WTH 2018

Monitorowanie systemu TETRA za pomocą TELIVE

Jacek Lipkowski SQ5BPF

~$ whoami

- Jacek Lipkowski

  Hobby:
- Krótkofalarstwo. Znak SQ5BPF (od 25 lat!)
- Unixy, sieci. I ich psucie :) (od ponad 20 lat)
- Elektronika (od zawsze)

  Pracuje w Pekao Financial Services Sp. z o.o.

  Prezentacja ta jest moja i nie wyraża poglądów pracodawcy.

TETRA

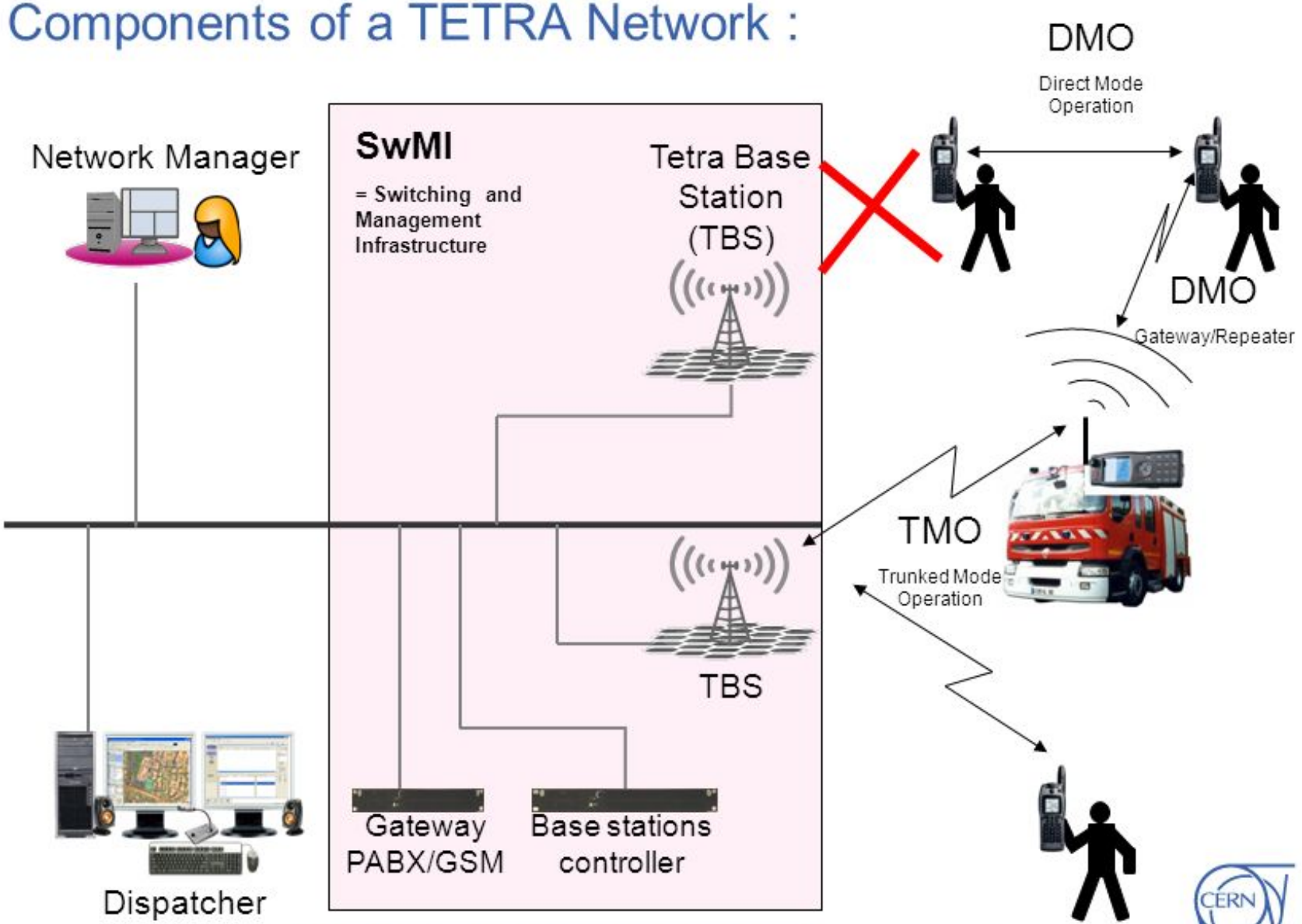
- Terrestrial Trunked Radio
- „Otwarty standard” ETSI, wielu producentów
- Podobny do GSM
- Do komunikacji krytycznej (służby, firmy)
- Nowoczesny i modny. Na każdej konferencji :)

TETRA

- Stacje bazowe, roaming pomiędzy nimi
- Połączenia głosowe, indywidualne, grupowe
- Transmisja danych połączeniowa i pakietowa
- Krótkie komunikaty: 2 bajty
- Krótkie wiadomości SDS (jak SMS)
- Inne ciekawostki :)
- Oprócz trybu TMO jest też DMO (radio do radia)

TETRA Infrastructure

Components of a TETRA Network :



CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

TETRA crypto

Niejawne algorytmy kryptograficzne, autorstwa SAGE (Security Algorithms Group of Experts)

- TEA1 – eksportowalny, ETSI
- TEA2 – tylko służby w Schengen, Policja Holenderska
- TEA3 – służby które nie dostaną TEA2, ETSI
- TEA4 – eksportowalny, ETSI

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."

:)

A5/1: powstał 1989, przeciek 1994, full rev. 1999

TETRA Radio

TDMA, Kanał 25kHz, QPSK. 4 rozmowy/kanał

Downlink (uplink: -10MHz):

- 390-395 MHz (służby)
- 420-430 MHz (służby i podmioty komercyjne)
- 450-470 MHz
- 870-876 MHz , 915-921 MHz

TETRA

- Skomplikowany system radiowy
- Szyfrowanie jest drogie
- Nasłuchiwanie wymaga specjalnego odbiornika, oprogramowania
- Czyli się nie da. Problem rozwiązany :)

W-Code Wavecom Elektronik GMBH

Motorola Scout

Sieci w Polsce

- 2101 MSWiA
- 2102 Miejskie Przedsiębiorstwo Komunikacyjne Sp. z o.o. (Wrocław)
- 2103 Przedsiębiorstwo Państwowe PORTY LOTNICZE
- 2104 Gdynia Container Terminal S.A.
- 2105 DCT Gdańsk S.A.
- 2106 Autostrada Eksploatacja S.A.
- 2107 Miejskie Przedsiębiorstwo Komunikacyjne S. A. (Kraków)
- 2108 ENERGA - OPERATOR S.A.
- 2109 Polski Koncern Naftowy ORLEN S.A.
- 2110 BCT - Bałtycki Terminal Kontenerowy Sp. z o.o.
- 2111 PGE Górnictwo i Energetyka Konwencjonalna S.A.
- 2112 Port Lotniczy Rzeszów-Jasionka Sp. z o.o.
- 2113 Port Lotniczy Gdańsk Sp. z o.o.
- 2114 Mazowiecki Port Lotniczy Warszawa-Modlin Sp. z o.o.
- 2115 Polski Koncern Naftowy ORLEN S.A.
- 2116 Port Lotniczy Gdynia-Kosakowo Sp. z o.o.
- 2117 Metro Warszawskie Sp. z o.o.
- 2118 Polskie LNG S.A.
- 2120 Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej

http://www.archiwum.uke.gov.pl/tablice/KodMnc-list.do

Nasłuch w Polsce

- Nie wymaga pozwolenia używanie urządzeń radiowych przeznaczonych wyłącznie do odbioru. Art 144 pkt 1 Pr. Telekomunikacyjne

- Art. 267

  § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

  § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

  § 3.Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

  § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

  § 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Nasłuch

- Każdy system telekomunikacyjny można nasłuchiwać jeśli znamy parametry (od kolegi :)

- Łamie art 144 i art 267.

SDR :)

- Sytuacja się zmieniła. Bajecznie tanie SDR z odbiornika DVB-T
- 24-1700MHz (dla tunera R820T)
- max około 2.5MHz pasma, ADC 8-bitowy
- 60zł !!!
-

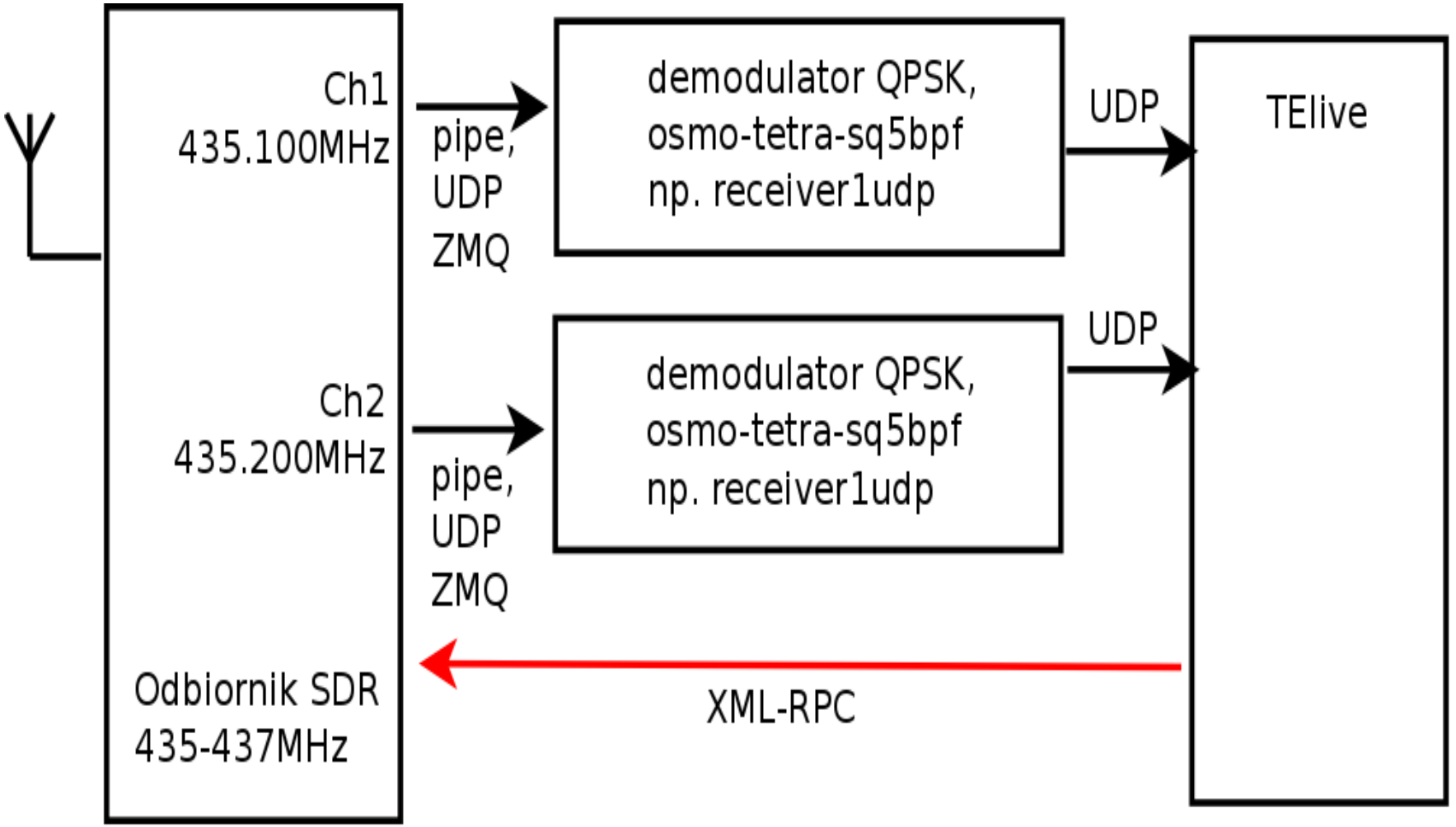
OSMO-TETRA

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

- Publikacja w 2010 roku
- Pełna implementacja niższych warstw
- Dekoduje troche sygnalizacji
- Okazuje się że prawie nie ma szyfrowania
- Wystarczy aby poznać parametry sieci i zaprogramować swoje radio (łamie Art 144 i 267)
- Był patch aby zrzucać głos do pliku

Telive – TETRA live monitor

- Rozdzielenie na odbiornik w gnuradio-companinon, osobny demodulator, osmo-tetra-sq5bpf
- Osmo-tetra-sq5bpf: dopisana obsługa części sygnalizacji
- Interfejs ad-hoc: osmo-tetra-sq5bpf wysyła głos i sygnalizację po UDP
- TElive odbiera UDP, składa sygnalizację z głosem
- Budowa modułowa, każdy składa sobie odbiornik z gotowych bloków (które łatwo jest modyfikować)


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

Telive – śledzenie sygnalizacji

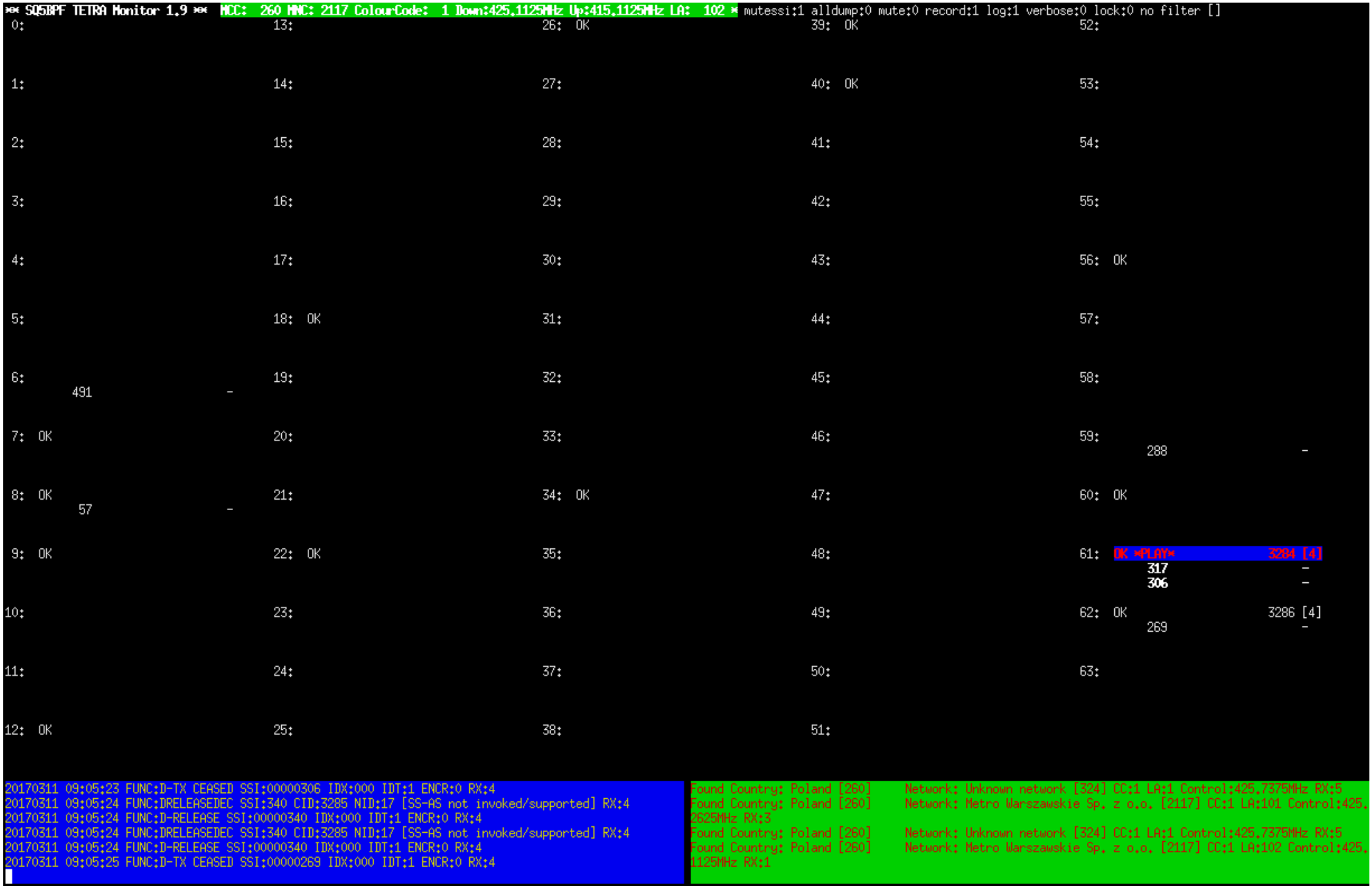
- Głos związany z „traffic usage marker”
- D-SETUP: informacje o SSI, „Call Identifier” i „traffic usage marker”
- D-CONNECT: ma informację o SSI i „traffic usage marker”
- D-TXGRANTED: ma informację o „Call identifier” i SSI itd...
- Znamy mapowanie SSI do głosu

TElive

- Odtwarza jedną aktywną rozmowę
- Nagrywa wszystkie (w nazwie daje SSI)
- Logowanie sygnalizacji do pliku
- Skrypt tetrad: kompresja audio do OGG
- Obsługa wielu kanałow

- 1773 curses GUI :)
- Wypuszczone w grudniu 2014
- Urządzenie przeznaczone tylko do odbioru :)

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



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 SDS

- „Short Data Service” (jak SMS)
- Komunikaty, ale też sterowanie (napisy w autobusach, Teltronic) itp.
- Logi od użytkowników (pastebin itp.) np:

20181201 11:59:01 FUNC:SDSDEC [CPTI:1 CalledSSI:4201 CallingSSI:4202 CallingEXT:0 UserData4: len:64 protoid:02(Simple Text Messaging) coding_scheme:01 DATA:[WTH 2018!]] RX:1

20150126 09:34:09 FUNC:SDSDEC [CPTI:1 CalledSSI:1050YYY CallingSSI:1050XXX CallingEXT:0 UserData4: len:73 protoid:03(Simple location system) DATA:[0x80 0x80 0x03 0x5D 0xDD 0x1F 0xF3 0x29 0xC2]] RX:1

TElive lokalizacja

- TETRA lubi własnościowe rozszerzenia :)
- LIP (Location information protocol) – standard
- Location system: NMEA, RTCM-DC104, proprietary
- Simple Location system: NMEA, RTCM-DC104, proprietary (w tym type 0x80)

Perełki z pastebin. Simple location system type 0x80 :)

Telive inne funkcjonalności

- Export lokalizacji do KML. Odświeżalna mapa w Google Earth
- System modułowy. Dużo odbiorników.
- Znajdowanie nowych częstotliwości (SYSINFO, D-NETWORK-BCAST, Channel Allocation)
- Filtrowanie odtwarzania po SSI
- Sterowanie odbiornikiem po XML-RPC:

  - kompensacja PPM

  - automatyczne strojenie

  - skanowanie :)

https://github.com/filipsPL/signals/blob/master/ground/TETRA/telive_frequency_report.txt

Telive 1.9 frequency report 20170311 08:46:19

######### MCC 260 (Poland) MNC 10 (SFERIA S.A.) #########
390.3875MHz MCC 260 MNC 10 LA 4 CC 4 CONTROL CHANNEL
390.5125MHz MCC 260 MNC 10 LA 5 CC 5 Control: 390.7125MHz
390.5875MHz MCC 260 MNC 10 LA 4 CC 4 Control: 390.3875MHz
390.7125MHz MCC 260 MNC 10 LA 5 CC 5 CONTROL CHANNEL
[...]

######### MCC 260 (Poland) MNC 324 (Unknown network) #########
425.4875MHz MCC 260 MNC 324 LA 1 CC 1 Control: 425.7375MHz
425.7375MHz MCC 260 MNC 324 LA 1 CC 1 CONTROL CHANNEL

######### MCC 260 (Poland) MNC 2101 (MSWiA) #########
390.6125MHz MCC 260 MNC 2101 LA 1 CC 1 Control: 390.2125MHz
390.6375MHz MCC 260 MNC 2101 LA 2 CC 2 CONTROL CHANNEL
390.8125MHz MCC 260 MNC 2101 LA 1 CC 1 Control: 390.2125MHz
[...]

######### MCC 260 (Poland) MNC 2117 (Metro Warszawskie Sp. z o.o.) #########
425.2625MHz MCC 260 MNC 2117 LA 101 CC 1 CONTROL CHANNEL
425.3125MHz MCC 260 MNC 2117 LA 102 CC 1 Control: 425.1125MHz
425.4625MHz MCC 260 MNC 2117 LA 101 CC 1 Control: 425.2625MHz
425.1125MHz MCC 260 MNC 2117 LA 102 CC 1 CONTROL CHANNEL

Demonstracja TElive

Video ściągnięte z youtube:

https://www.youtube.com/watch?v=Hh9qpyHA3Ik

Youtube dorks: „telive” „ tetra listening” itp.

- Nie polecam publikowania takich filmów we własnym zakresie
- Wiele filmów które były na YT zostało usuniętych przez autorów

KODEK ACELP

- TETRA to „otwarty standard”, ale:
- Niejawne szyfrowanie i wymiana kluczy
- Duże pole dla własnościowych rozszerzeń
- Nieotwarty kodek, ale są źródła
- Nie wiadomo jak z rozpowszechnianiem

https://github.com/sq5bpf/install-tetra-codec

Instalacja Telive

- Systemy debianopodobne: Debian, Raspbian, Mint, Ubuntu :

  $ wget https://github.com/sq5bpf/telive/raw/master/scripts/install_telive.sh

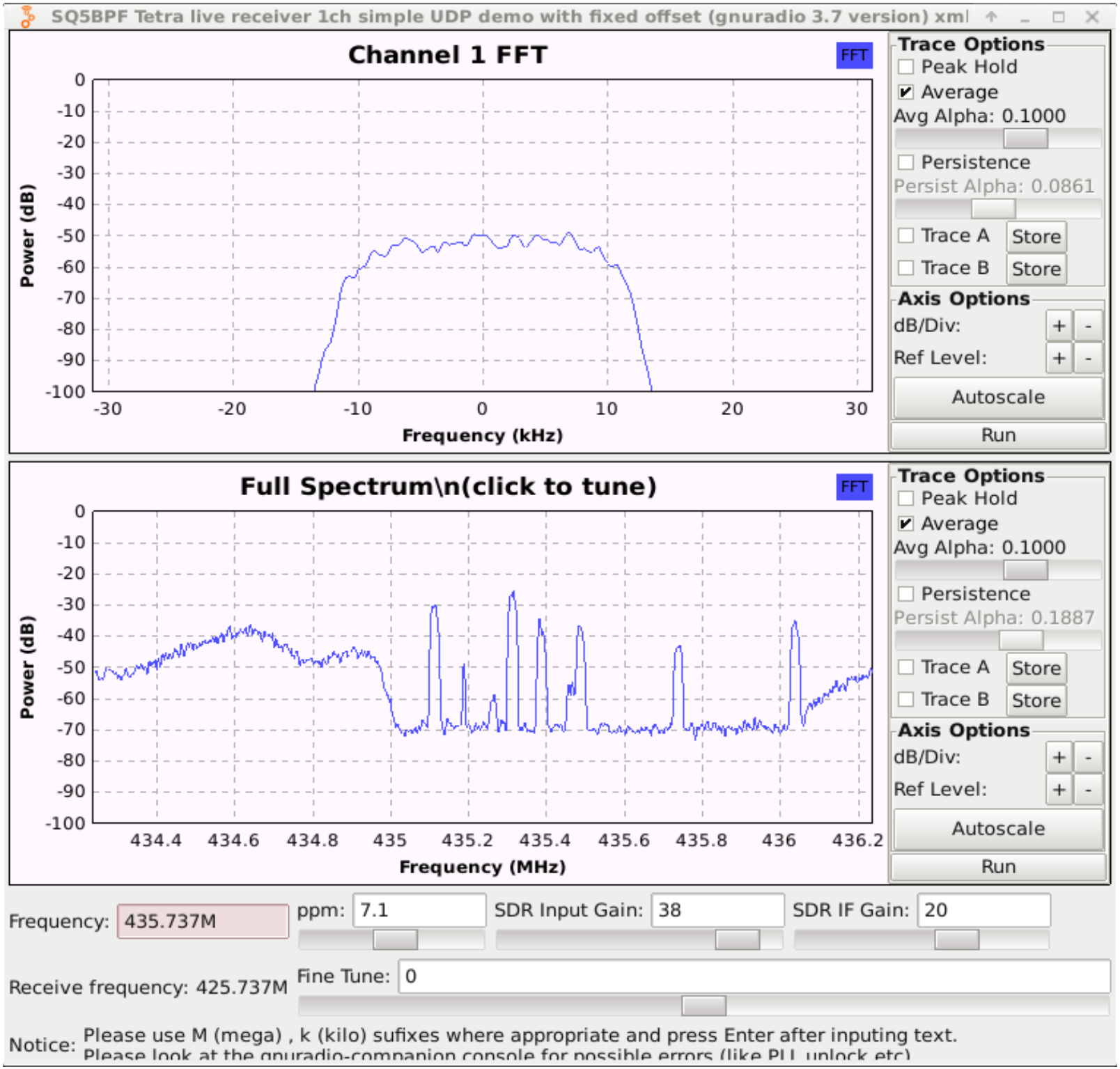
  $ ./install_telive.sh

- Dokumentacja:

  https://github.com/sq5bpf/telive/raw/master/telive_doc.pdf

Jak zacząć?

- Ustalić PPM dla swojego odbiornika
- Wersja jednokanałowa simple xml-rpc
- Znaleźć kanał kontrolny swojej sieci (bez szyfrowania)
- Cierpliwości, nie zawsze jest głos


SQ5BPF Tetra live receiver 1ch simple UDP demo with fixed offset (gnuradio 3.7 version) xml
Channel 1 FFT
FFT
Power (dB)
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-30
-20
-10
0
10
20
30
Frequency (kHz)
Trace Options
Peak Hold
Average
Avg Alpha: 0.1000
Persistence
Persist Alpha: 0.0861
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Run
Full Spectrum\n(click to tune)
FFT
Power (dB)
434.4
434.6
434.8
435
435.2
435.4
435.6
435.8
436
436.2
Frequency (MHz)
Trace Options
Peak Hold
Average
Avg Alpha: 0.1000
Persistence
Persist Alpha: 0.1887
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Run
Frequency:
435.737M
ppm:
7.1
SDR Input Gain:
38
SDR IF Gain:
20
Receive frequency: 425.737M
Fine Tune:
0
Notice:
Please use M (mega) , k (kilo) sufixes where appropriate and press Enter after inputing text.
Please look at the gnuradio-companion console for possible errors (like PLL unlock etc)

Jak mogę pomóc?

- Udostępnić infrastrukturę TETRA (LAB?)
- Nie namawiam nikogo do udostępniania logów, mimo że np. te znalezione w internecie bywają bardzo przydatne
- Tym bardziej nie namawiam do reverse engineeringu firmware, np. aby poznać jak działa kryptografia
- Jakie funkcje mogłyby być przydatne dla wdrożeniowców/administratorów TETRY?
- Jestem otwarty na sugestie

PYTANIA?

Jacek Lipkowski SQ5BPF
SQ5BPF@lipkowski.org

https://github.com/sq5bpf/telive