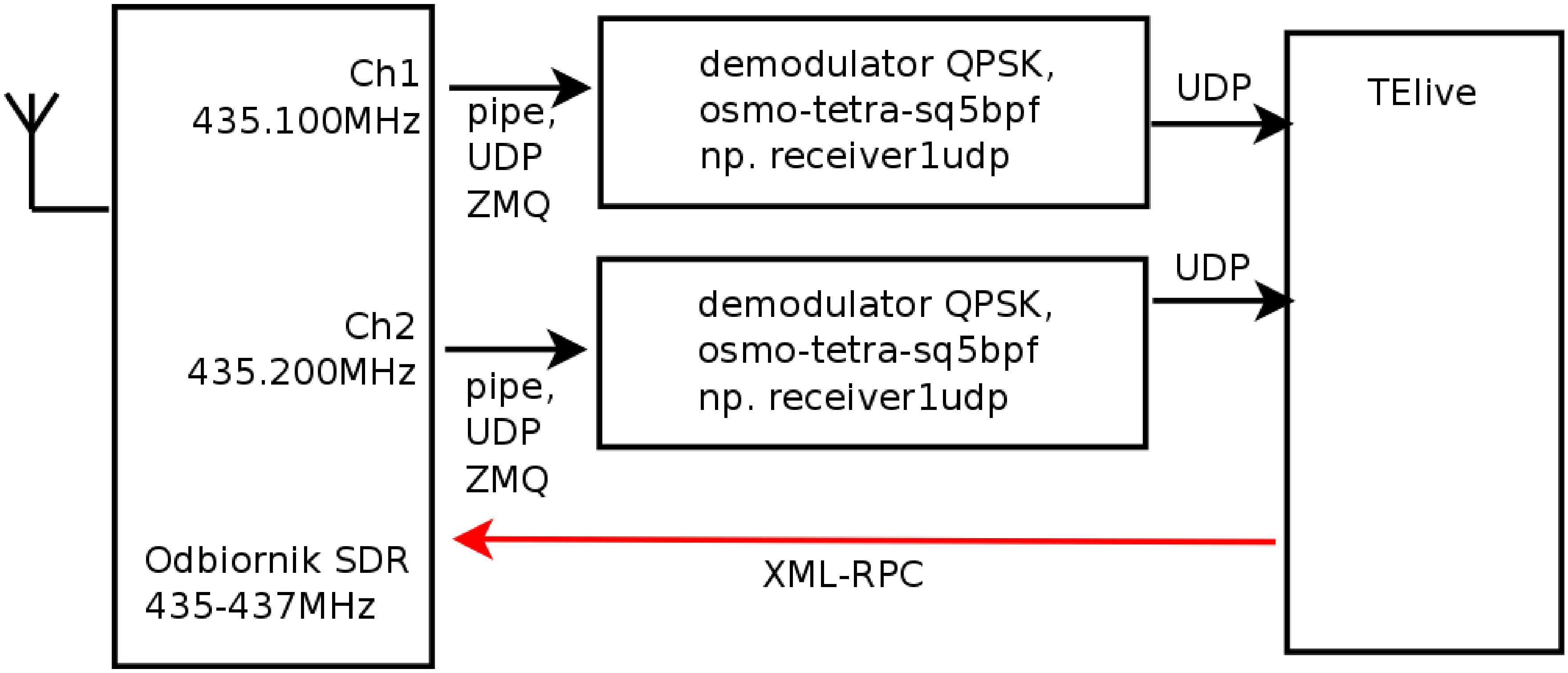
http://osmocom.org/projects/tetra/wiki/OsmocomTETRA

- Published by Osmocom in 2010
- Full implementation of the lower layers of the TETRA protocols
- Decodes some signalling information

- Decoded enough to program a radio
- Turns out most traffic was unencrypted

Telive – TETRA live monitor

- Chopped osmo-tetra into blocks: SDR receiver implemented in gnuradio-companinon, separate DQPSK demodulator, osmo-tetra-sq5bpf
- osmo-tetra-sq5bpf: implemented a lot of signalling, SDS, fragmentation etc
- osmo-tetra-sq5bpf sends signalling and voice data via a simple UDP based protocol
- Telive receives this UDP, merges call and signalling data
- Modular design: blocks are easy to modify and replace


Ch1
435.100MHz
pipe,
UDP
ZMQ
demodulator QPSK,
osmo-tetra-sq5bpf
np. receiver1udp
UDP
TElive
Ch2
435.200MHz
pipe,
UDP
ZMQ
demodulator QPSK,
osmo-tetra-sq5bpf
np. receiver1udp
UDP
XML-RPC
Odbiornik SDR
435-437MHz

Telive – following a voice call

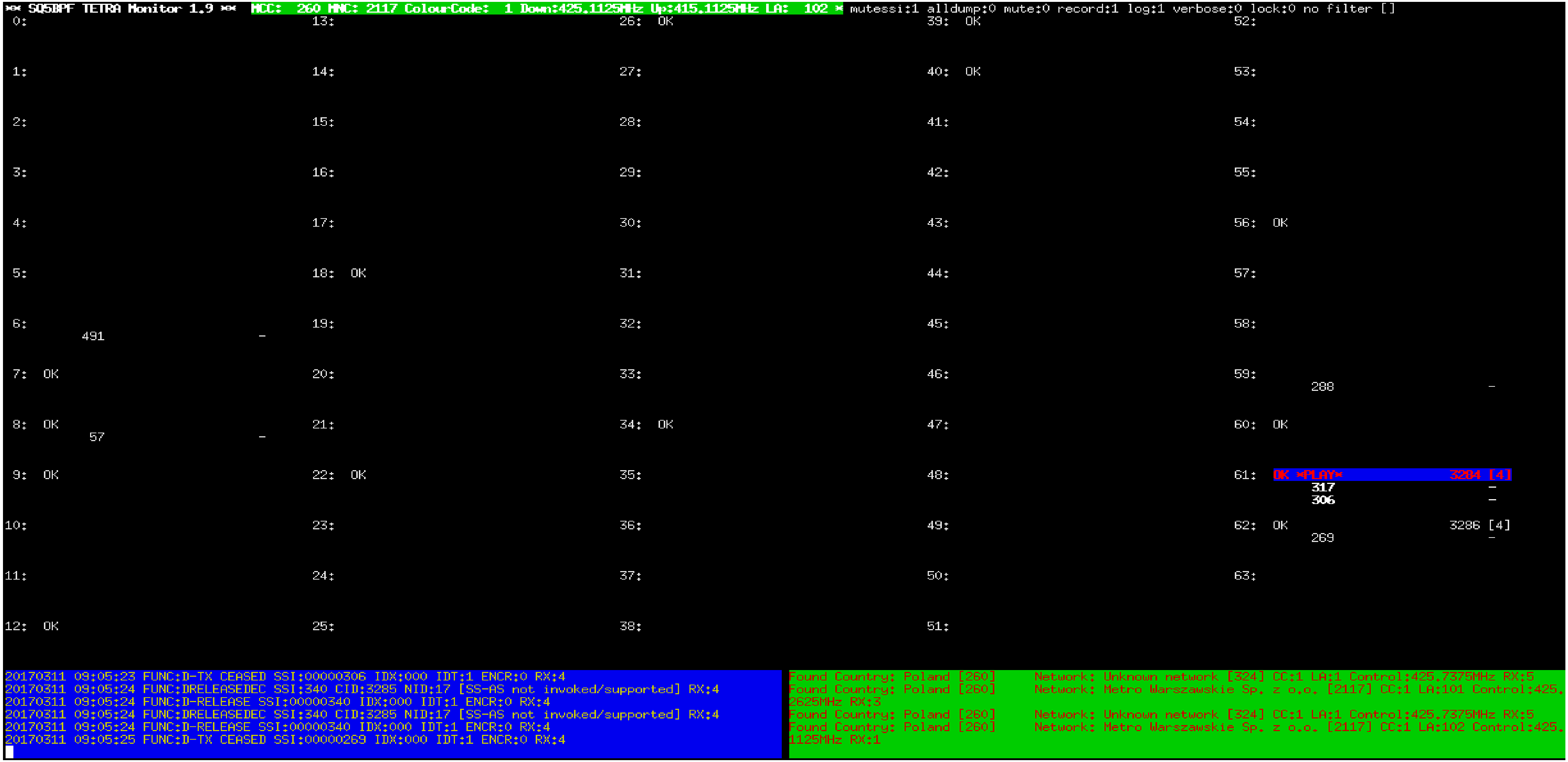
- Voice traffic has a „traffic usage marker”
- D-SETUP: info about SSI, „Call Identifier” and „traffic usage marker”
- D-CONNECT: info about SSI and „traffic usage marker”
- D-TXGRANTED: info about „Call identifier” and SSI etc...
- We can use this to group individual traffic usage markers into calls, and see which SSIs participate in them

Telive

- Plays one active voice call
- Can record all ongoing calls at once (with SSIs in file name)
- Logs signalling to a file
- Old recordings compressed to OGG
- Can handle multiple radio channels at once
- Dump location information to a KML file
- Autodiscovery of network info (additional frequencies etc)
- Can control the receiver via XML-RPC (clock drift compensation, tuning additional channels, scanning etc)

- Released December 2014

https://github.com/filipsPL/signals/tree/master/ground/TETRA



```
** SQ5BPF TETRA Monitor 1.9 **  MCC:  260 MNC: 2117 ColourCode:  1 Down:425.1125MHz Up:415.1125MHz LA:  102 * mutessi:1 alldump:0 mute:0 record:1 log:1 verbose:0 lock:0 no filter []
 0:                                     13:                                     26:  OK                                 39:  OK                                 52:

 1:                                     14:                                     27:                                     40:  OK                                 53:

 2:                                     15:                                     28:                                     41:                                     54:

 3:                                     16:                                     29:                                     42:                                     55:

 4:                                     17:                                     30:                                     43:                                     56:  OK

 5:                                     18:  OK                                 31:                                     44:                                     57:

 6:                                     19:                                     32:                                     45:                                     58:
          491                       -
 7:  OK                                 20:                                     33:                                     46:                                     59:
                                                                                                                                                                                   288                    -
 8:  OK                                 21:                                     34:  OK                                 47:                                     60:  OK
           57                       -
 9:  OK                                 22:  OK                                 35:                                     48:                                     61:  OK *PLAY*                 3284 [4]
                                                                                                                                                                                   317                    -
                                                                                                                                                                                   306                    -
10:                                     23:                                     36:                                     49:                                     62:  OK                         3286 [4]
                                                                                                                                                                                   269                    -
11:                                     24:                                     37:                                     50:                                     63:

12:  OK                                 25:                                     38:                                     51:
```

```
20170311 09:05:23 FUNC:D-TX CEASED SSI:00000306 IDX:000 IDT:1 ENCR:0 RX:4
20170311 09:05:24 FUNC:DRELEASEDEC SSI:340 CID:3285 NID:17 [SS-AS not invoked/supported] RX:4
20170311 09:05:24 FUNC:D-RELEASE SSI:00000340 IDX:000 IDT:1 ENCR:0 RX:4
20170311 09:05:24 FUNC:DRELEASEDEC SSI:340 CID:3285 NID:17 [SS-AS not invoked/supported] RX:4
20170311 09:05:24 FUNC:D-RELEASE SSI:00000340 IDX:000 IDT:1 ENCR:0 RX:4
20170311 09:05:25 FUNC:D-TX CEASED SSI:00000269 IDX:000 IDT:1 ENCR:0 RX:4
```

```
Found Country: Poland [260]      Network: Unknown network [324] CC:1 LA:1 Control:425.7375MHz RX:5
Found Country: Poland [260]      Network: Metro Warszawskie Sp. z o.o. [2117] CC:1 LA:101 Control:425.
2625MHz RX:3
Found Country: Poland [260]      Network: Unknown network [324] CC:1 LA:1 Control:425.7375MHz RX:5
Found Country: Poland [260]      Network: Metro Warszawskie Sp. z o.o. [2117] CC:1 LA:102 Control:425.
1125MHz RX:1
```

Tetra Security

Jacek Lipkowski SQ5BPF

Early TETRA security

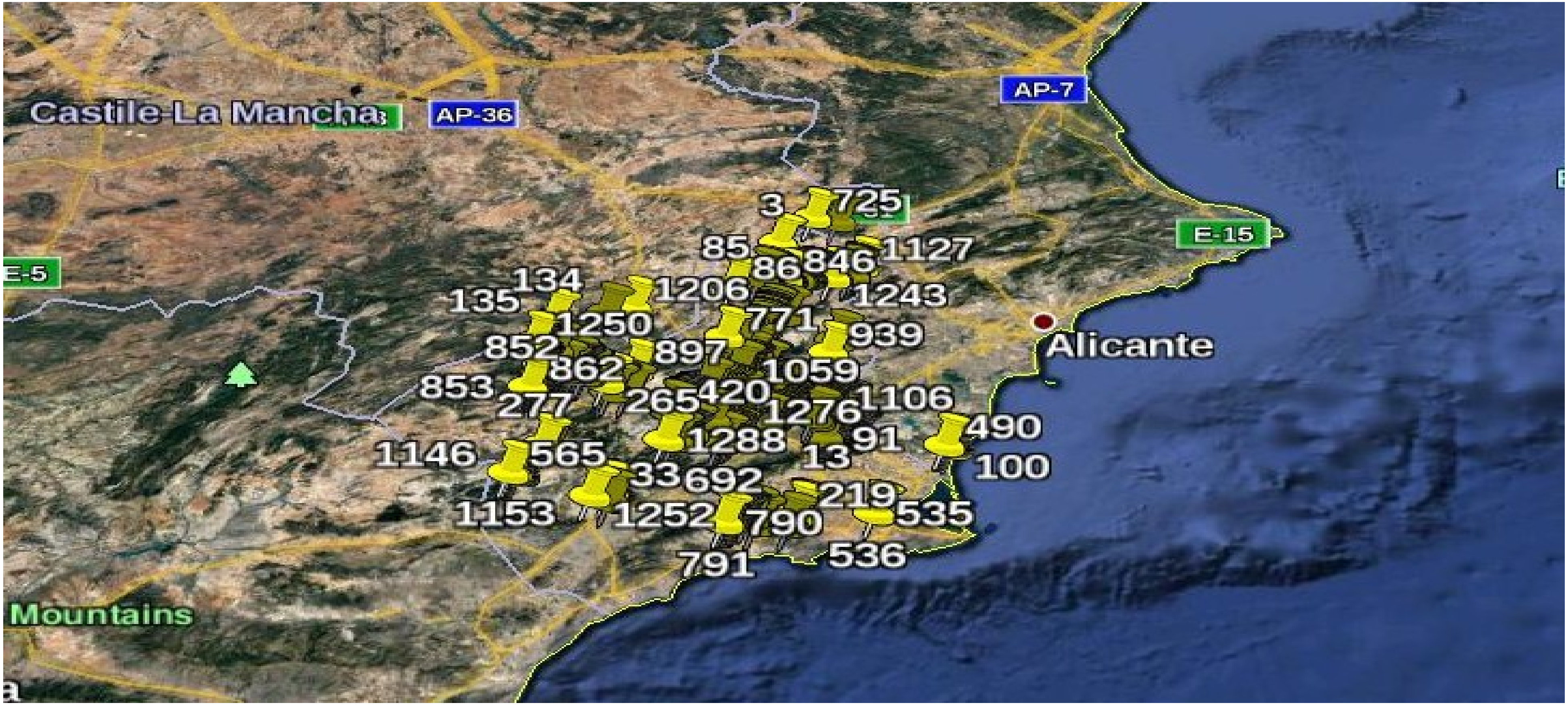
- Complicated/expensive radio system
- Encryption is an additional expense
- Monitoring it would need a special receiver
- Special receiver not (widely) avaliable (before telive)
- So no need for encryption. Problem solved :)

https://forums.radioreference.com/voice-control-channel-decoding-software/302347-tetra-decoding-48.html

Excellent work SQ5BPF. I'd like to know more about the capabilities of the software. Am I just decoding Tetra or is this also decrypting/decoding the so called TEA 1 ?

The reason I'm asking is because I'm able to listen in on my own traffic, which I was told by the provider was secure. Obviously they're relying on security through obscurity and so I'm not getting any definitive answers on the security provided to me, and the answers I get I don't trust. So I look to you.

Telive log found on pastebin. Used to try to understand Simple location system type 0x80
Allegedly this is some police/goverment force in Spain :)



TETRA crypto

Non-public proprietary crypto, authored by SAGE (Security Algorithms Group of Experts) in the 1990s (export restrictions etc)

- TEA1 – exportable, ETSI
- TEA2 – goverment services in Schengen area, Dutch Police
- TEA3 – goverment services in countries not eligible for TEA2, ETSI
- TEA4 – if TEA1 seems fishy you can use this one, ETSI

TAA1 – key management/distribution

Recently TAA2/TEA5-TEA7 released, with public specs

TETRA crypto

"The standard TETRA Encryption Algorithms TEA1, TEA3 and TEA4 can be obtained under a 'Non disclosure and restricted usage licence' from ETSI. This undertaking requires, among other things, that the algorithms are implemented in such a way that it is difficult to recover their design from the implementation."

GSM A5/1: created 1989, leak 1994, full rev. 1999

But surely this will be different than with other non peer-reviewed proprietary crypto right?

TETRA:BURST July 2023

TEA1-3 reversed (after 28 years) by MidnightBlue

TEA1 deliberately weakened from 80 bits to 32 bits (easlily bruteforced)

TEA3 s-boxes considered suspicious, requires futher work

AIE (encryption of data over the air) has no integrity protection (only CRC)

Keystream recovery attacks possible

etc...

https://www.midnightblue.nl/research/tetraburst

https://media.ccc.de/v/37c3-11761-all_cops_are_broadcasting

Can glue mend the burst? December 2024

Commentary of ETSI reply to TETRA:BURST by MidnightBlue on CCC congress

Algorithm specs published (including TEA4, not in TETRA:BURST).

TEA4 deliberately weakened from 56 bits (weak but better than TEA1)

TEA7 weakened to 56 bits (with possible speedups)

https://media.ccc.de/v/38c3-tetra-algorithm-set-b-can-glue-mend-the-burst

After TETRA:BURST

Users are encouraged to use E2EE

E2EE – end to end encryption

Expensive

Not readily avaliable

Also proprietary crypto. What could possibly go wrong :)

2TETRA:2BURST August 2025

E2EE reverse engineered by Midnight Blue

E2EE algorithm 135 is AES128 but weakened to 56 bits

E2EE has no replay protection. Attacker can inject old messages (SDS, voice streams etc)

Also (not E2EE related):

Keys are same for all algorithms, recover TEA1 key, use for TEA2

ETSI fix for TETRA:BURST keystream recovery attack is ineffective

etc...

https://www.midnightblue.nl/research/2tetra2burst

https://media.ccc.de/v/why2025-194-the-why-the-how-the-what-an-assessment-of-tetra-end-to-end

Summary

https://github.com/sq5bpf/misc

VY 73

Marcin / SP8MB sp8mb@swidnik.net

Jacek / SQ5BPF sq5bpf@lipkowski.org

Notes added after M17 conference

Wojtek SP5WWP and I were able to get TETRA audio decoding working on the LinHT from the M17 team. Took abt 1h. Shows that this is great hardware, congrats to the LinHT team!

Please contrast the info in this talk with M17:

- In M17 everything is open (incl. audio codec). And you can change it if you want (or suggest changes), even suggest changes to the specification itself
- Source for everything is avaliable and can be audited (incl. crypto)
- Hardware is also open. And you can port M17 to your own hardware too
- Currently crypto is not a priority for HAMs (integrity protection might be), but for professional use you could make sure it fits your use case exactly (known good algorithms, number of key bits, integrity protection, no intentional weakening and backdoors, integration with key servers etc)
- Currently no “professional” radio system allows this (and unlikely it will)

Questions?

VY 73

Marcin / SP8MB sp8mb@swidnik.net

Jacek / SQ5BPF sq5bpf@lipkowski.org