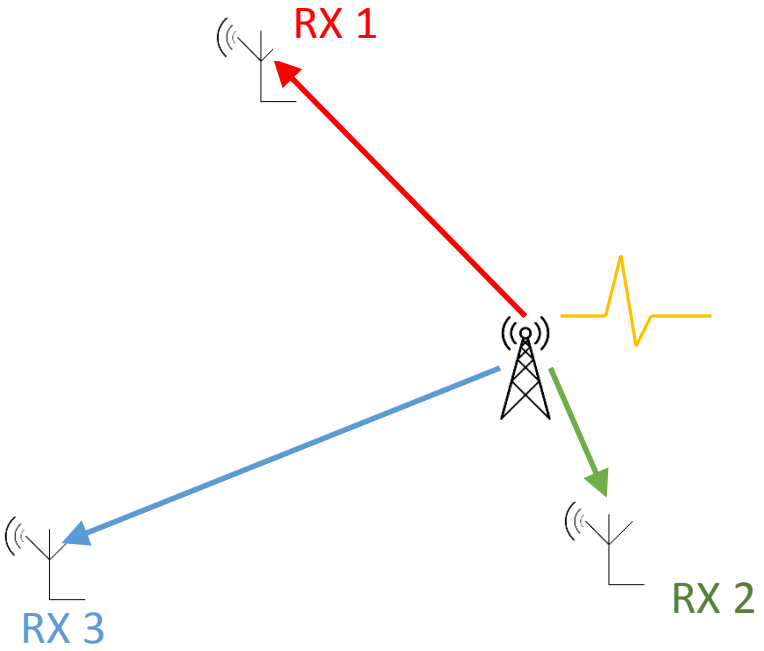
Introduction and Experiments on Transmitter Localization with TDOA

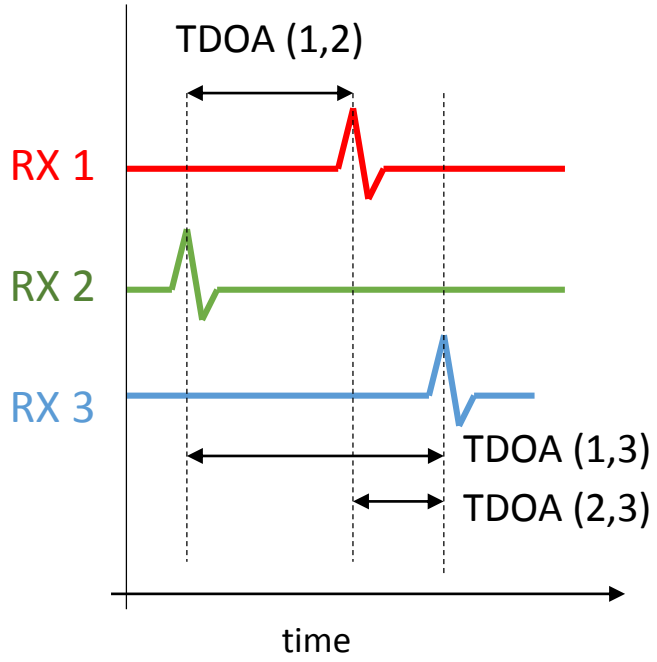
Stefan Scholl, DC9ST

Software Defined Radio Academy,
Friedrichshafen, Germany, 07/2017

Basic Idea of TDOA

- TDOA = Time-Difference-of-Arrival (Multilateration)
- use several receivers and
- analyze time **difference** of received signal
- apply geometry to determine position of transmitter

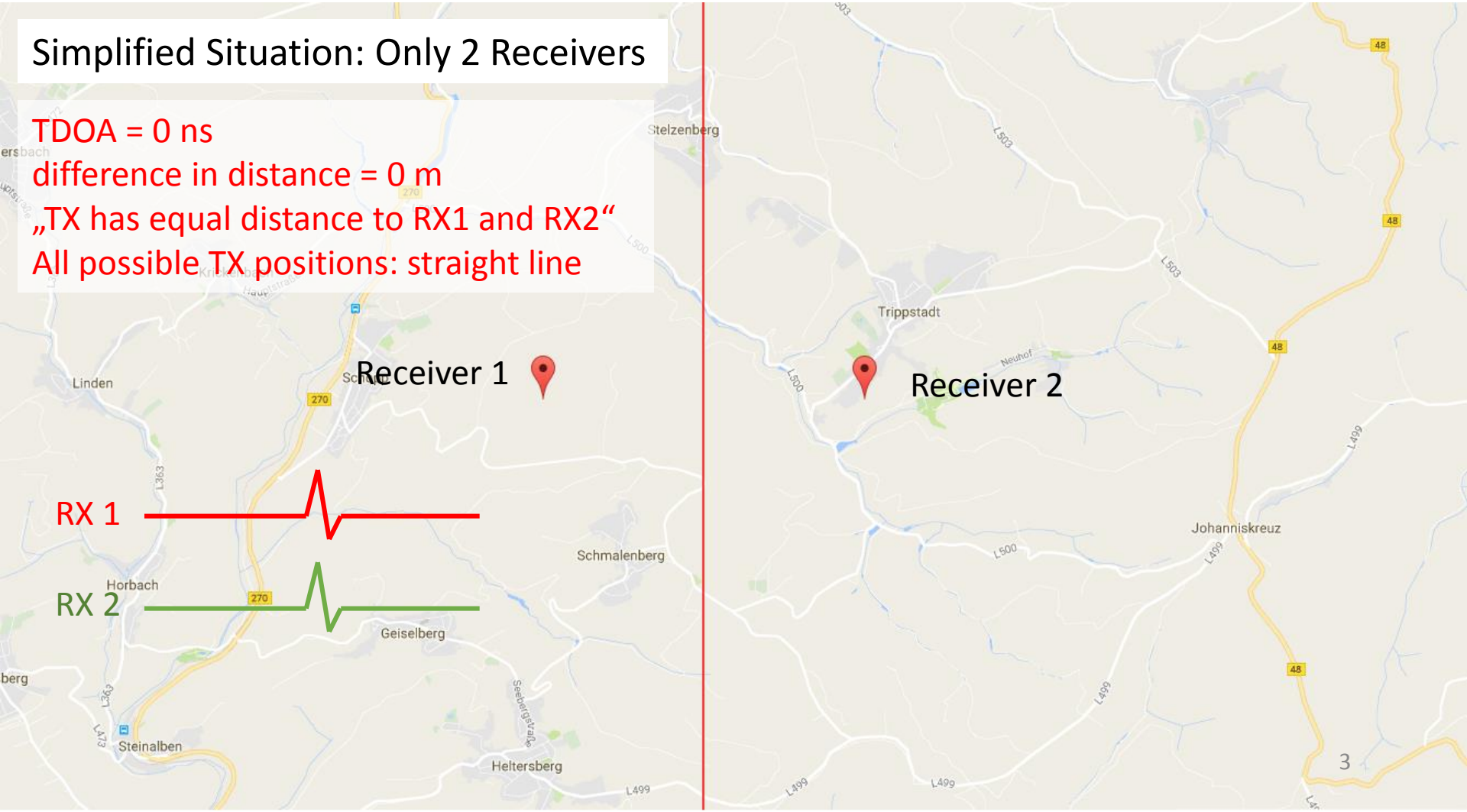




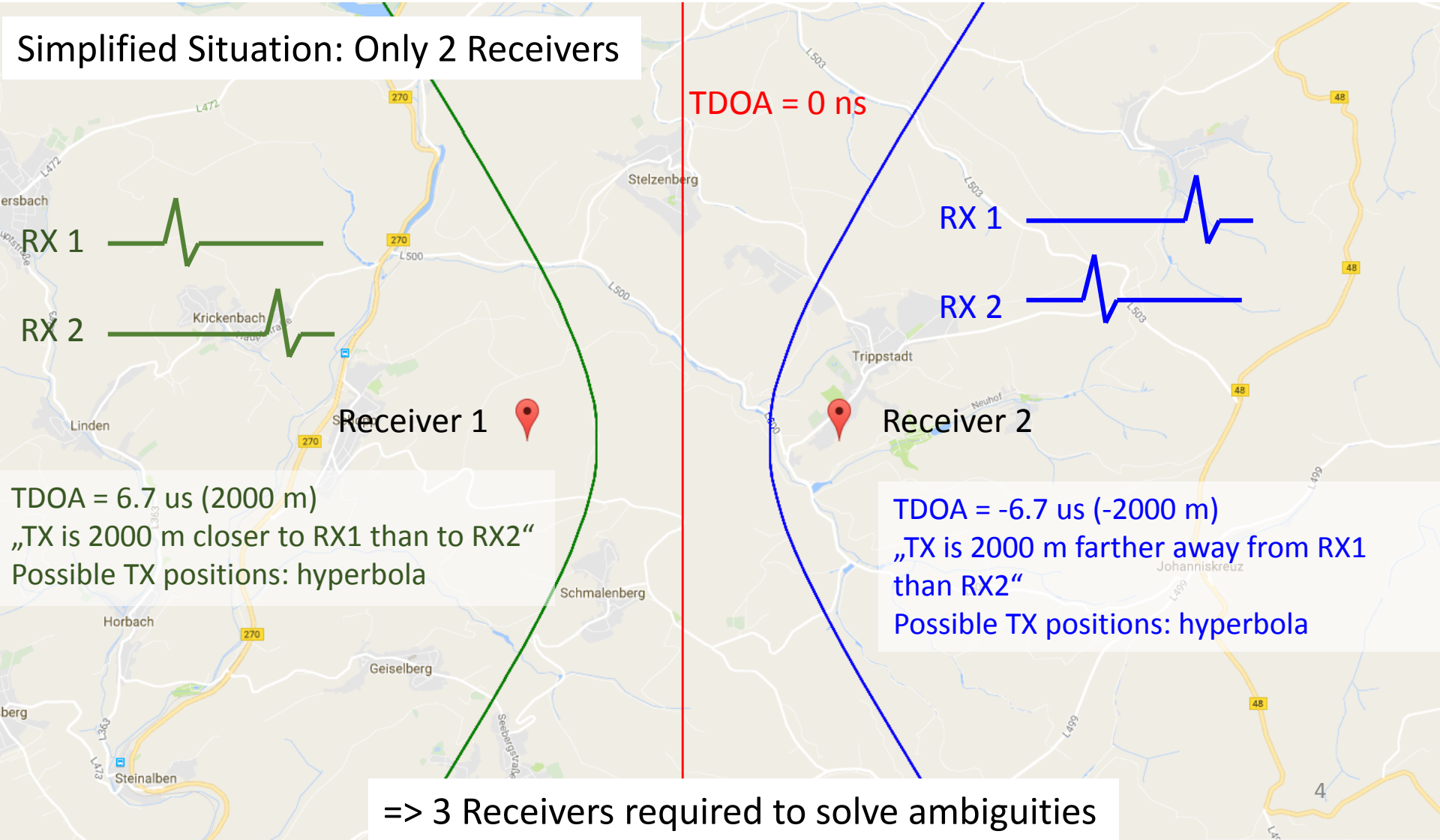
Multilateration: Basics

Simplified Situation: Only 2 Receivers

TDOA = 0 ns
difference in distance = 0 m
„TX has equal distance to RX1 and RX2“
All possible TX positions: straight line

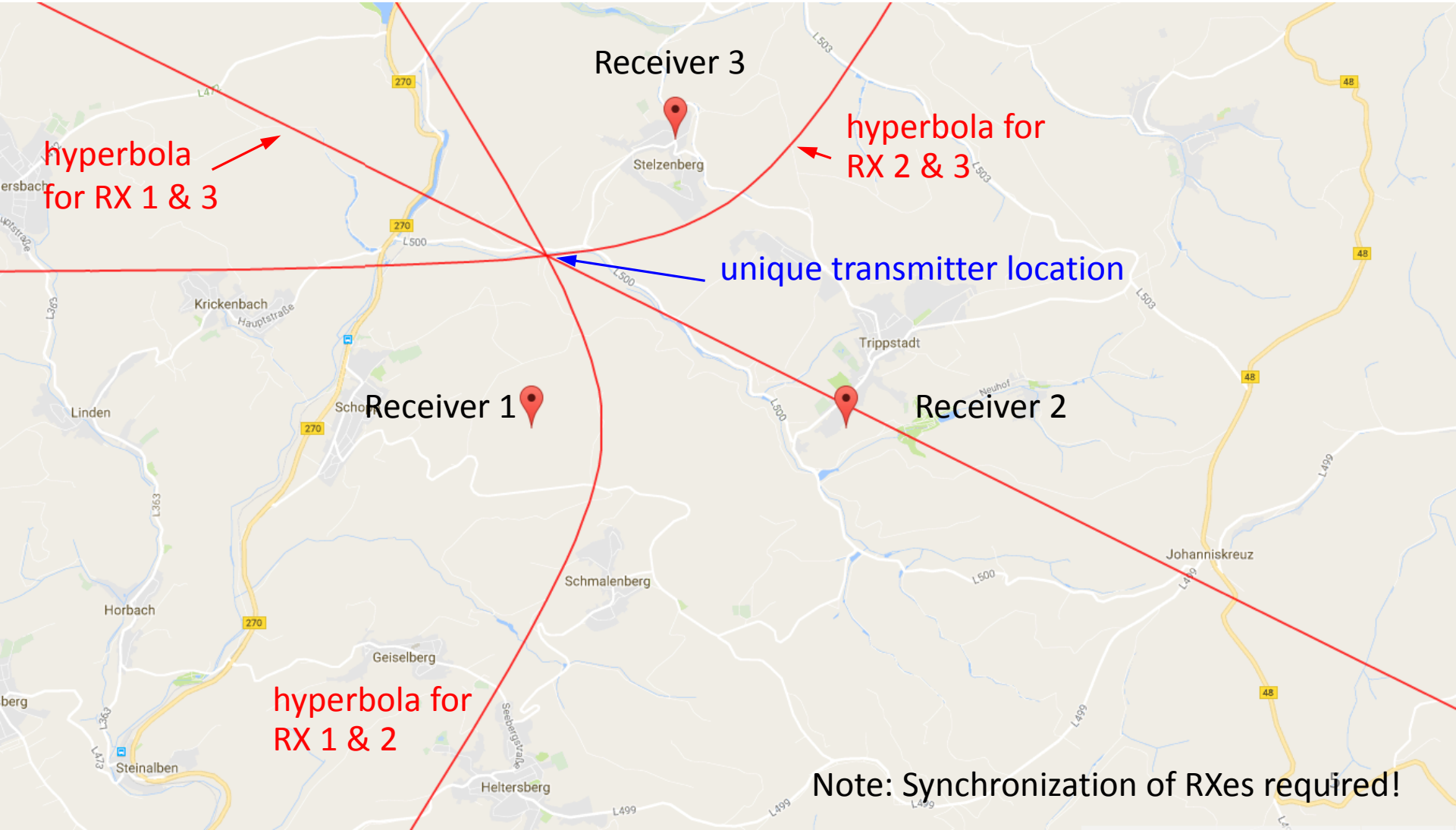


Multilateration: Basics



Multilateration: Basics

Full system with 3 receivers



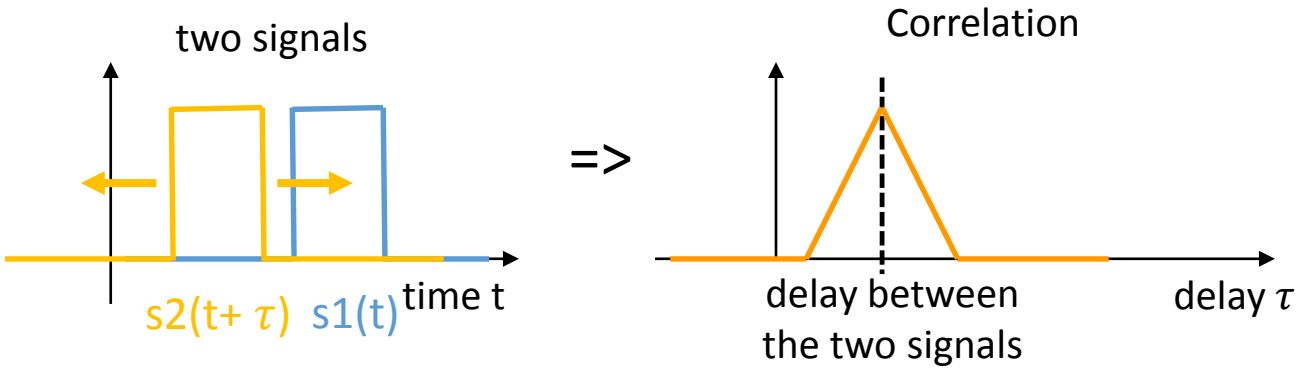
Delay Measurement

- How to measure delay between two signals?
- **Correlation function**

$$Corr(\tau) = \sum_{t=0}^{N-1} s_1(t)s_2(t+\tau)$$

s1(t), s2(t): received signals by RX1 and 2

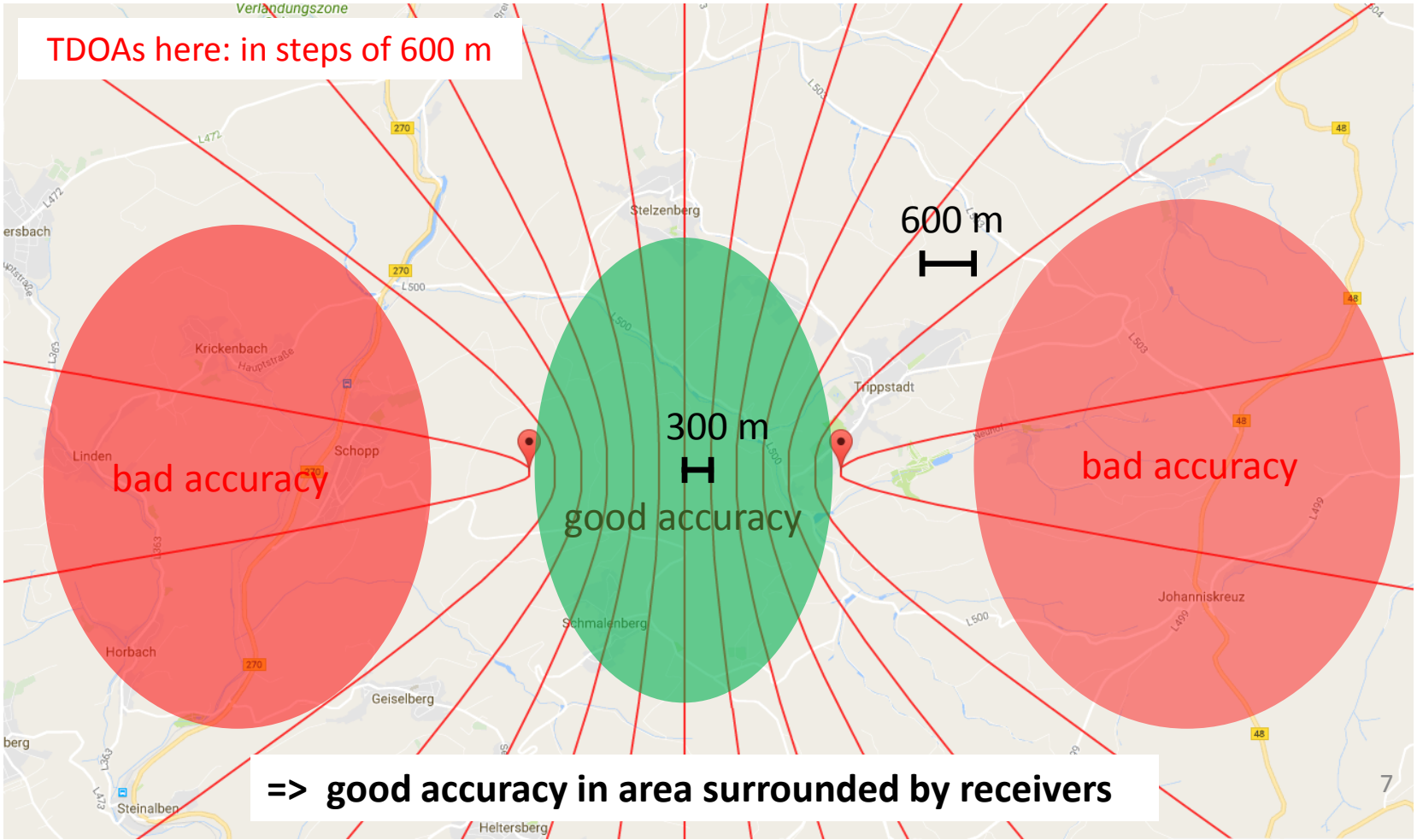
- „Tries every possible delay and records how good the signals match“
- Example:



- Peak -> best match, most likely delay

Resolution Analysis

Resolution of delay measurement ≠ Resolution of localization on map!



Summary on Basics

- Theory:
  - TDOA analyzes time differences of signal arrival
  - requires 3 synchronized receivers
  - difference /delay measurement with correlation
  - good accuracy in area surrounded by RXes

NEXT:

- Praxis:
  - How to build a real system
  - Receiver setup, synchronization and connection
  - Signal processing
  - Results

Low Cost TDOA System: Overview

- Goal: Localize transmitter in the city of Kaiserslautern, Germany, with simple system

- 3 Simple Receivers
  - Raspberry PI + RTL-Stick
  - simple antenna
  - antenna indoor
  - correct frequency with „kalibrate-rtl“ (using GSM channel)
  - newer versions of RTL-SDR: better frequency stability

- RTL-SDR Properties
  - receives any signals from 70 MHz to >1 GHz
  - bandwidth 2 MHz
  - achievable resolution for *delay measurement*

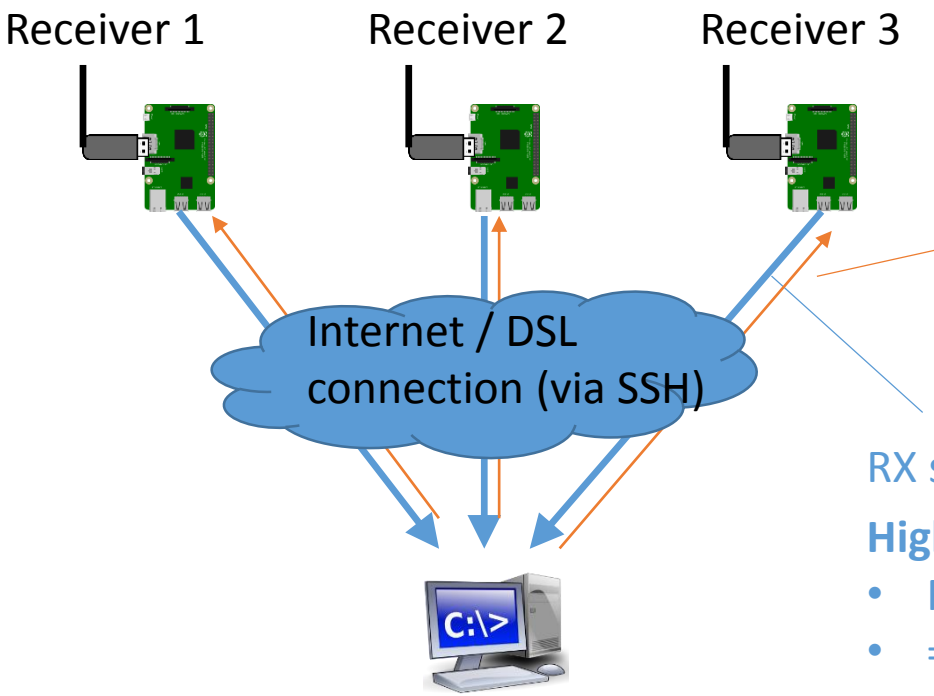
    2 MHz sampling => 500 ns * 3e8 m/s = 150 m

Low Cost TDOA System: Receiver Placement

- standard indoor antenna
- suboptimal placement in city

-> **very simple setup**

Low Cost TDOA System: Infrastructure



Master PC for RX control and (offline) signal processing

Master triggers reception at all RX

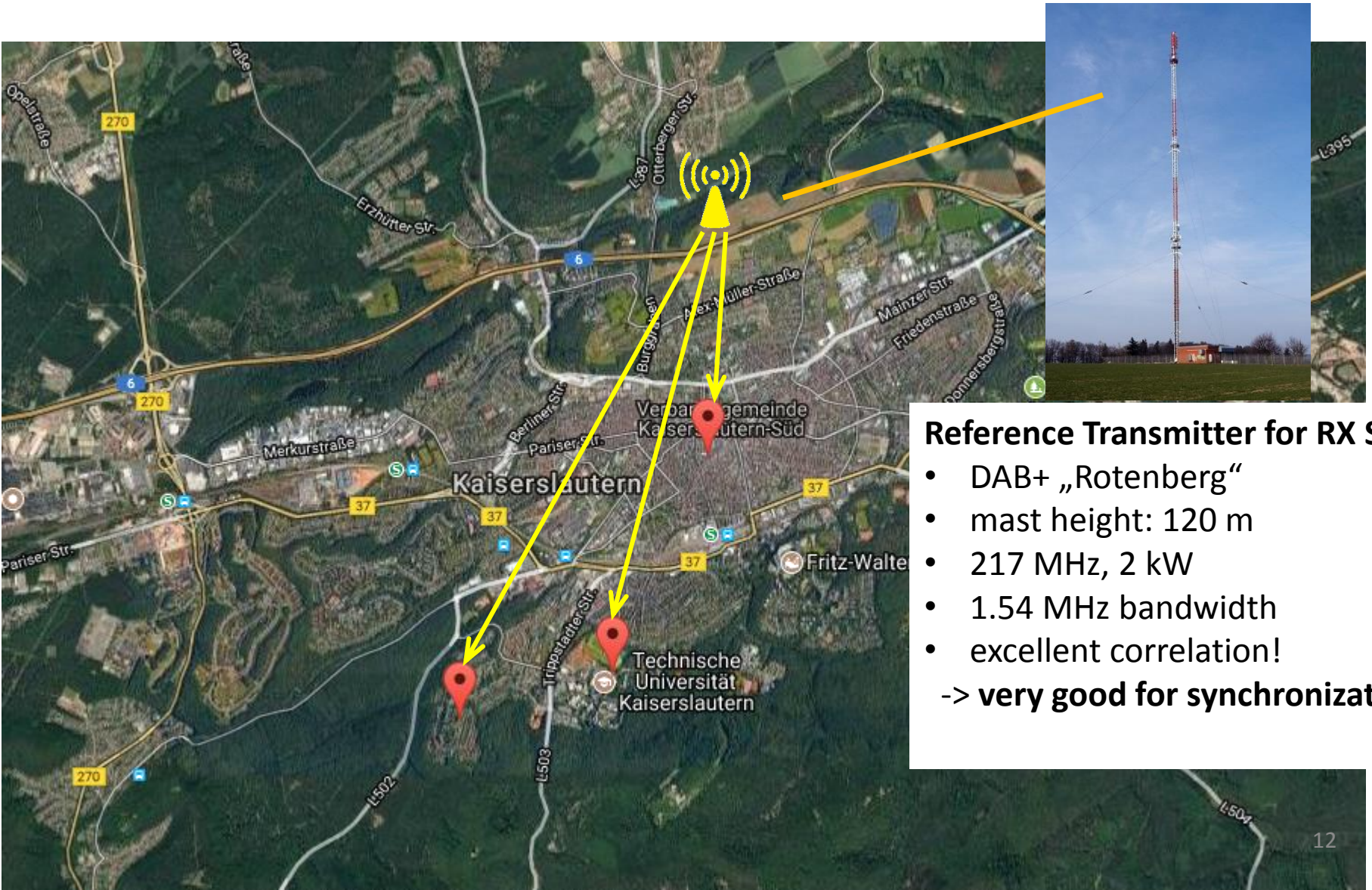
RX send back received data

High Data Rate Challenge:

- RTL SDR: 8 Bit IQ, 2 MHz
- => 16 Bit x 2 MHz = 32 Mbit/s
- our available DSL upload: max. 1 Mbit/s

- 1s recording takes approx. 1/2 min to copy

Low Cost TDOA System: Synchronization



Reference Transmitter for RX Sync

- DAB+ „Rotenberg“
- mast height: 120 m
- 217 MHz, 2 kW
- 1.54 MHz bandwidth
- excellent correlation!

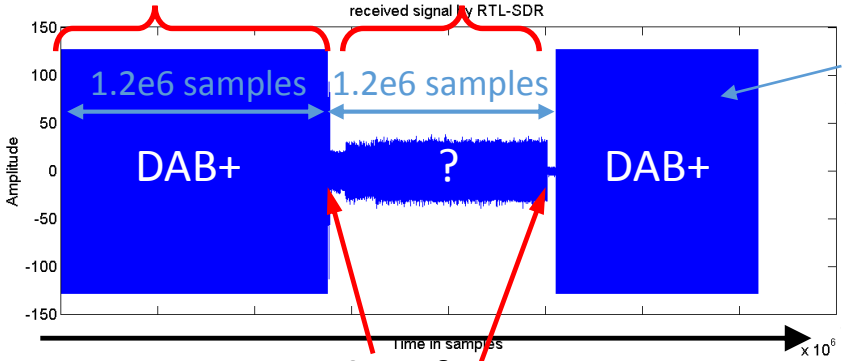
-> **very good for synchronization**

Low Cost TDOA System: Synchronization

reference signal for synchronization

unknown signal to localize

Reception at each receiver



optional:
for checking synchronization
or re-synchronization

seamless frequency switching required!

time

Synchronization:

1. start reception at RXes roughly the same point in time
2. align received signals along reference signal (+ known delay to reference TX)

-> Received signals get synchronized, not the RXes themselves!

Is seamless switching possible with the RTL-SDR?

librtlsdr (c lib to talk to RTl-SDR) crashed, when modified to switch frequencies during reception

Yes! Solution:

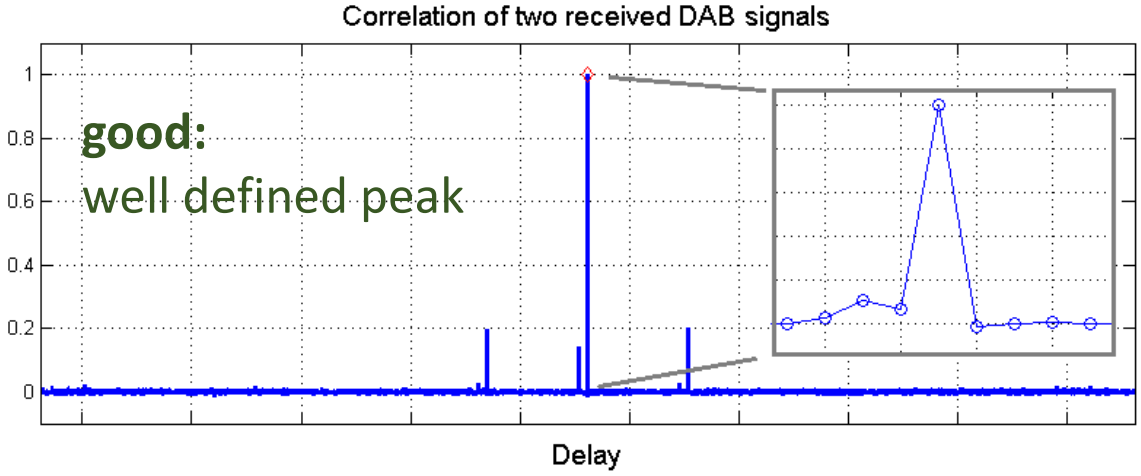
use branch async-rearrangements, https://github.com/mutability/librtlsdr/tree/async-rearrangements

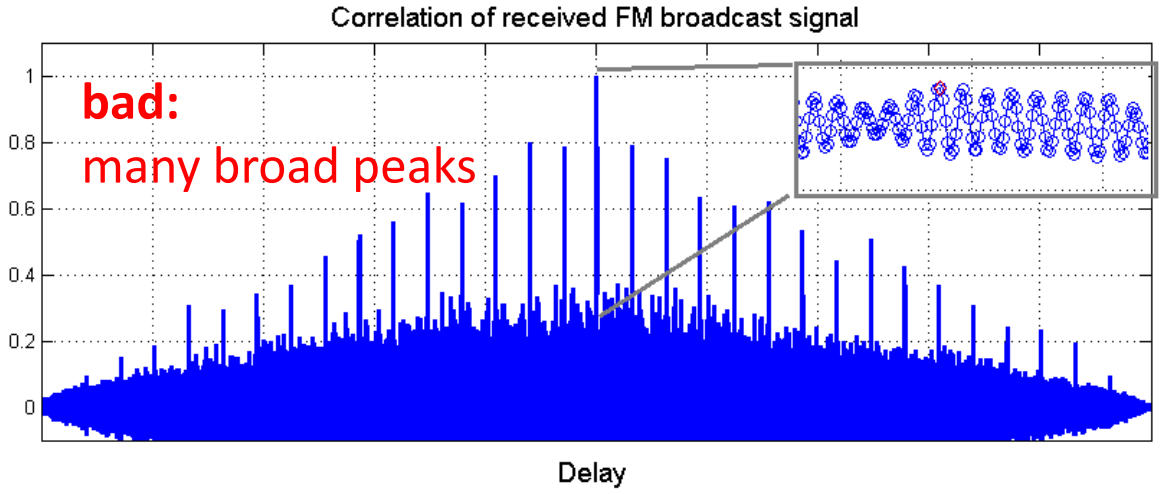
Seamless switching works perfectly fine:

Download of modified lib at: http://www.panoradio-sdr.de/tdoa-transmitter-localization-with-rtl-sdrs/

Correlation of Real Signals

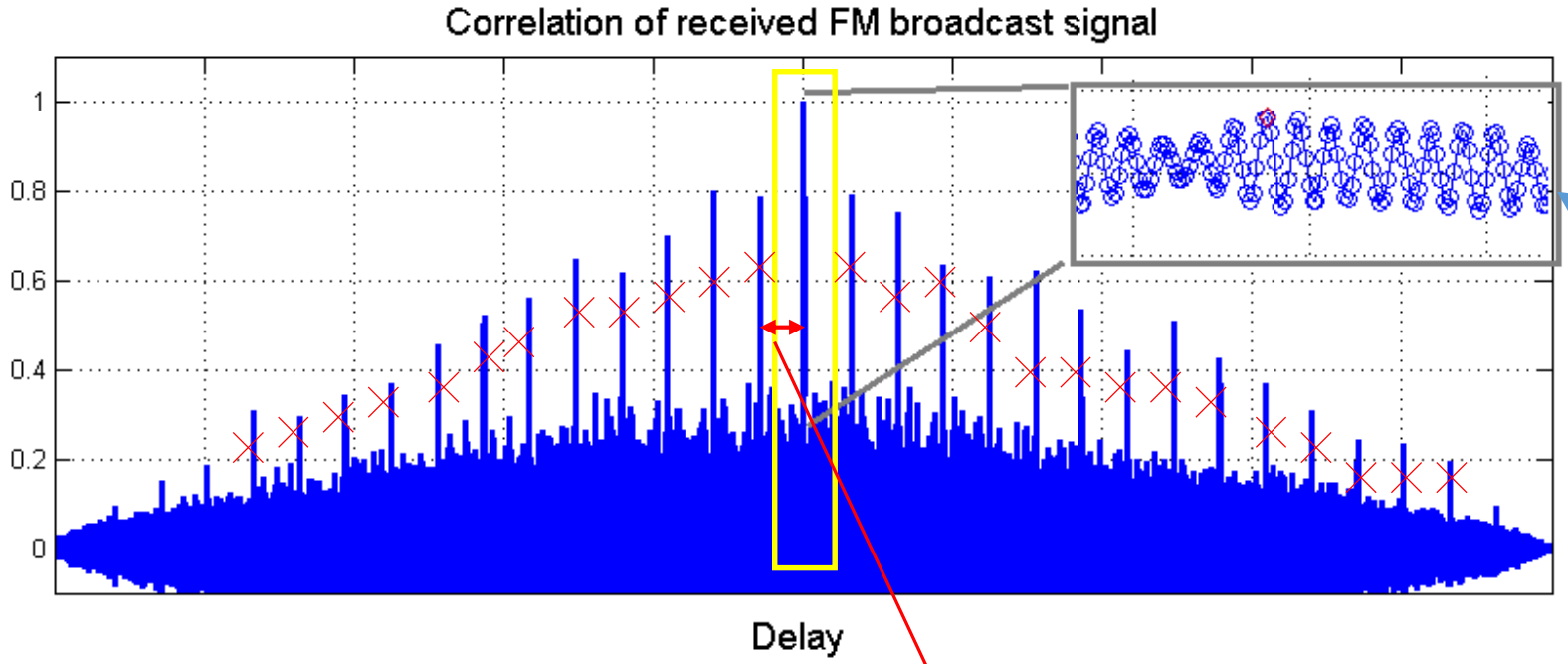
Real signals received by 2 RTL-SDRs at different locations





- Quality of correlation dependens on
  - Noise / SNR
  - Signal length
  - Signal bandwidth
  - Multi-Path Propagation
  - Signal content !
- Correlation may have:
  - multiple ambiguous peaks
  - no distinct peaks

Improvements On Correlation



use smoothing to determine precise peak

- any peak could be the true delay!
- **Analyse absolute delay values:**

  delay between peaks: here 61.000 samples = 9150 km,

  max possible TDOA is distance between RXes, here a few kilometers!

Signal Processing

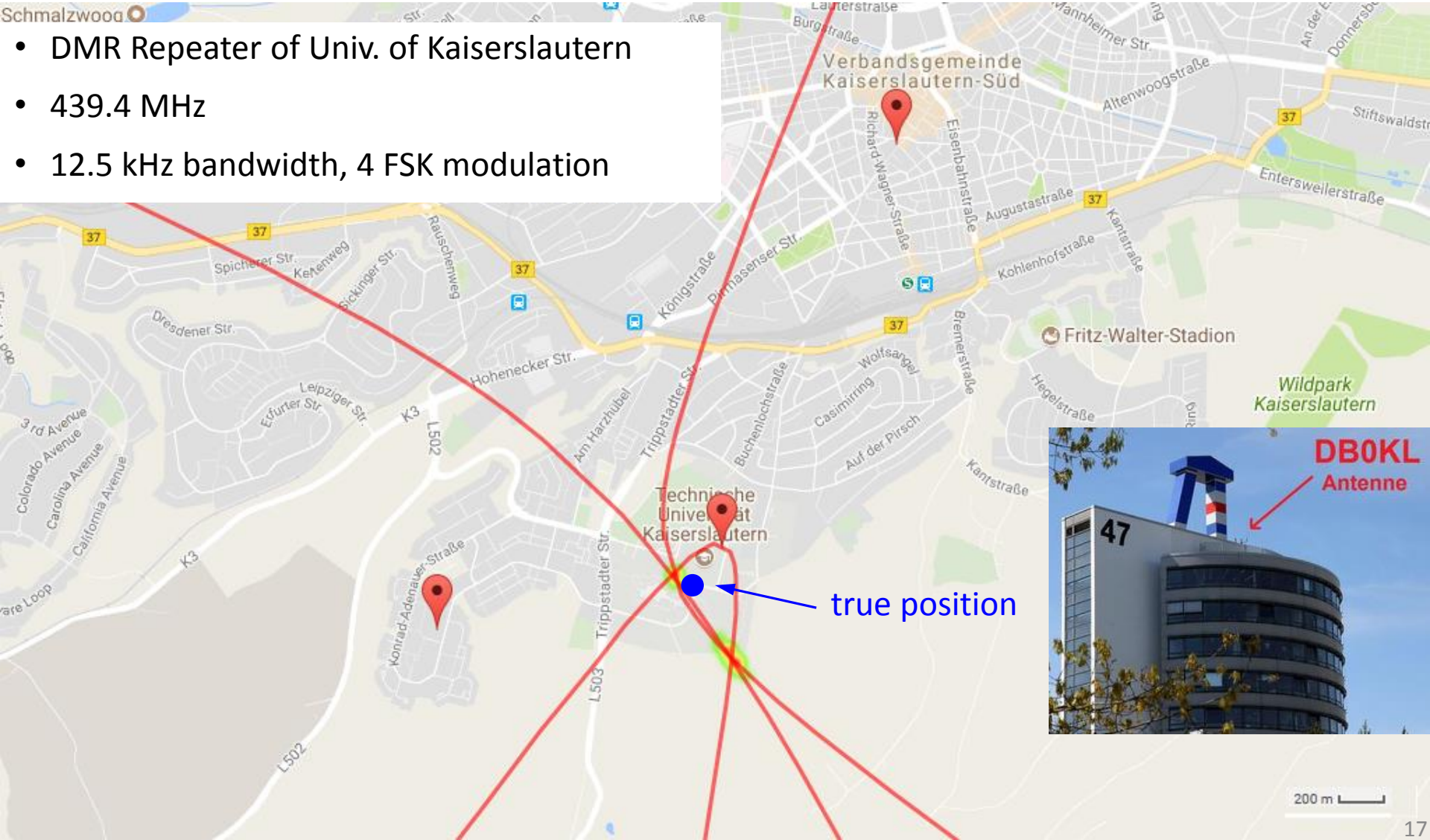
- Matlab script running on Master PC
- consider receptions pairwise to create a hyperbola

---

1. receive signals & send to master
2. synchronize RXs:
    - interpolate reference signals (optional)
    - calculate correlation (dphase or abs)
    - discard invalid peaks of correlation function
    - use measured delay to synchronize
3. measure unknown signals
    - interpolate signals (optional)
    - correlation (dphase or abs)
    - discard invalid peaks of correlation function
    - determine TDOA in samples and distance
4. calculate hyperbola using geometry
5. create a html / javascript file for google maps to display results

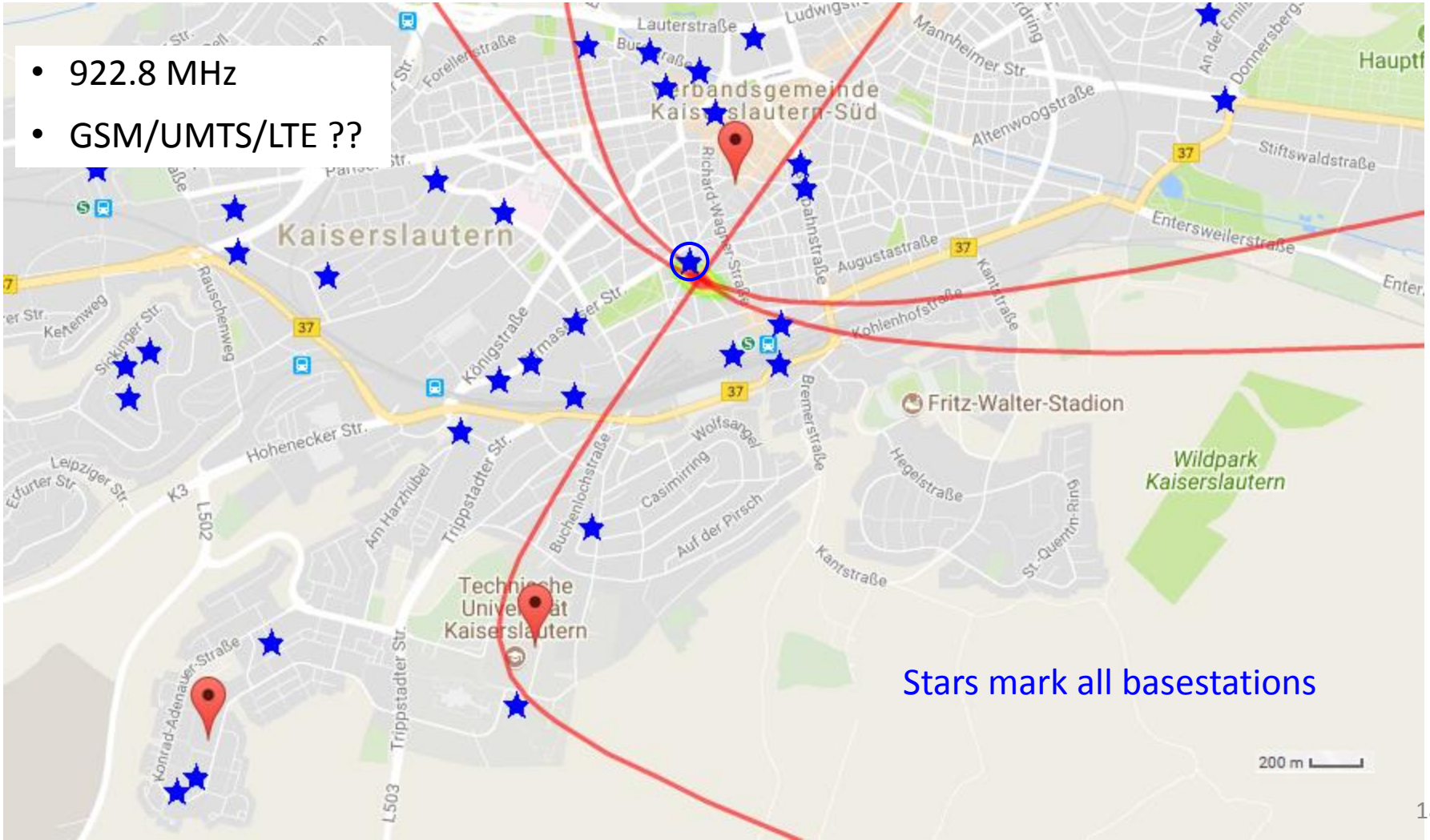
Results: 70cm DMR Repeater

- DMR Repeater of Univ. of Kaiserslautern
- 439.4 MHz
- 12.5 kHz bandwidth, 4 FSK modulation



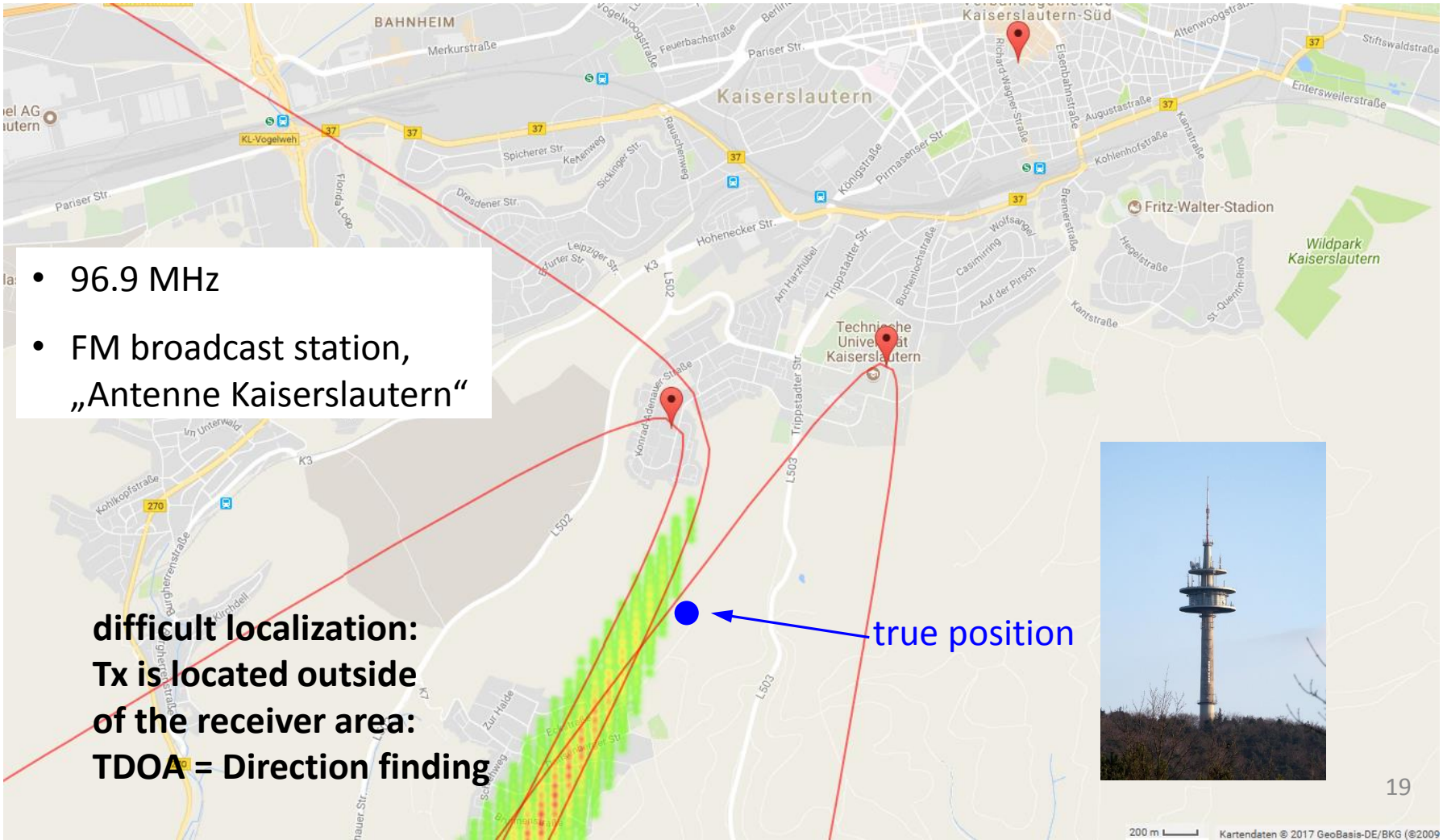
Results: mobile telephony

- 922.8 MHz
- GSM/UMTS/LTE ??



Stars mark all basestations

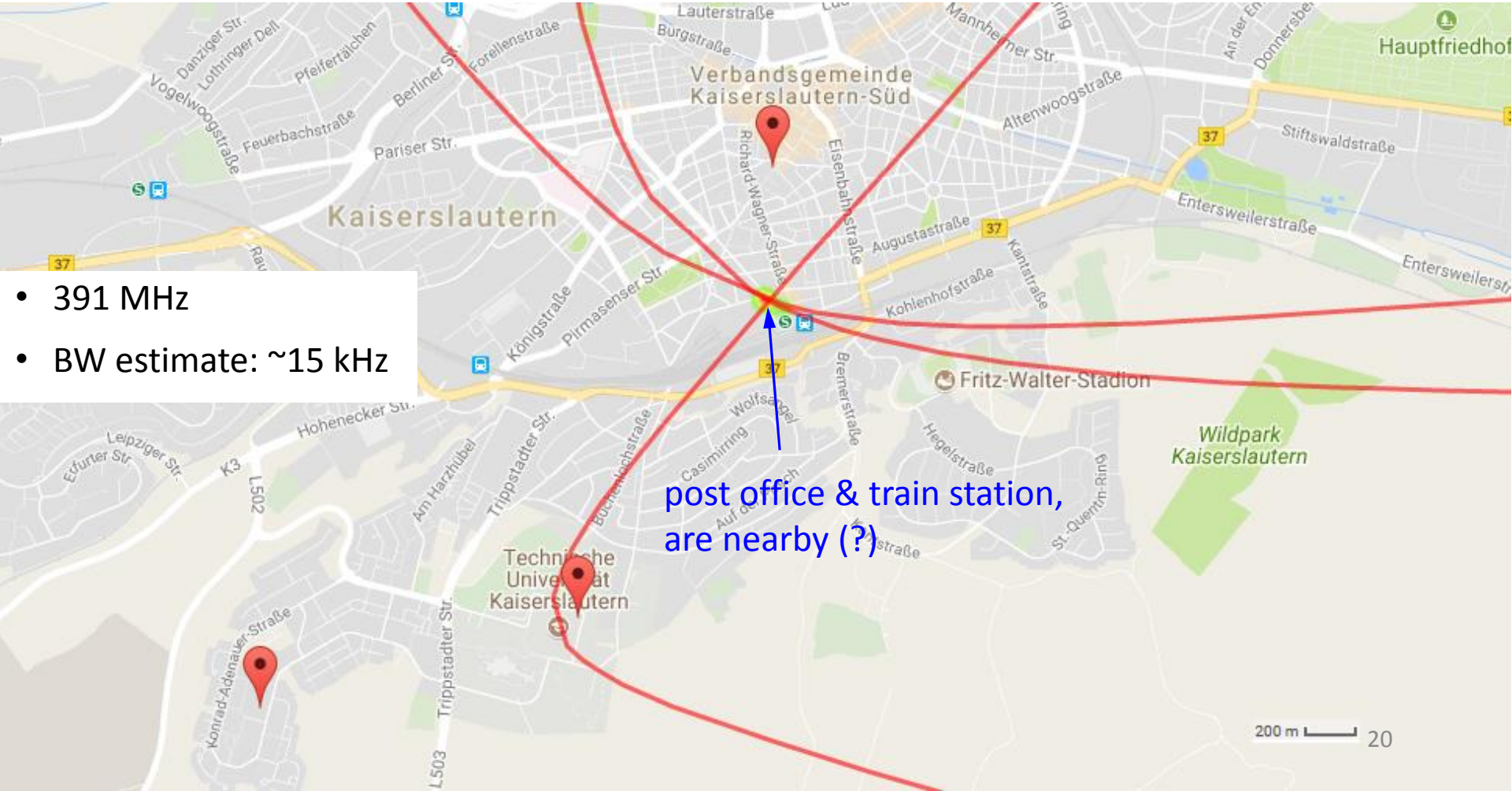
Results: FM broadcasting



- 96.9 MHz
- FM broadcast station, „Antenne Kaiserslautern“

difficult localization:
Tx is located outside
of the receiver area:
TDOA = Direction finding

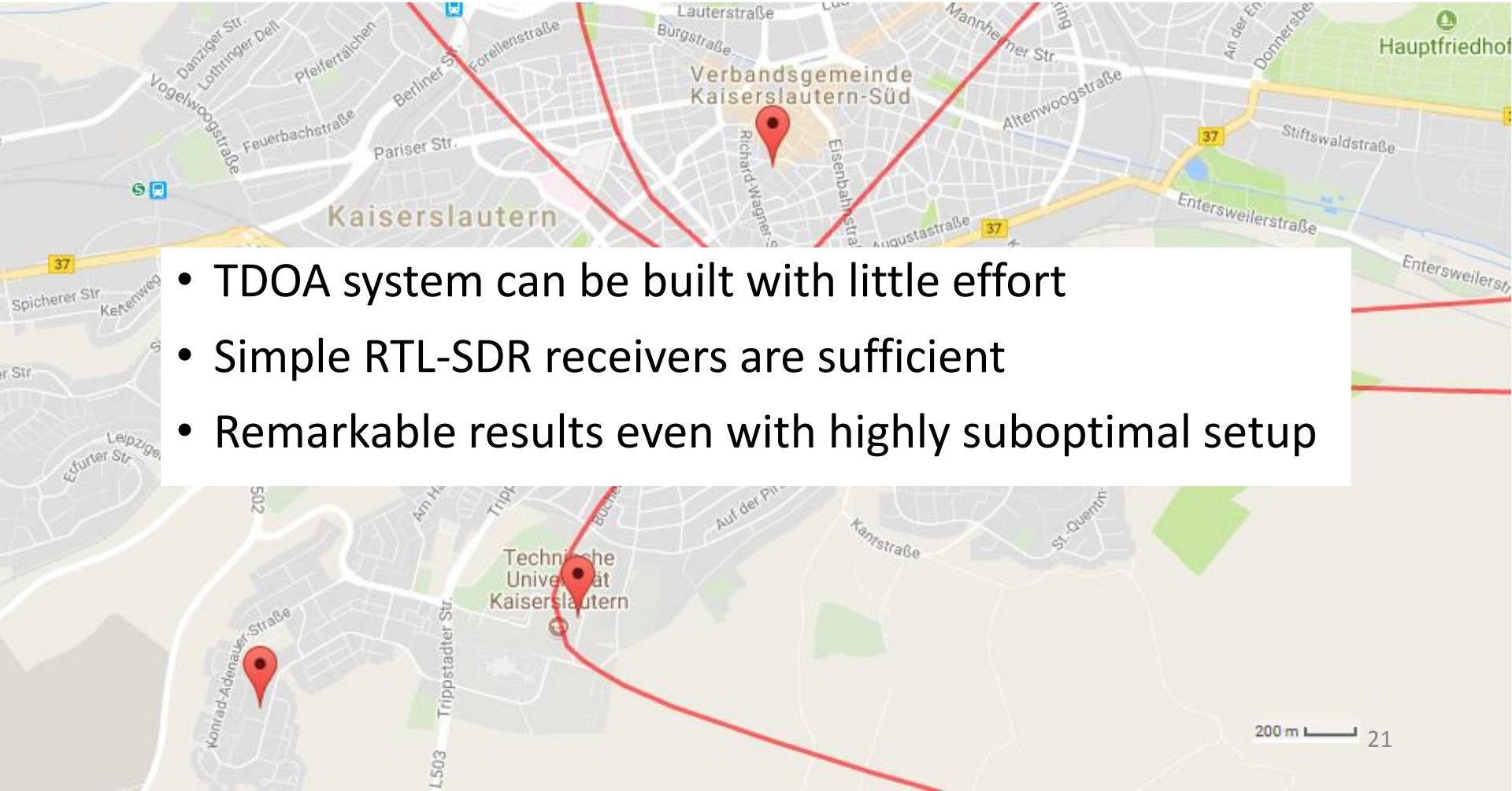
Results: unknown signal



- 391 MHz
- BW estimate: ~15 kHz

post office & train station,
are nearby (?)

Summary



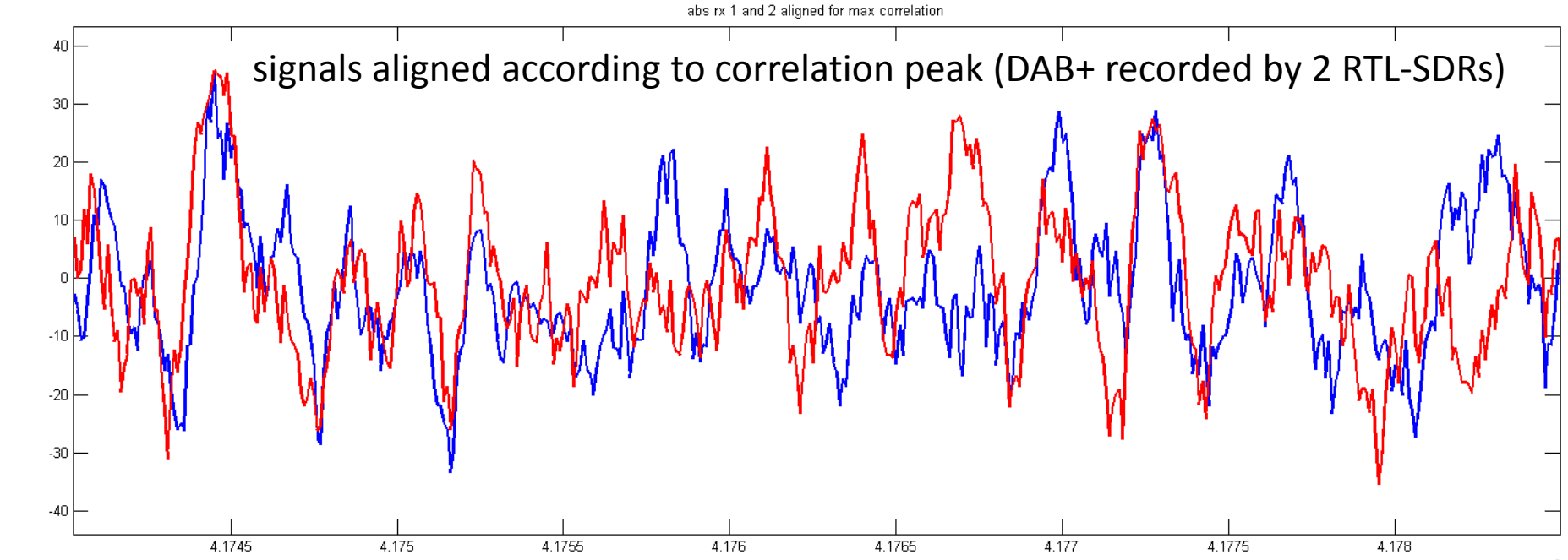
- TDOA system can be built with little effort
- Simple RTL-SDR receivers are sufficient
- Remarkable results even with highly suboptimal setup

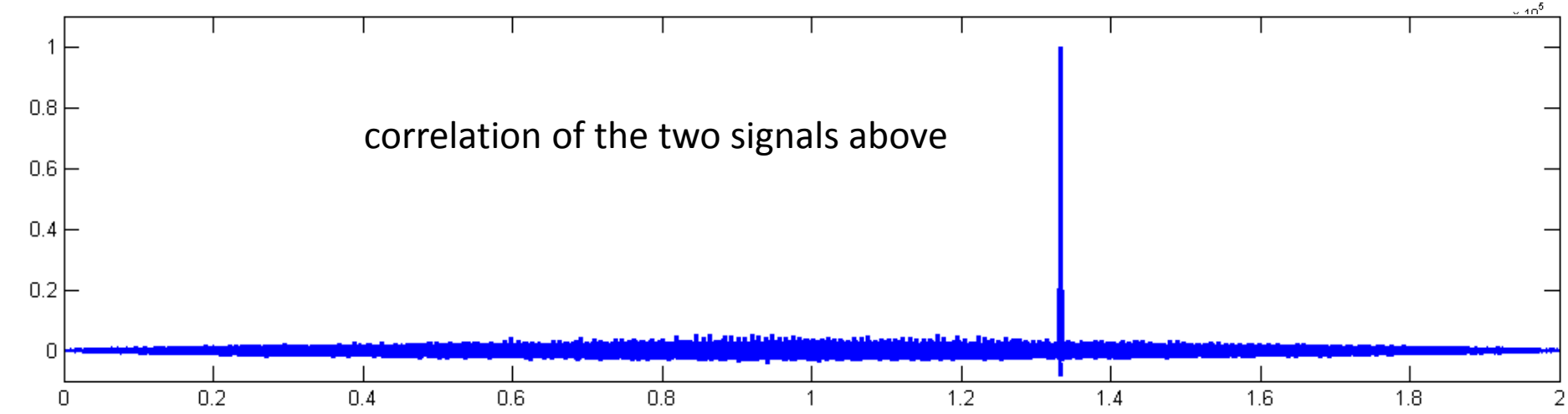
Further information and project files available:

http://www.panoradio-sdr.de/tdoa-transmitter-localization-with-rtl-sdrs/

Email: dc9st@panoradio-sdr.de

Correlation in Time Domain





Correlation for IQ signals

- Correlation function introduced for real signals
- RTL-SDR delivers I/Q outputs
- treat I/Q value as complex value: (I+j*Q)
- options for IQ correlation:
  - complex correlation
  - real correlation with abs(I+j*Q)
  - **real correlation with phase difference of (I+j*Q)**