Signals intelligence

or

How to start your own NSA

Jan Hrach
NSA Litoměřice
http://jenda.hrach.eu/
CD98 5440 4372 0C6D 164D A24D F019 2F8E 6527 282E

Slides: http://jenda.hrach.eu/f2/nsal-ctjb.pdf

This talk

- Radio signals, not computer networks
- Ideas what is in the air (and what to do with it)
- Most of it is fake
  - sometimes even source code is given

Hardware

- rtl-sdr ($10)

- 2 MS/s (oc'd to 3.2), 48 dB, RFI/IMP :(

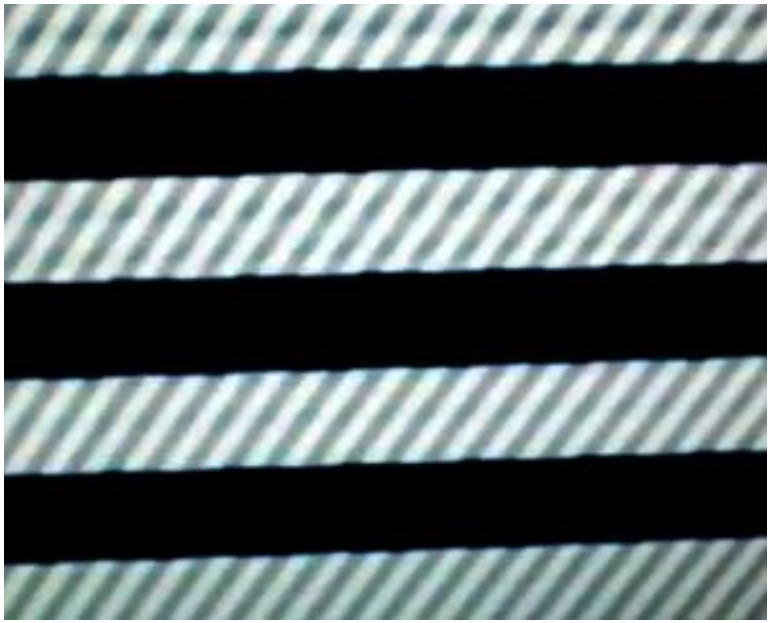
Hardware

- rtl-sdr + filter + tinfoil hat ($30)

- kalibrate rtl

Hardware

- TX: bladeRF ($400), RaspberryPi, Baofeng ($40), GPU (https://www.brmlab.cz/project/gctx)



RaspberrySpy

Wide input range switching PSU 7-40 V

3G modem for remote operation

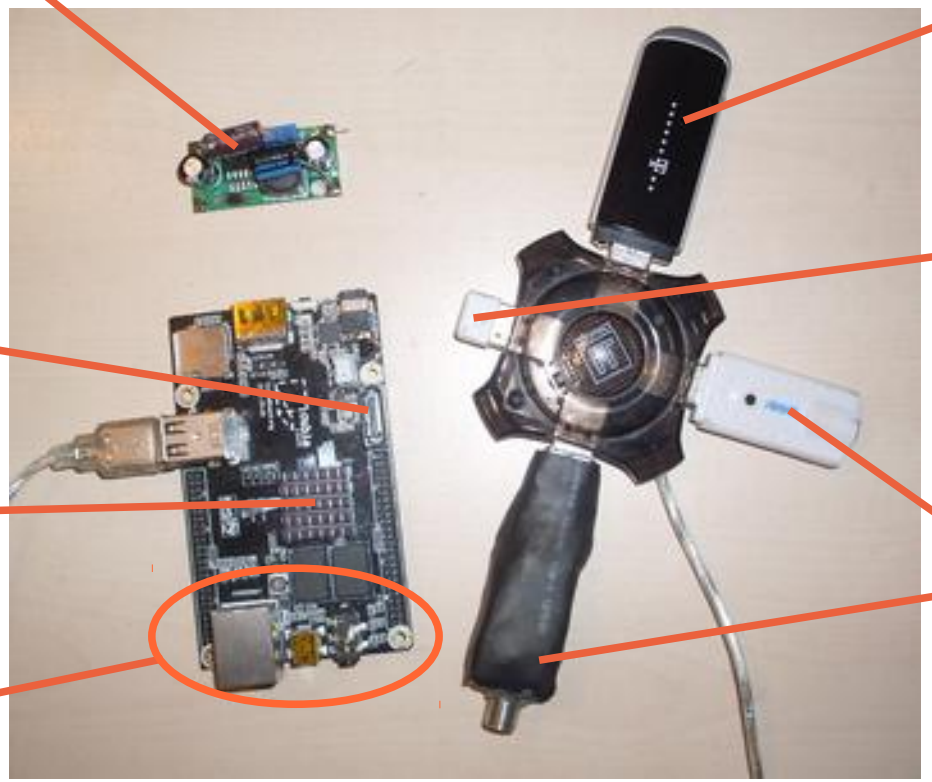
SATAII port for excessive data capture

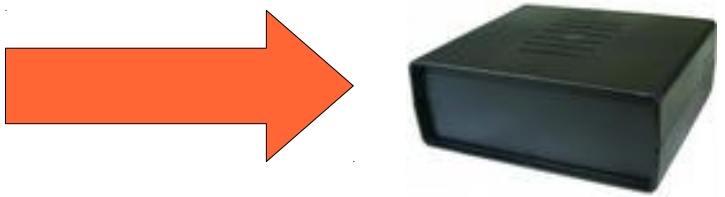
802.11bgn WiFi + packet injection

Dual core A20 Cortex-A7 @ 1 GHz with 1 GB DDR3 RAM

Multiple rtl-sdr sticks + application-specific filters

Fast ethernet
GPIOs
USB OTG
Audio in/out





RaspberrySpy Usecase

- Conference
- Unknown facility
- SCADA network
- Rooftop

- 3G TX & SDR RX → fail

Software

- GQRX (crap) (demo)
- https://www.brmlab.cz/project/sdr/tritchori
- libgnuradio
- …and custom software
- crap :(

Signals

- Plain FM voice
  - 150-180, 440-480 MHz
  - taxi
  - messengers
  - security
  - drug enforcement agency
  - wireless microphones (670-800 MHz)
  - baby monitors (always on!)
  - hobby, HAM
  - RX: rtl_fm, gqrx, https://www.brmlab.cz/project/sdr/szdc

Signals

- GSM
  - RX: Airprobe, OsmocomBB
  - plain preamble (IMSI!), then encrypted
    - SMS easy to intercept, voice calls complicated
  - A5/1 cracked (https://www.brmlab.cz/project/gsm/deka)
  - https://brmlab.cz/event/codenight
  - 3G → A5/3
  - GSM-R!!


Eee PC
FIXME: Watchdog sucks
FIXME: Pool support not implemented
FIXME: Session save/restore (at least bursts-to-be-cracked)
FIXME: Crack queue and offloading
Loading firmware

Tetra

- “Rugged GSM”
- Police (municipal), public transport, emergency teams [“krizový štáb”]
  - Lots of communication crap
- Encryption modes “0” to “3”, costs $$$
- Most networks are “mode 0”
- RX: Osmo-tetra
  - gr3.6 (http://jenda.hrach.eu/brm/rad/tetra-3.6-3.7.patch)
  - Decodes frames, add traffic channel dump
  - Run reference codec (non-free C)
  - 4 CPU cores can do the whole network in parallel!

Mototrbo/DMR

- DMR: standard similar to Tetra
- Mototrbo: Motorola proprietary extension
- RX: DMRDecode, dsd
- Encryption:
  - None
  - Basic (8-bit key + 16-bit LFSR)
  - Enhanced (40-bit RC-4, IV in LSBs, unknown)
  - 2014 AES-256 update
- Municipal police, industry, SCADA (!)

At present, ČEZ is using both time slots for voice communication, but future plans include using the second time slot for transferring data from remote terminal units in the field to the control centre. This will enable the remote measurement and control of power distribution and facilitate the monitoring of power quality, highlighting potential problem areas before outages occur.

Also with Enhanced Privacy, you enjoy encryption protection using 16 encryption keys with 40-bits per key to protect voice, text messages and GPS data.

Tetrapol/Matra

- Yet another trunked network
- Police, army
- Encryption: none or unknown
- RX: none
- Early experimental L1 decoder
- Specification (without crypto) available, code!

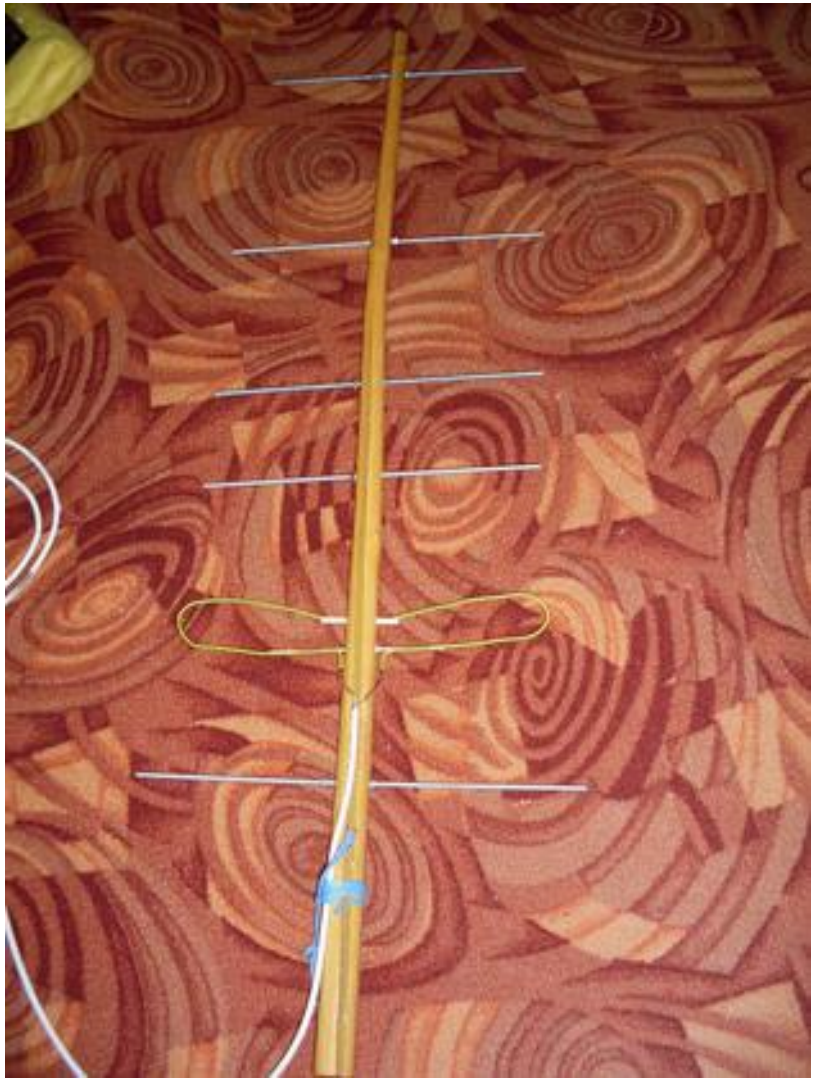
Paging

- RX: multimon-ng
- Emergency incident info

FM(AFSK(Data))

- Varies, e.g. trains
  - https://www.brmlab.cz/project/sdr/szdc
- Sirens
- Weather sonde
  - Find, fix and finish practice
  - https://www.brmlab.cz/project/sdr/fff
  - https://www.brmlab.cz/project/weathersonde/start

Find, fix and finish



http://petr-kubac.blog.cz/1301/radiokompas-1

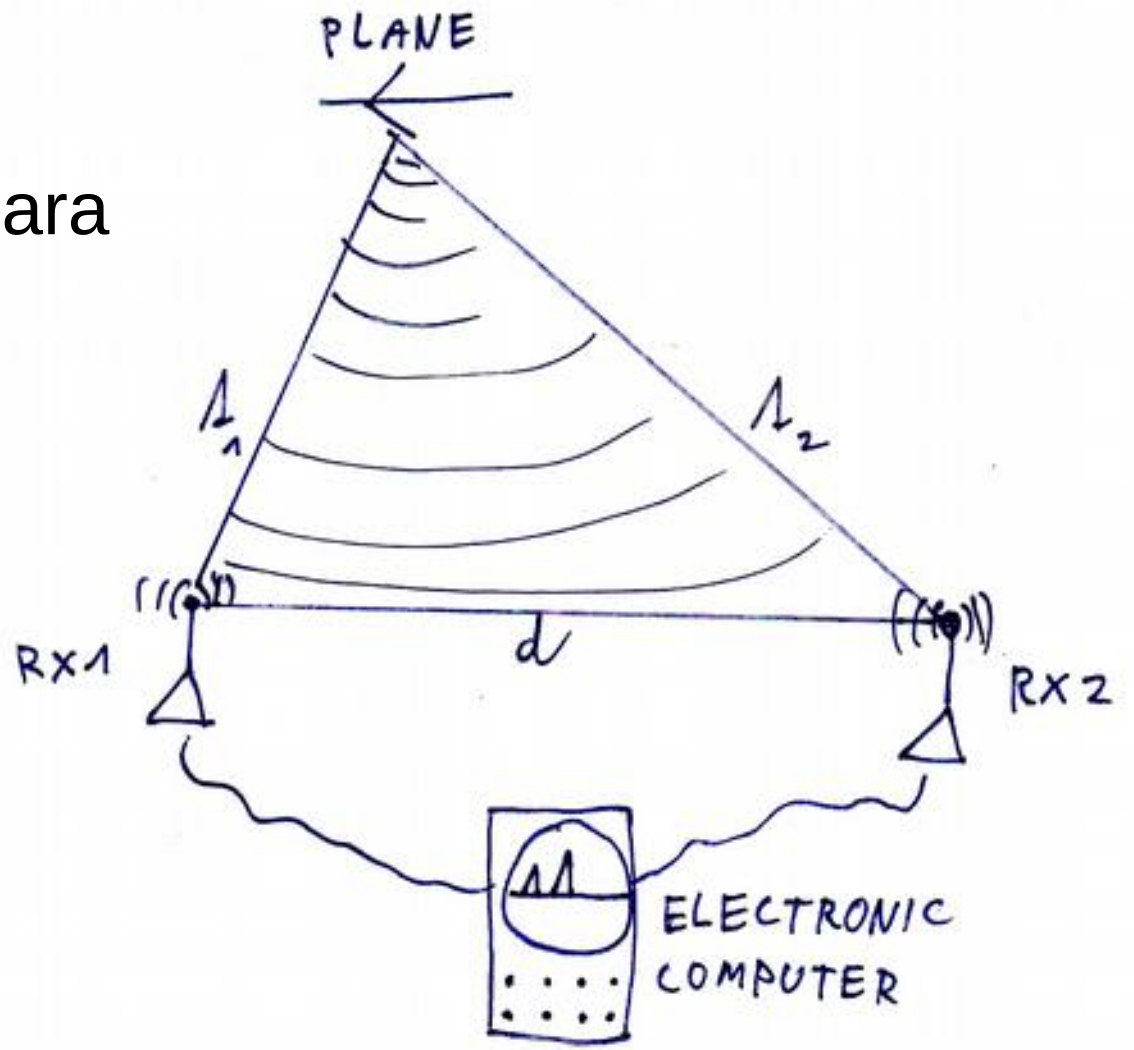

SEARCHER

Planes

- Active: radar, ACARS, ADS-B
- RX: acarsdec, dump1090
  - rtl-adsb is L1-only
- ADS-B TX?

Planes

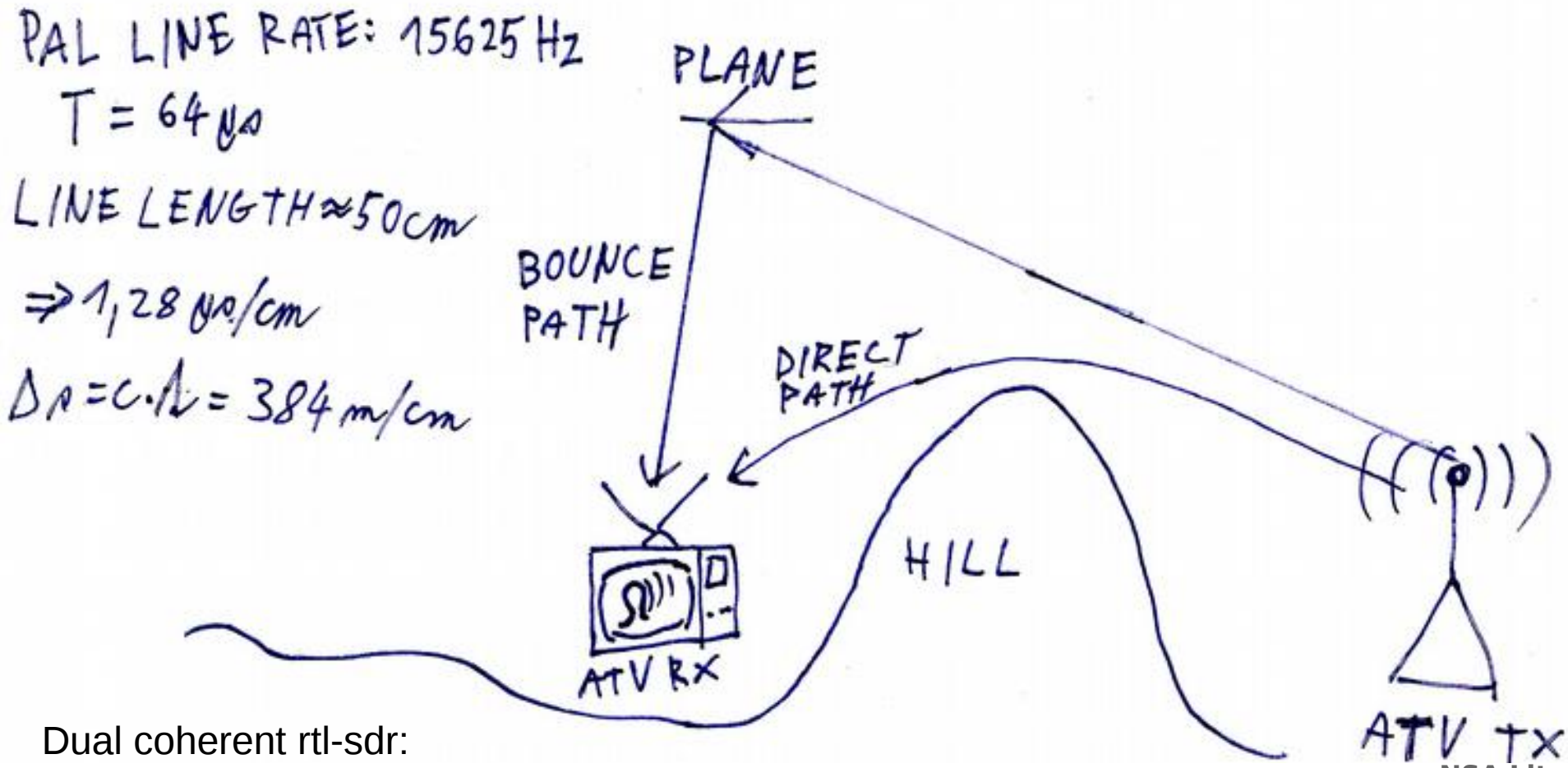
- Active-passive:
  - Kopáč/Ramona/Tamara
  - Flightradar24 MLAT



ATV signal ghosting

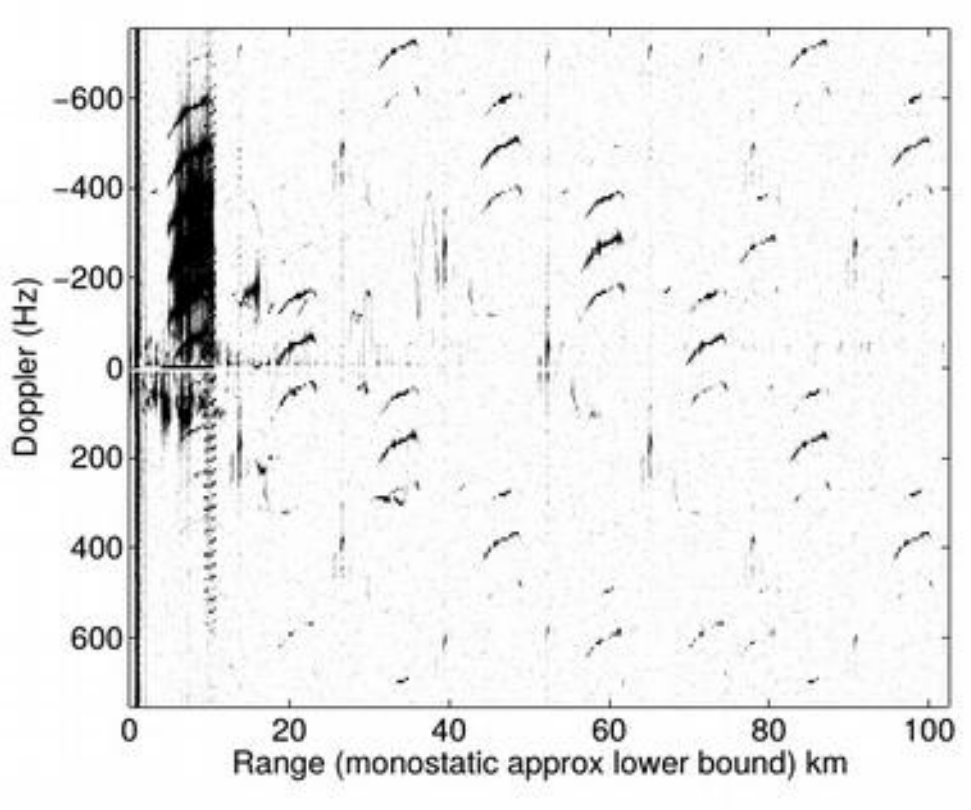
source: http://www.rsm.govt.nz/cms/consumers/reception-problems/what-does-interference-look-like

- Fully passive
  - VERA (Věra)
  - http://people.duke.edu/~hah16/papers/passive-radar-processing-preprint.pdf
    - Anyone knows the math for this^?



Dual coherent rtl-sdr:
https://www.youtube.com/watch?v=KRqtqtCVRR0

http://www.armadninoviny.cz/cesky-tichy-strazce-vidi-i-neviditelna-letadla-.html
http://clanekvera.sweb.cz/



NSA Litoměřice
the only company that actually listens to your needs

ASMKS

- ASMKS (Automatic system for frequency spectrum monitoring) by ČTÚ
- Coherent scanners + MLAT
- DYI: SDR + GPS, SDR + FM?
- Anyone?

EOF

- kthxbye