

Zaměřování vysílačů s rtl-sdr

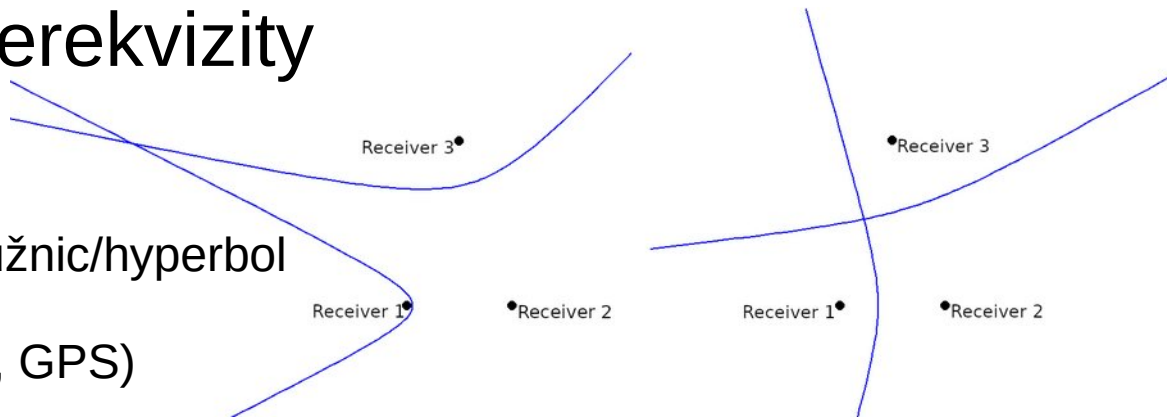
Jan Hrach
jenda@hrach.eu

2020-02-29

Prerekvizity

- **Určování polohy cíle**

- triangulace – průsečík (polo)přímek
- trilaterace (multilaterace) – průsečík kružnic/hyperbol
- úhel+vzdálenost
- a to všechno i inverzně (zeměměřičství, GPS)
- dilution of precision



- **Softwarově definované rádio**

- digitalizuje rádiové vlny v okolí zvolené frekvence a posílá je do počítače
- dále s nimi lze dělat cokoli co zvládnete naprogramovat
- přednáška z InstallFestu 2016: <https://www.youtube.com/watch?v=i1ZB70nPF-g>

- **rtl-sdr**

- levné SDR (200 Kč)
- USB klíčenka pro příjem TV a rádia
- SDR režim
- nekvalitní
- více druhů dle tunerů, použil jsem konkrétně R820T2

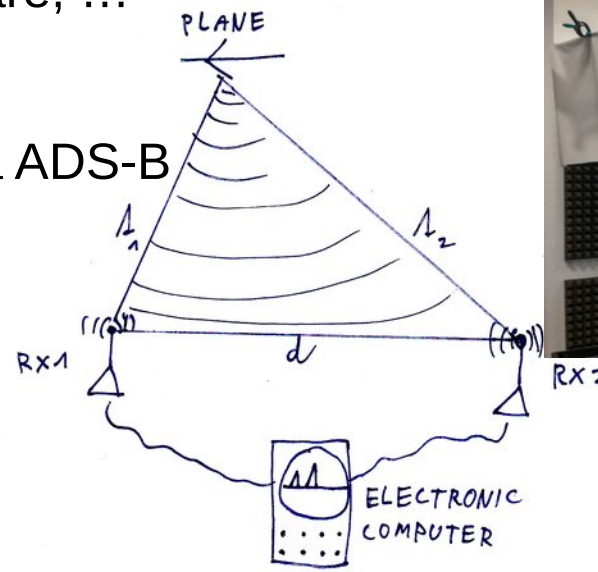


Úvod, kontext, motivace

- Aktivní/primární radar
 - vyšle signál, rozptyl na překážce, návrat se zpožděním
 - přednáška: <https://popelka.ms.mff.cuni.cz/~hrach/smrst-2019/>
- Odpovídače letadel: ADS-B, OGN (malá letadla)
 - Interrogation svazek nebo samovolně
 - 1090 MHz, 868 MHz
 - Levné přijímače → FlightRadar24, FlightAware, ...
 - Neoznamování polohy
- Multilaterace letadel podle palubních radarů a ADS-B
 - Tamara, Věra (jedna z funkcí)



src: <https://en.wikipedia.org/wiki/Radar>



Mutability mlat-server

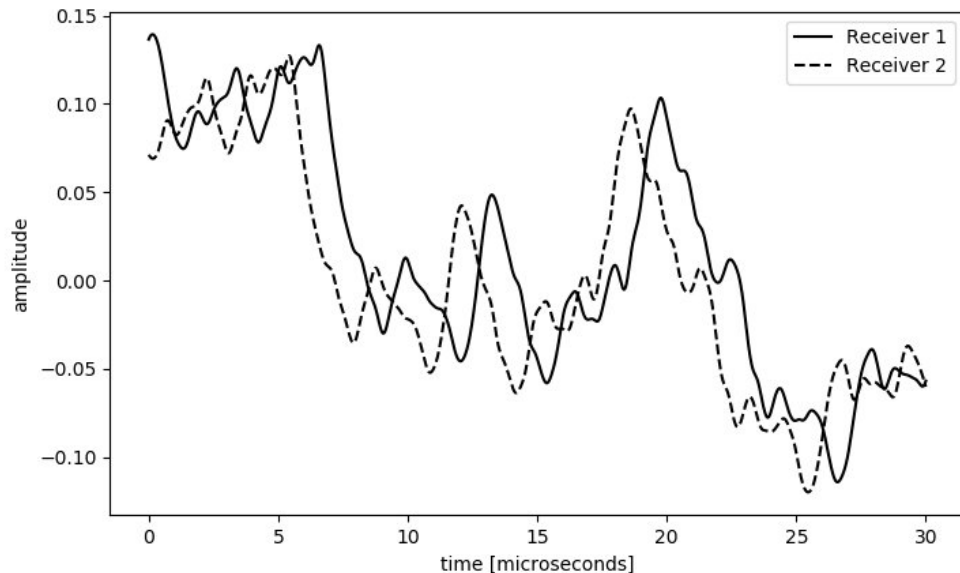
- <https://github.com/mutability/mlat-server>
- ADS-B multilaterace s rtl-sdr
 - jak tohle může fungovat?!
 - mlat/server/clocktrack.py
 - mlat/server/solver.py
- s rtl-sdr se dá tamarovat a já chci svoji vlastní Tamaru!

Multilaterace obecných nekooperujících vysílačů

- Nekooperující – nemůžeme ovlivnit signál (e.g. žádné časové značky)
- třeba komerční TV/rádio, mobily, ...
- Hon na lišku/na sondu, záchranné operace, zaměřování rušení, sledování vysílaček no

Multilaterace obecných nekooperujících vysílačů (cont.)

- Obecně neumíme ten signál demodulovat, ale můžeme porovnávat zpoždění přímo na samplech



$$\text{distance}(\text{transmitter}, \text{receiver1}) - \text{distance}(\text{transmitter}, \text{receiver2}) = \Delta tc$$

- Chtělo by to něco na určení podobnosti, třeba crosscorrelation $x(f, g)_k = \sum_{j=-\infty}^{\infty} f_{j+k} \overline{g_j}$
- kvadratické, ale jde pomocí FFT v $O(n \log n)$

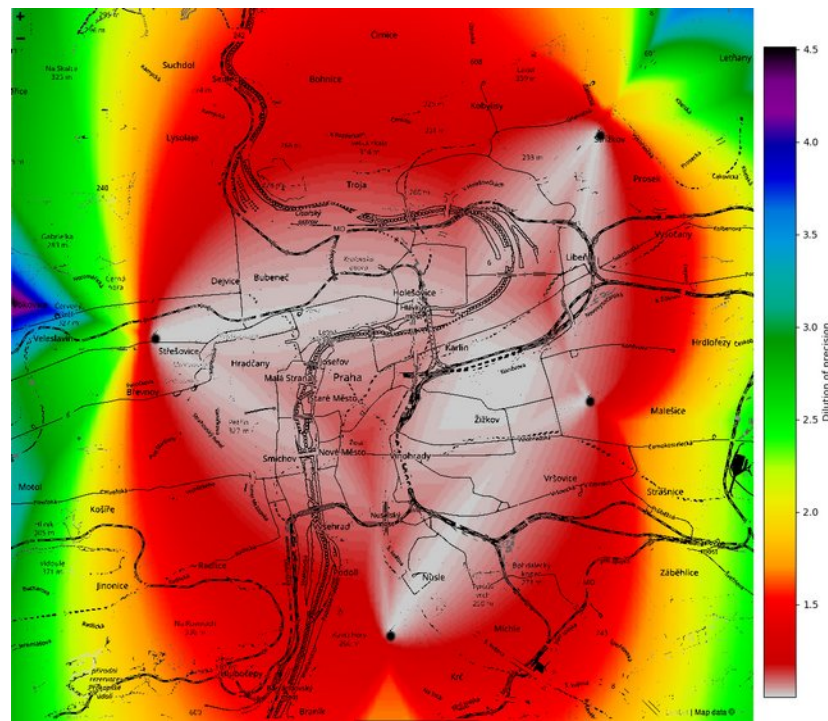
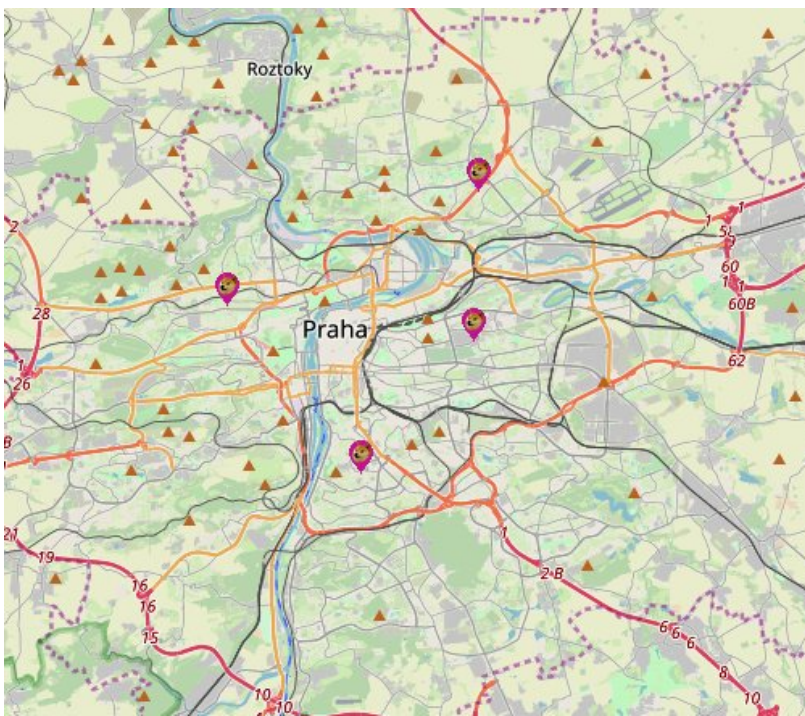
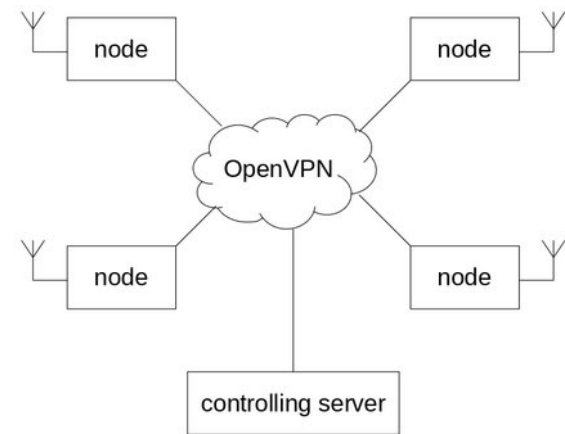
Synchronizované přijímače

- Budeme potřebovat přesný čas
- Obecně nemáme multiplex jako na ADS-B
- 100 ns = 30 m
 - NTP bez šance
- Tamara má mikrovlnné pojítko/optiku s distribucí času
 - drahé, máme jen obyčejný internet
- atomové hodiny
 - drahé
- GPS PPS (pulse per second)
 - problémy s připojením do SDR („mlátička“)
 - custom HW, Blitzortung
- Vysílač se známým umístěním → známým Δt
 - přijímat současně s cílem (dvoukanálový přijímač)
 - přeladit se s udržením synchronizace
 - THIS



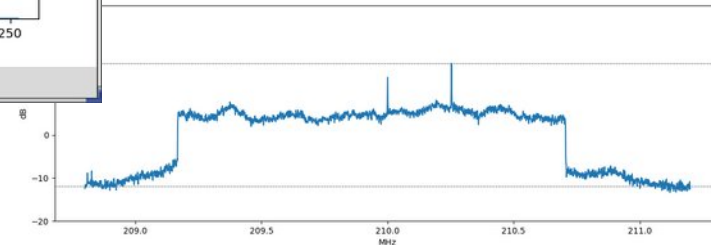
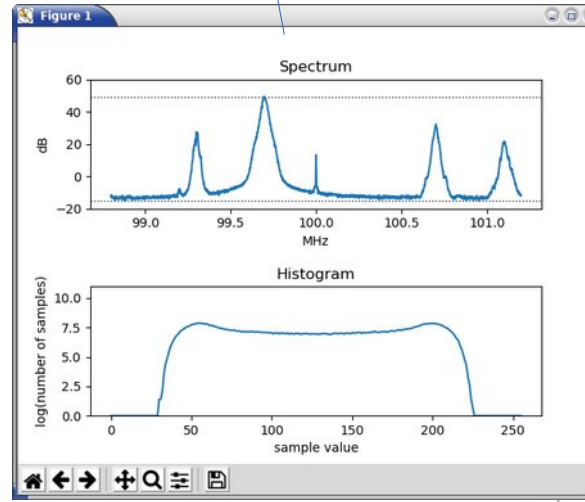
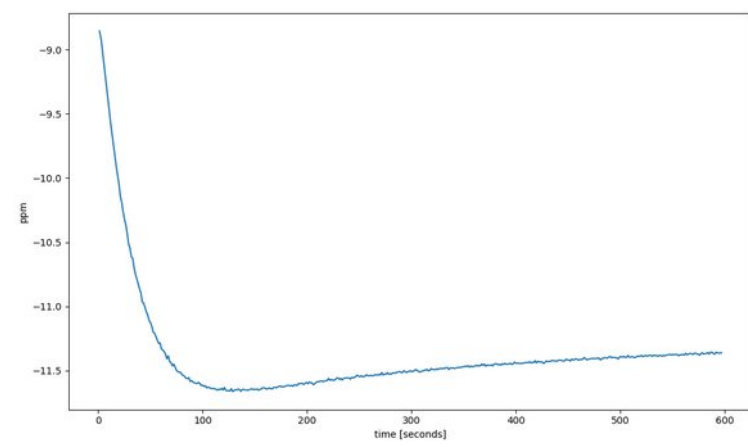
Moje síť

- 4 obyčejné počítače a OvocePi s Linuxem (bez RT jádra)
- 4 různé antény od 50 do 1500 Kč
- 4 rtl-sdr
- 4 střechy v Praze



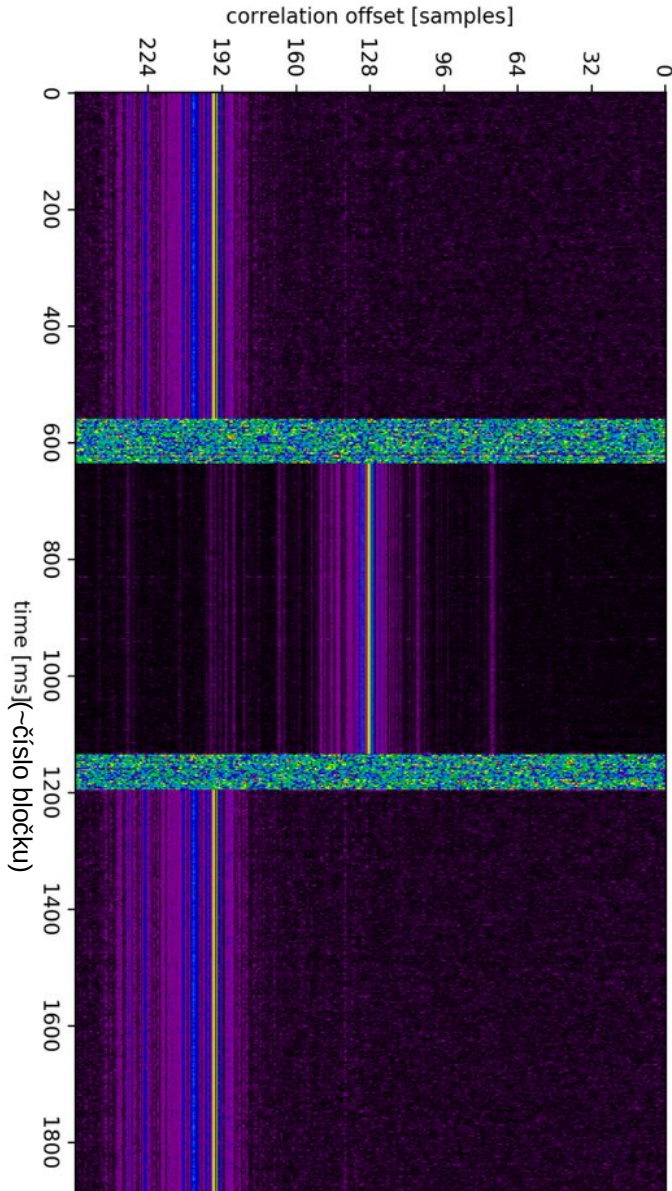
Měření

- Spustit rádio, číst sample a počkat na zahřátí
- Změřit přibližnou chybu hodin pomocí GSM
- Odhadnout nastavení zesílení pro referenci a cíl
- Synchronizovat čas přes NTP, zbytek musí udělat přiměřeně současně celá síť
- Naladit se na cíl
- Počkat 0.5s
- Naladit se na referenci
- Počkat 0.5s
- Naladit se na cíl
- Počkat 1s
- Tyto 2s uložit a poslat masterovi

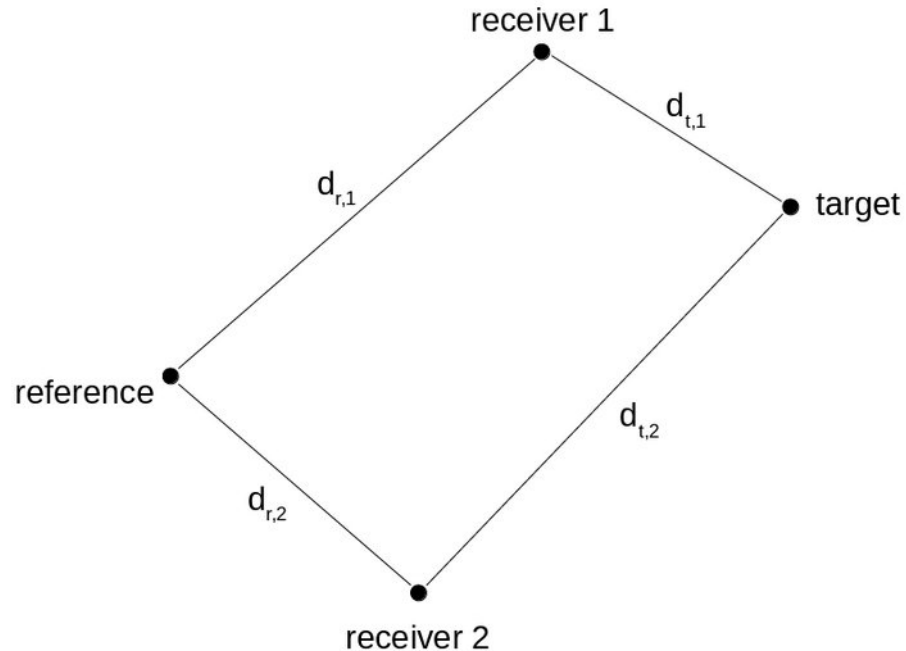


Zpracování

- Budeme zpracovávat po dvojicích přijímačů
- Máme odhad chyby lokálního oscilátoru (z GSM) → signál natáhneme v čase a posuneme ve frekvenci
 - tohle obecně nechcete dělat pomocí featur v rtl-sdr (PLL dithering, omezená přesnost aritmetiky)
- Dále víme že NTP + ne-RT počítač vnese chybu ~50 ms
- Rozsekáme referenci (tu prostřední část) na bloky ~200ms
- Crosscorrelation překrývajících se bloků
- Kvantizace výsledků
- Získáme posun s přesností ~10 samplů (5 μ s), zarovnáme signály
 - btw. co dalšího by šlo dělat s přijmači syncnutými na μ s?
- Rozsekáme na bločky po ~200 μ s, crosscorrelation
- Vykreslíme



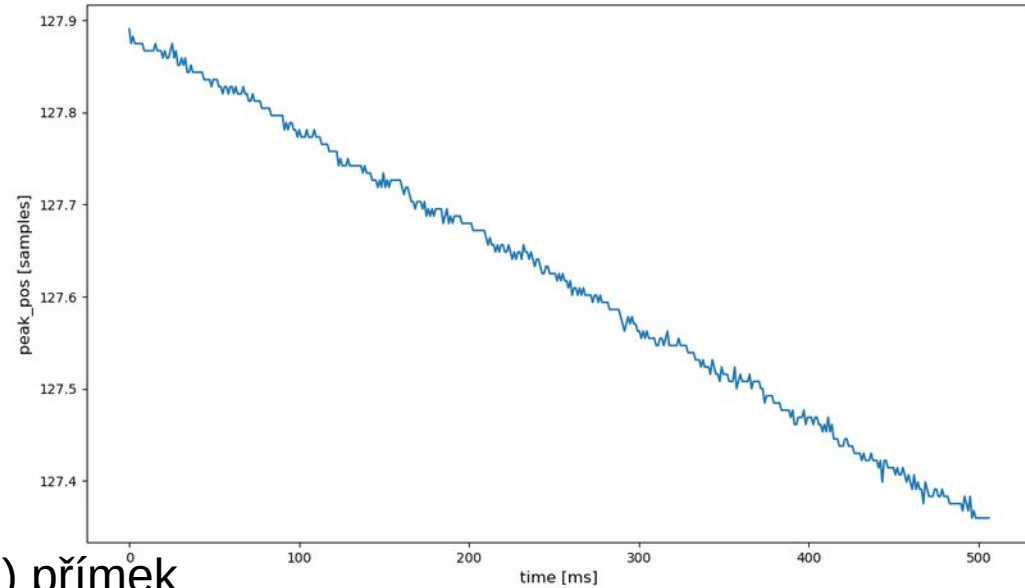
barva = abs(dot(bloček z přijímače 1, bloček z přijímače 2 posunutý o offset))

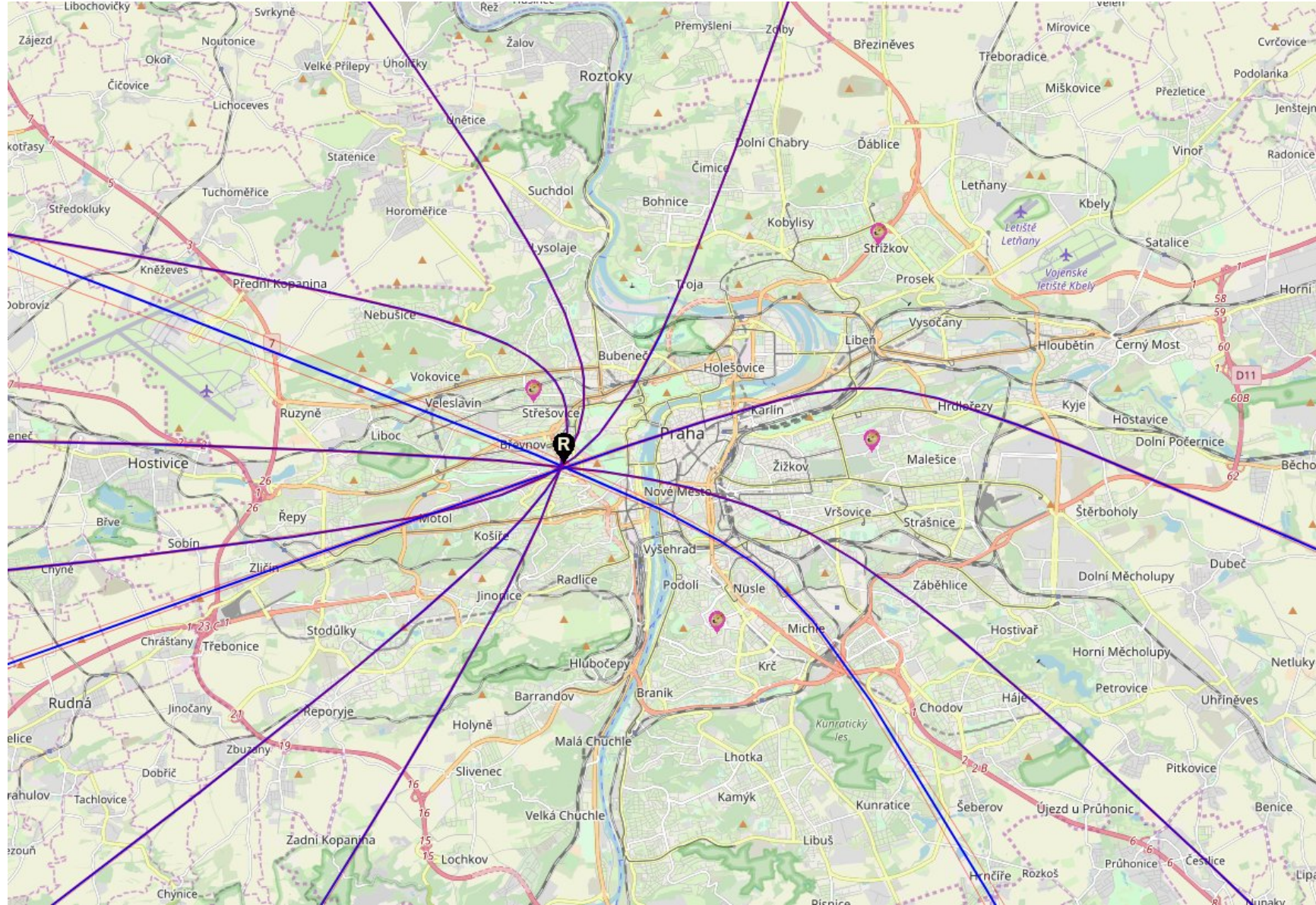


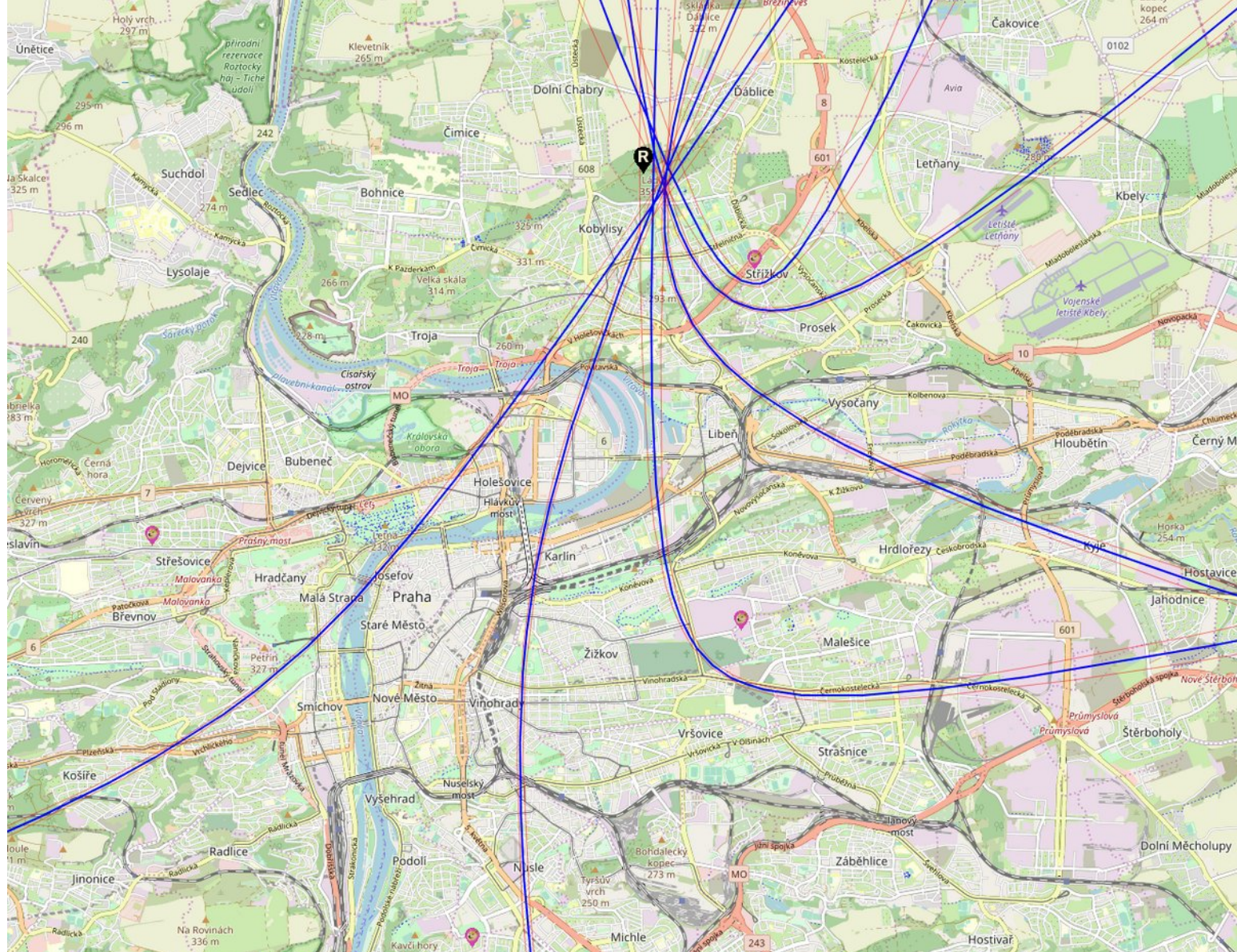
- Odhadneme, že Δt je 66 samplů, což při vzorkování našeho rádia 2.25 MHz = 8.8 km
- Vlezeme na ctu.cz a ty vysílače tam najdeme
- Změříme na mapě kolik to jako mělo vyjít
- A ono je to správně!

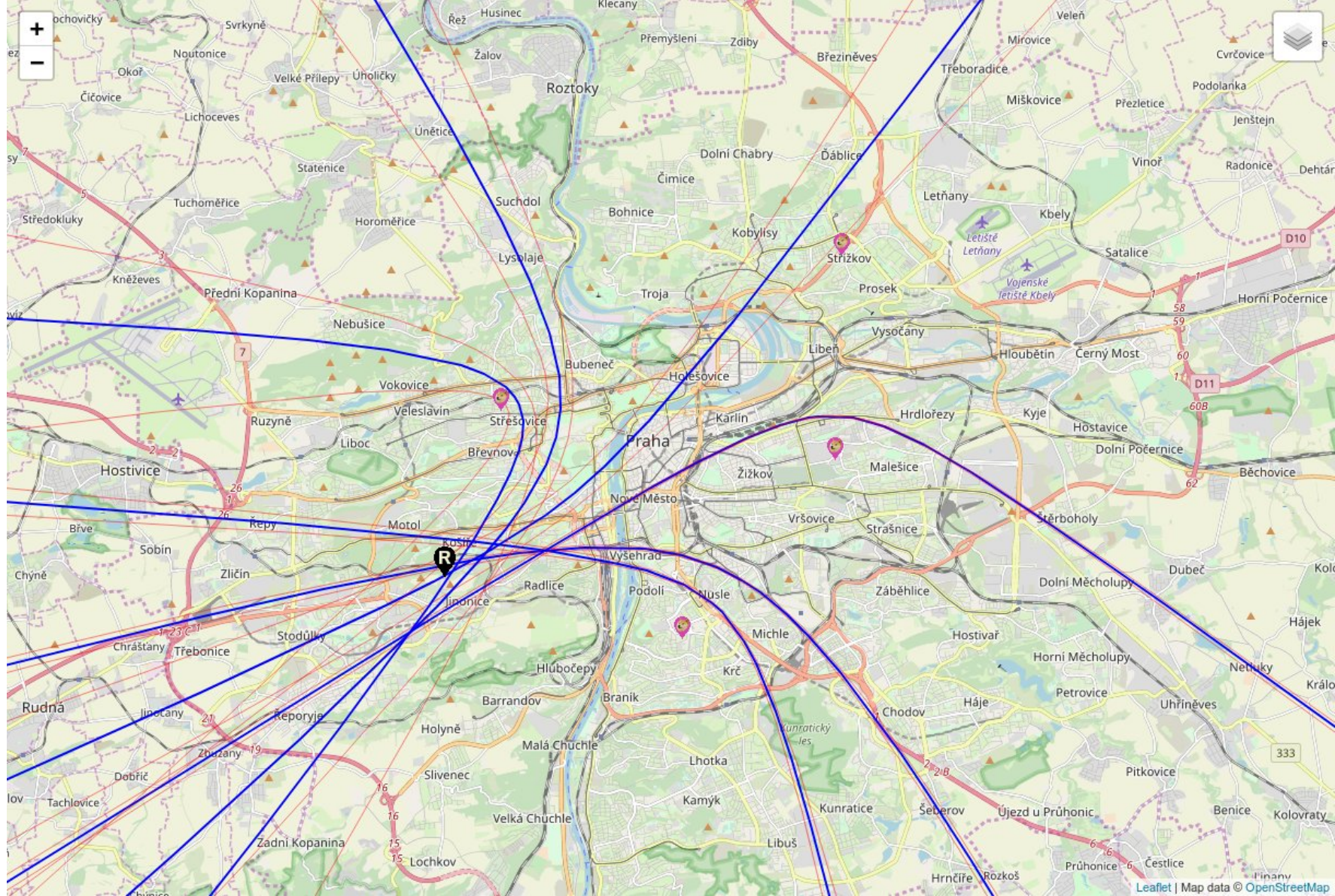
Zpracování (cont.)

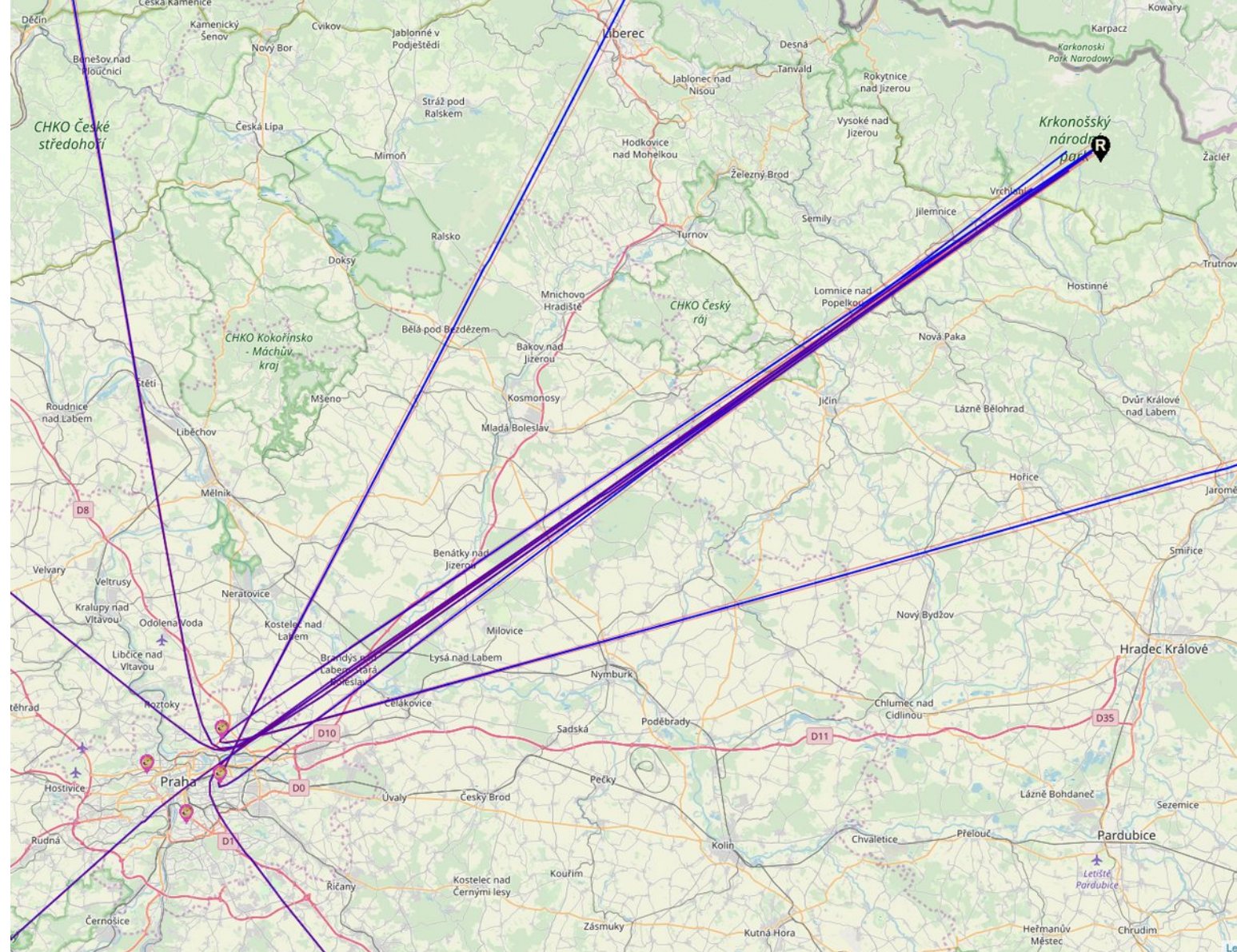
- Subsamplevé rozlišení
 - proložení peaku parabolou/gaussiánem
 - zkusmo posunutí o zlomek samplu
- Argmax korelace se trochu posouvá
 - Naše GSM korekce nebyla přesná!
 - Nafitujeme přímkou
 - Sklon přímky = hodnota korekce
- Přepočítáme
- Argmax pro referenci i cíl proložíme přímkami
- Spočítáme vzdálenost (podle té správné osy :) přímek
- Získali jsme Δt pro jednu dvojici přijímačů!!!
- Opakujeme pro všechny dvojice
- Vykreslíme do mapy
 - btw. vyrobit GPX je easy
 - btw2. přiložím tečnou rovinu ke kouli, na ni to nakreslím, pak naškáluju lat,lon podle prostředku a ono to nějak dopadne; bylo by hezké řešit projekce





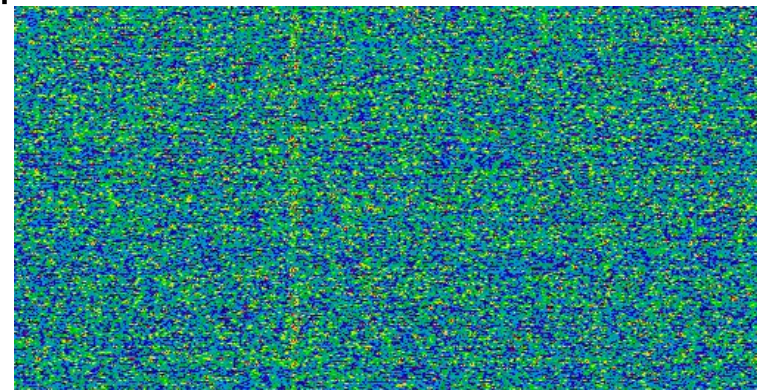
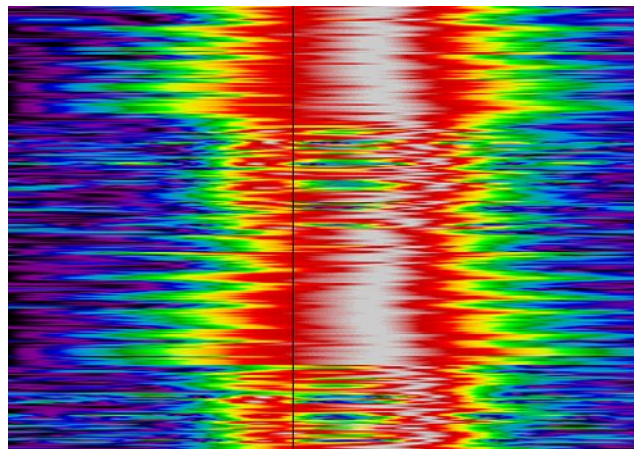
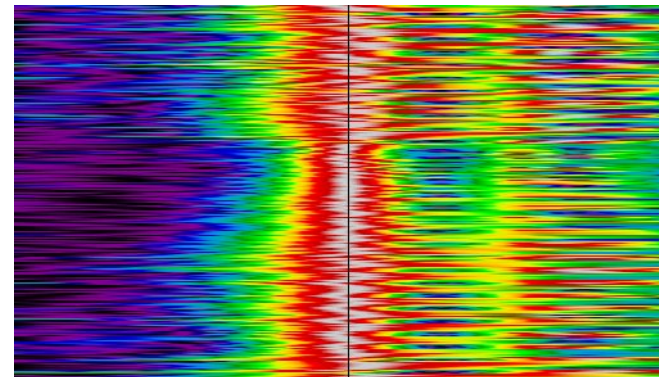






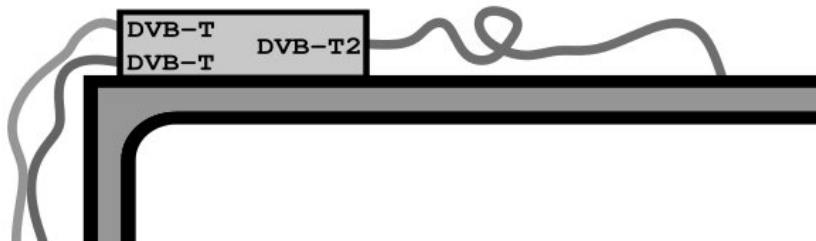
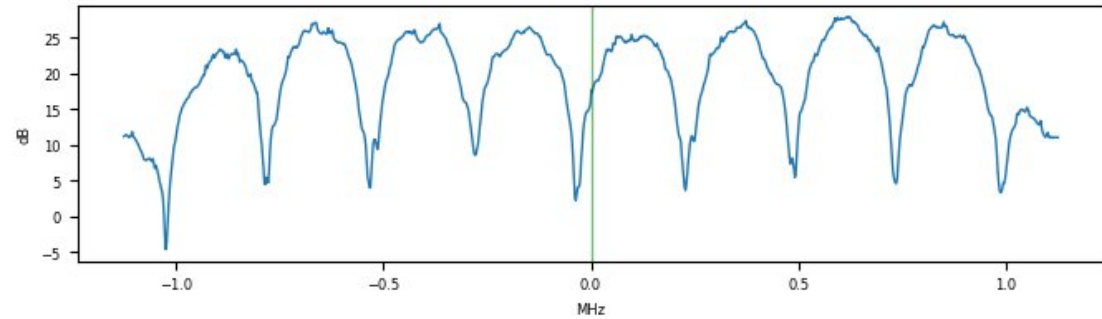
Problémy

- Pro DVB-T a DAB to funguje naprosto skvěle!
- FM rádio – špatná korelační funkce
- Slabý signál (Pardubice z Prahy) – utopené v šumu
- Statistické zpracování (kvantizace a filtrace argmaxů) pomůže
- Interference
 - při ní to úplně selže :(
- Whitening signálu
 - nezlepšil to



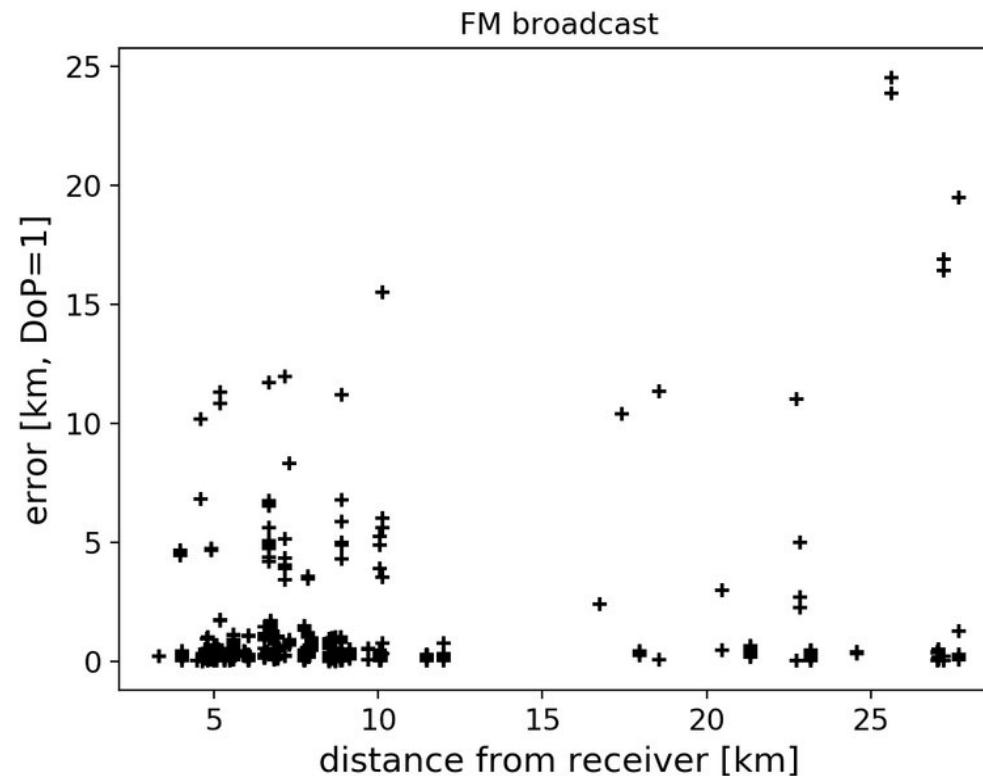
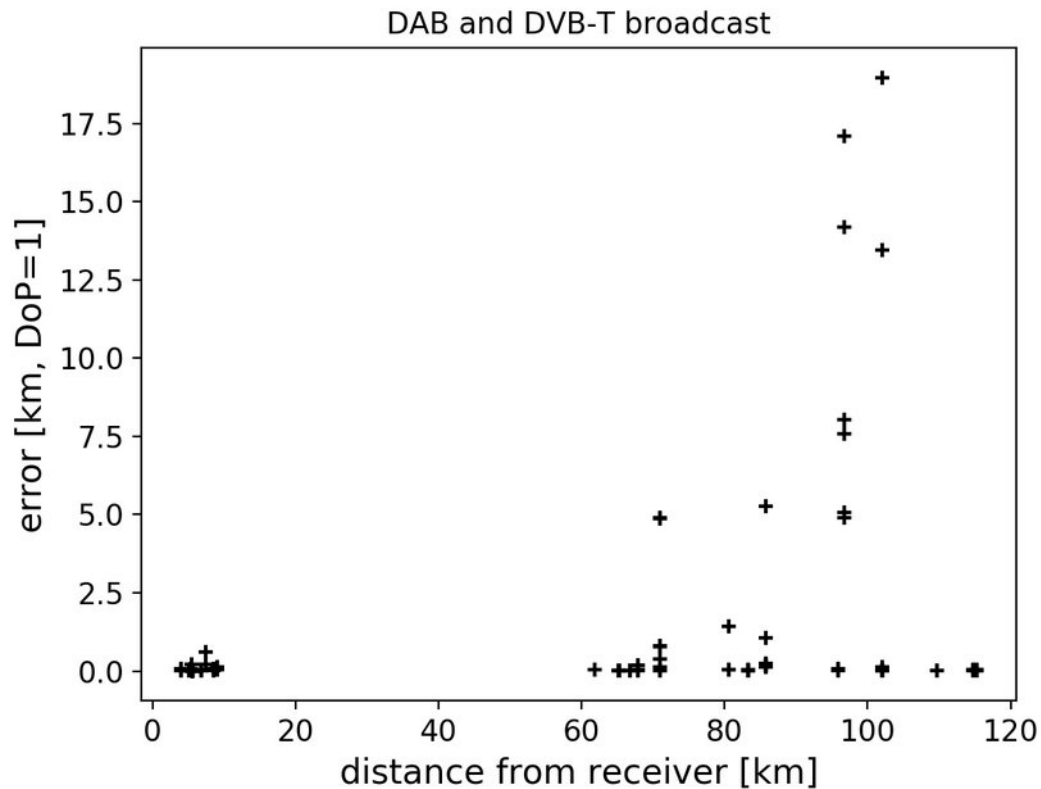
Problémy (cont.)

- Úzkopásmové signály (Tetra, Tetrapol, NFM) úplně na nic
- DVB-T a DAB SFN ?čas, možná skipnout a pak se vrátit
 - můžeme počítat více argmaxů
- DVB-T2 velmi-SFN



Výsledky

- Stáhneme tabulku z ctu.cz, zaměříme všechno, porovnáme



Pasivní zaměřování nevysílajících cílů



- Typicky dvě směrové antény (direct + surveillance)
- Extrémní dynamika
- Falešné cíle kvůli Doppleru
- Složitě
- Husté

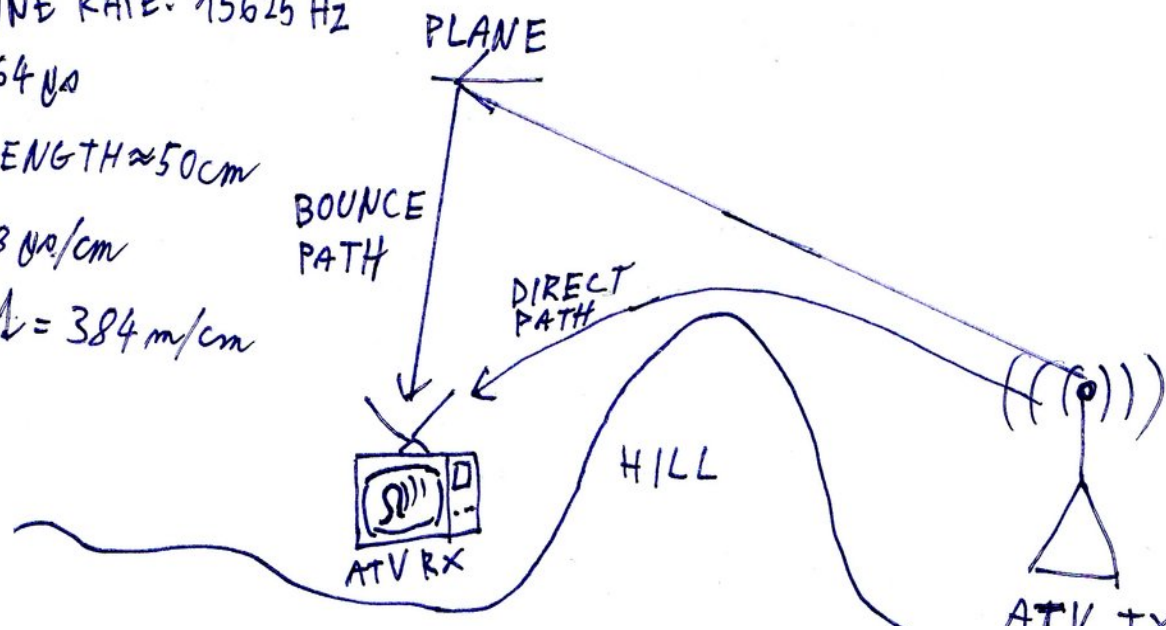
PAL LINE RATE: 15625 Hz

$T = 64 \mu s$

LINE LENGTH $\approx 50 cm$

$\Rightarrow 1,28 \mu s/cm$

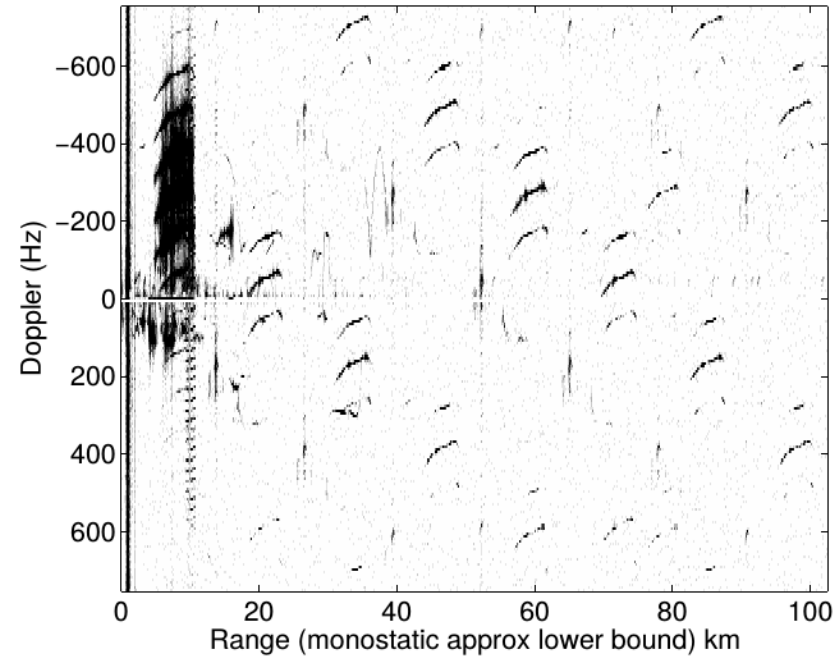
$\Delta R = c \cdot \Delta t = 384 m/cm$



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

<http://clanekvera.sweb.cz/>

<https://jenda.hrach.eu/f2/passive-radar-processing-preprint.pdf>



- <https://jenda.hrach.eu/dipl.pdf>