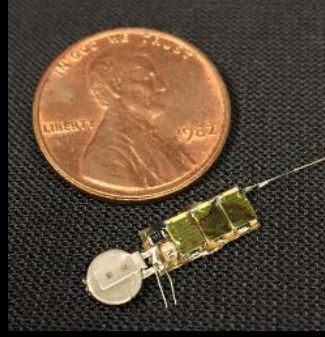
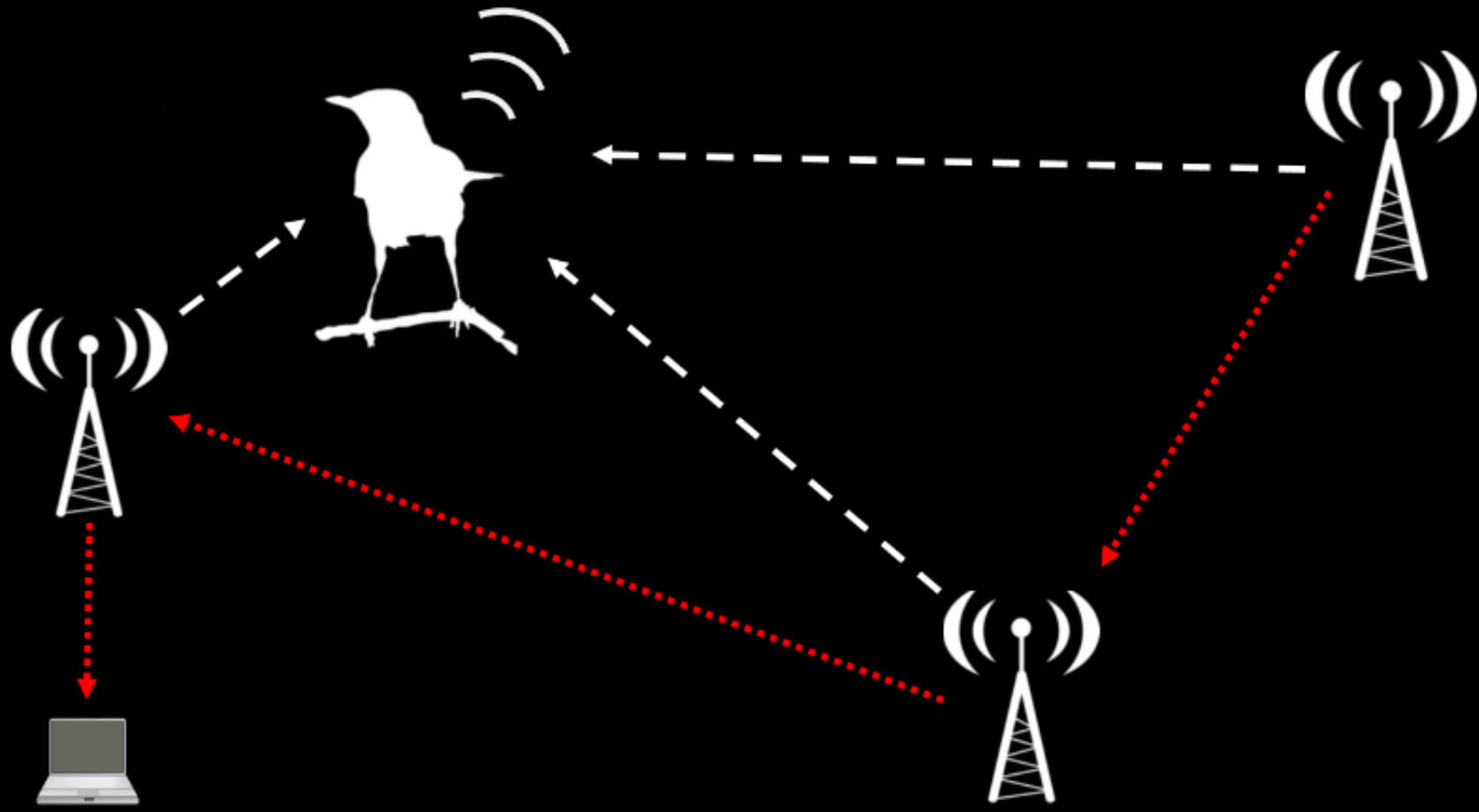
AMRUPT

(Animal Movement Research Using Phase-based Trilateration)



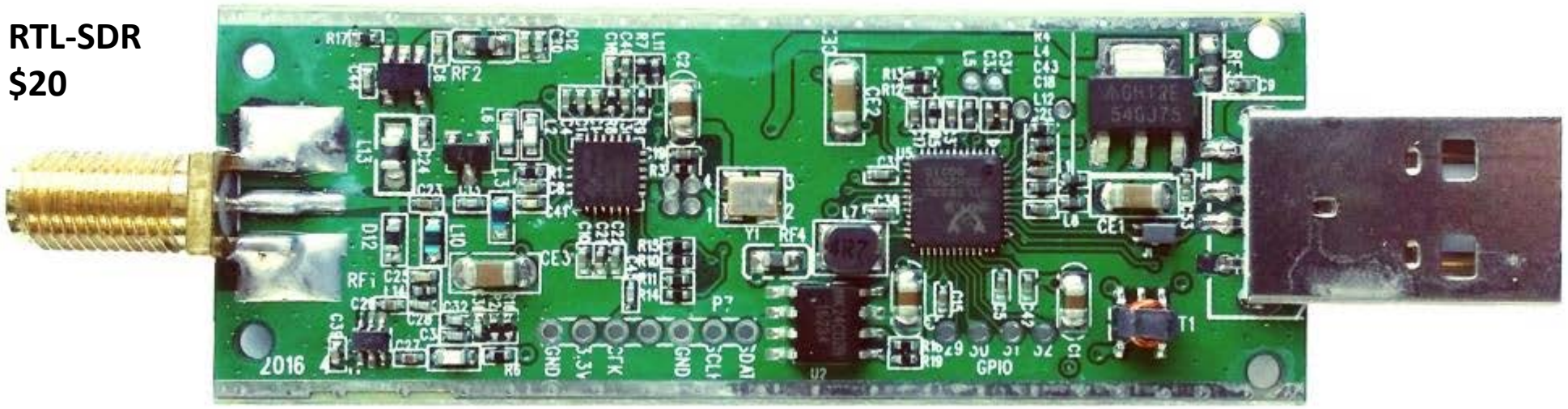


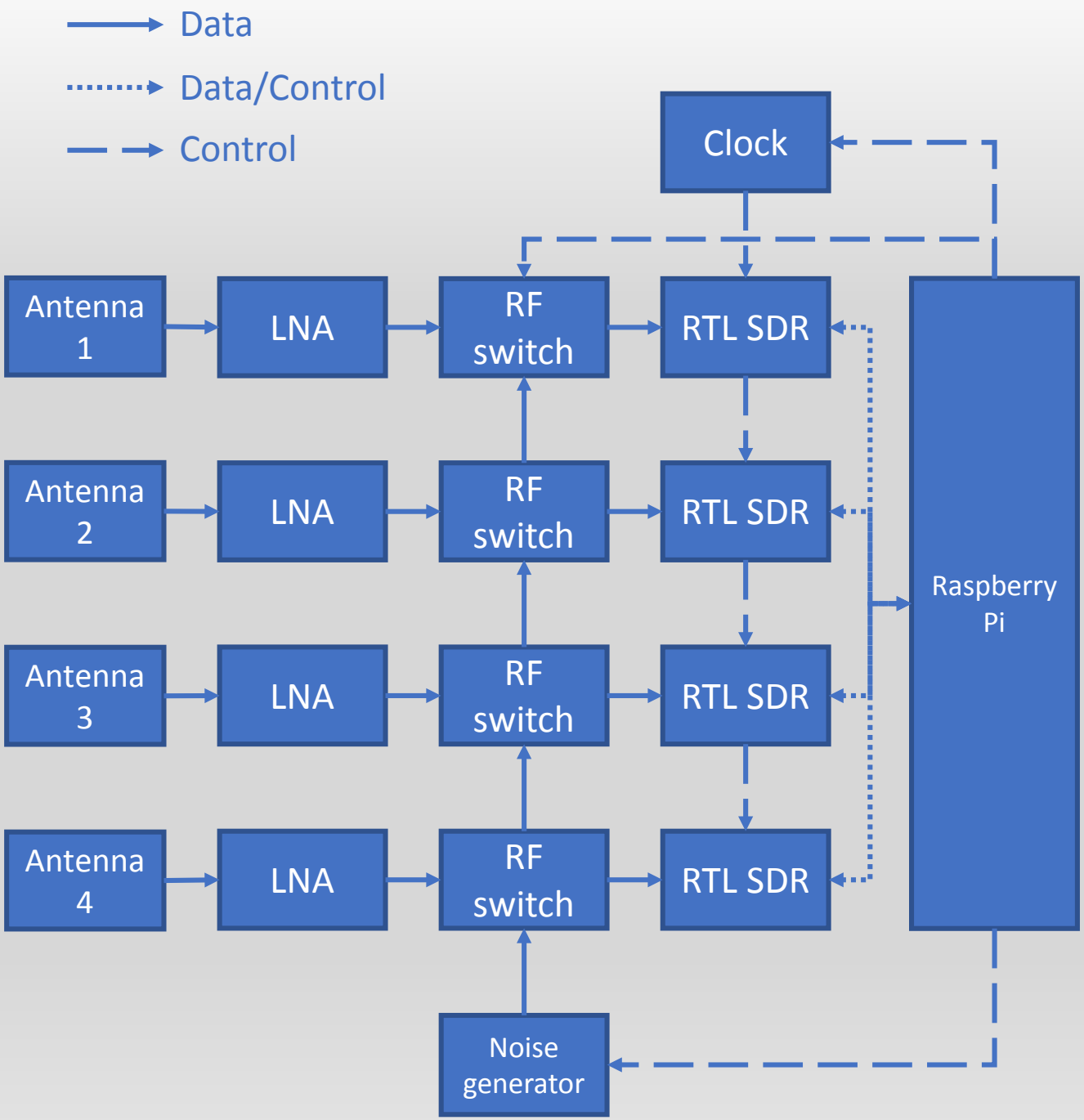
Technical Approach:
Receiver architecture

Will the CC1310 be sufficient for DF?

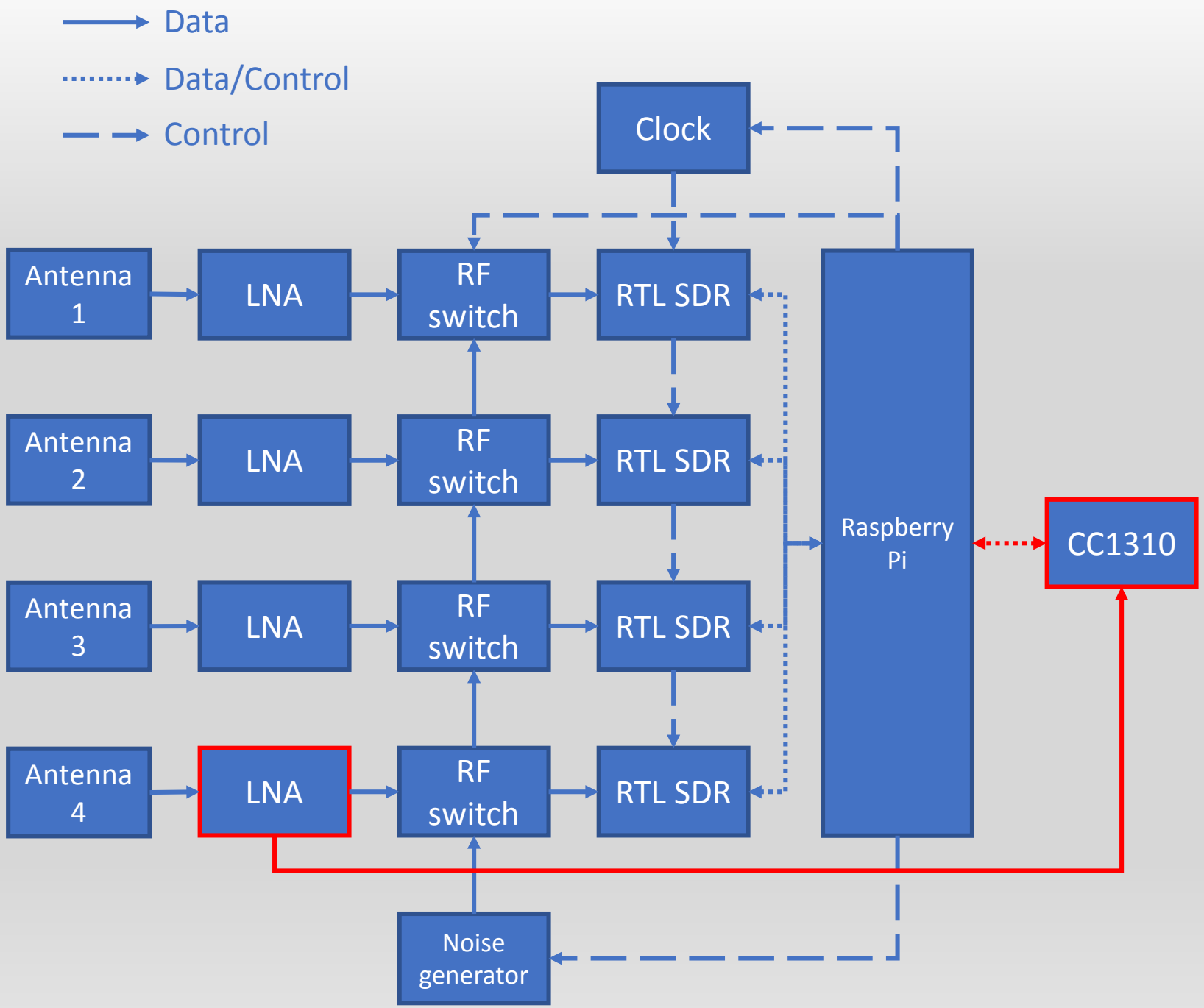
What about SDRs?

RTL-SDR
$20



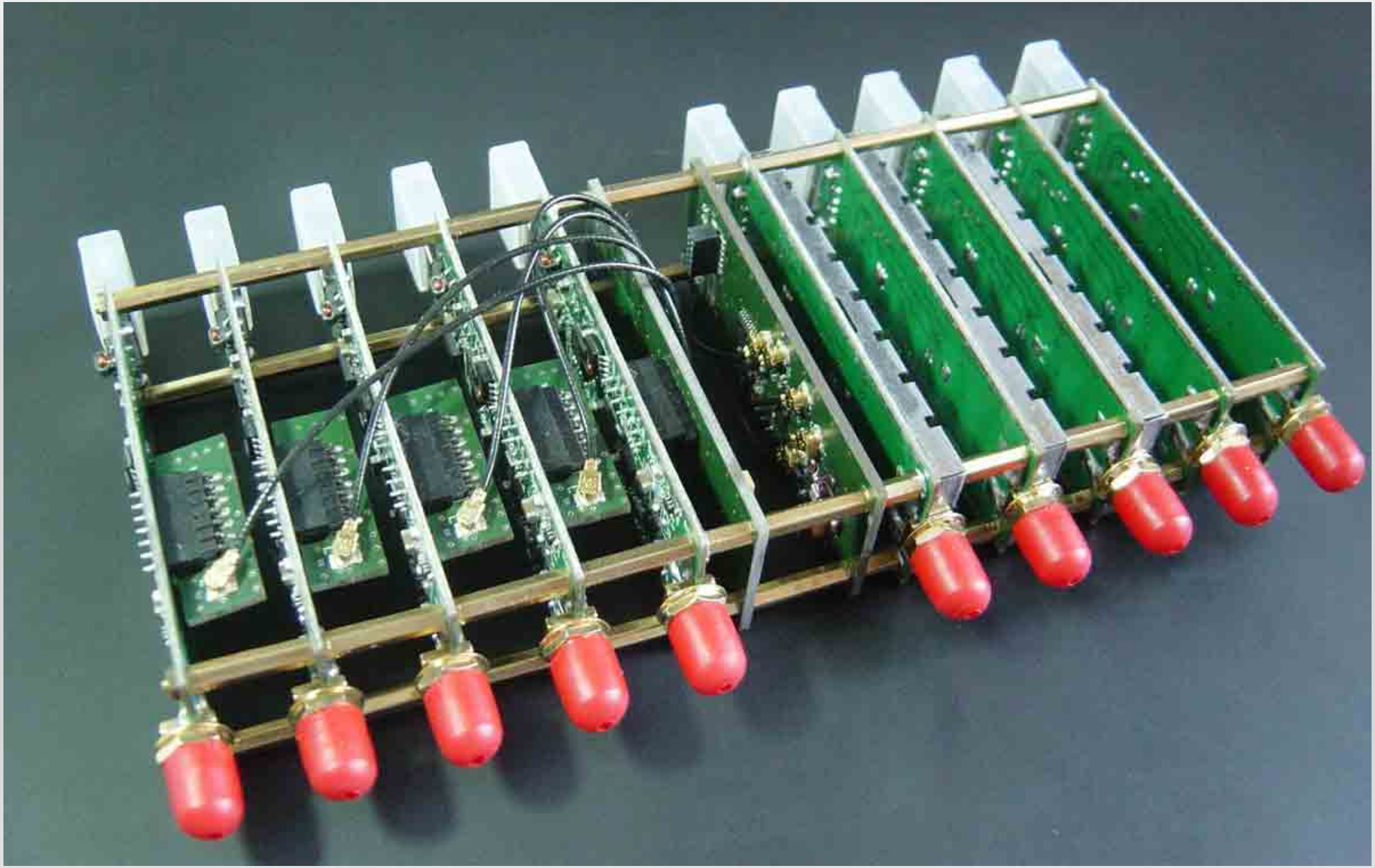


- 4 antennas – allows for Watson-Watt AOA measurement
- LNA – Improved SNR
- 4 RF switches and noise generator – switching in RF noise calibrates for initial phase offsets due to program execution differences
- RTL-SDR – cheap ($20) SDRs which can be synchronized with a common local oscillator, and fast I/Q sampling (2 Msps)
- Clock – dedicated board with highly stable (0.1 ppm) TCXO and enough drive strength for multiple SDRs, synchronize SDRs
- Raspberry Pi – cheap interface for DSP, and to control Clock, Noise generator, RF switches, and SDRs



What about transmitting commands to the mobile nodes?

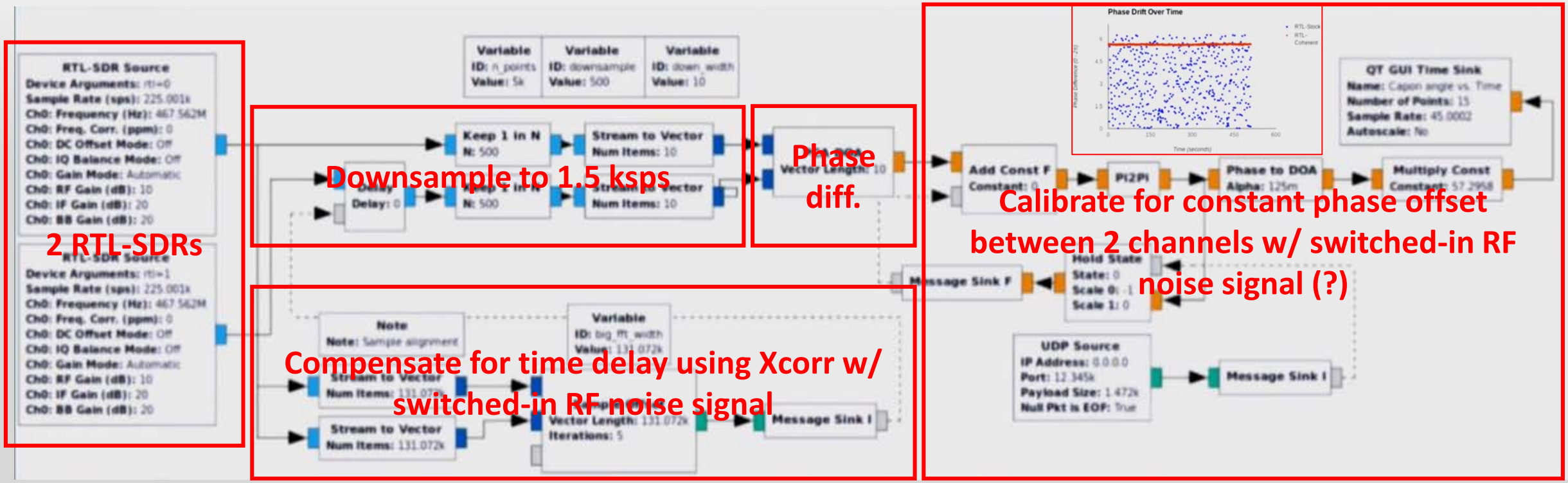
Boards available from www.coherent-receiver.com



Boards available from www.coherent-receiver.com

We must reverse-engineer and simplify design to reduce cost!!

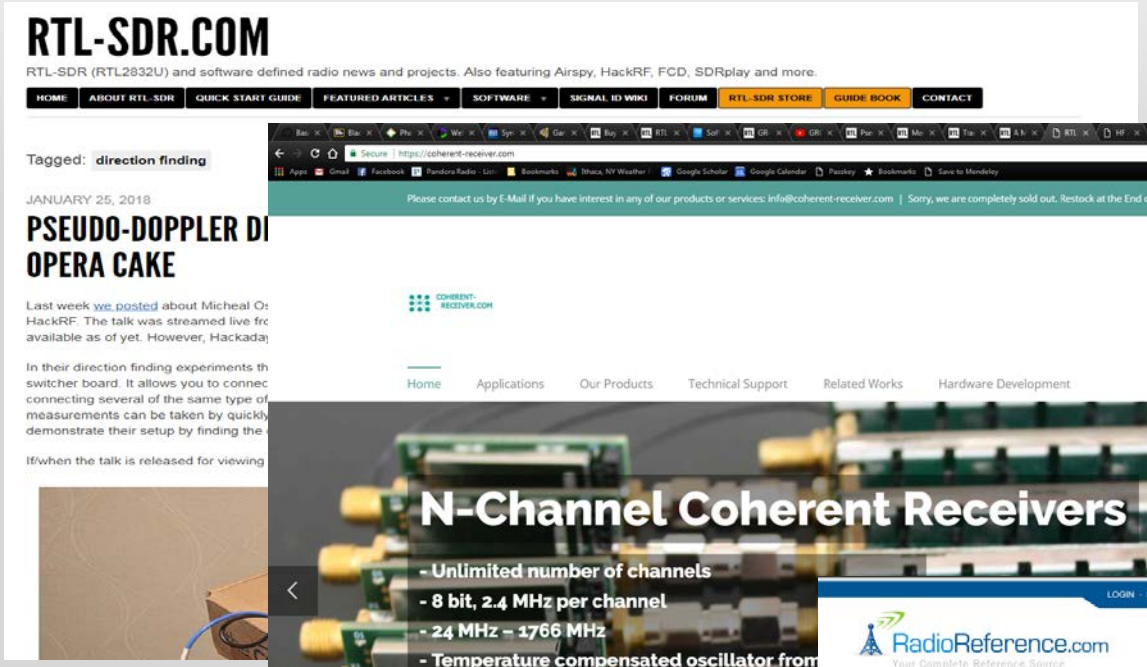
Software/DSP: GNU Radio

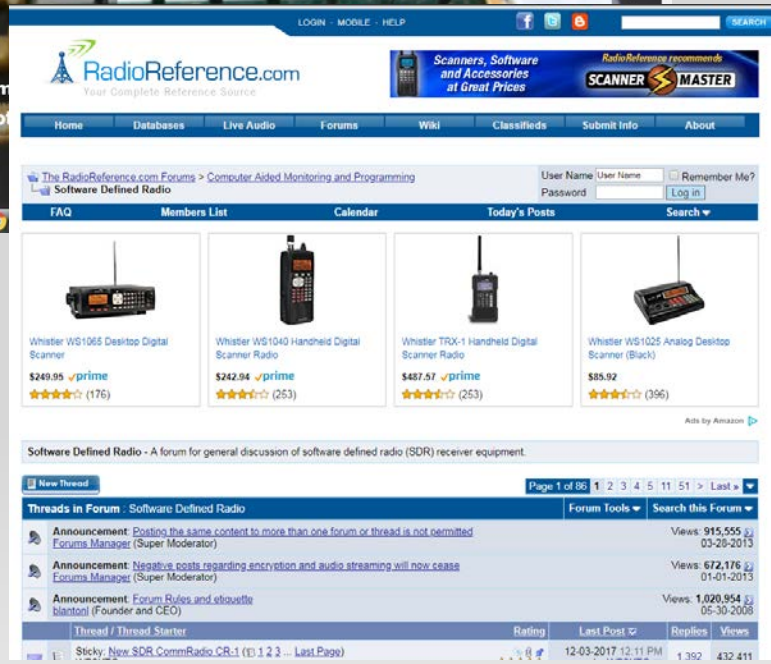


1. Use existing SDR hardware, rather than proprietary systems
2. Existing code blocks for high-level functionality
3. Simulate RF signals and signal processing
4. Create DSP algorithms for processing real output from RTL-SDR sources
5. Well supported, open-source, and free

Resources to jump-start our project

1. www.RTL-SDR.com
2. www.coherent-receiver.com





Coherent-receiver.com - provides support for RDF

Direction Finding

You can use a 4-channel Entry Level Receiver for these experiments (e.g. https://coherent-receiver.com/wp-content/uploads/2018/02/DirectionFindingSystem.jpg).

1. Identify all receivers and set custom serial numbers
2. Tune the supervisor to the FM-Station and test that it works
3. Connect the single channel receiver to the USB: you need to have connected following devices: noise generator; supervisor and single channel receiver
4. https://coherent-receiver.com/support; Please take a look at the section Management of the antenna switch and noise generator cards:
    - Try to switch the bias_tee on on the receiver. Bias_tee is the power supply of the antenna switch card (antenna switch does not work without power supply). You can use the existing program rtl_biast for this proposes
        - ON: rtl_biast -dX -b 1
        - OFF: rtl_biast -dX –b 0
    - X is the number of the dongle (0, 1, 2, 3); please note; the supervisor don't have the antenna switch but the command will work (it changes only the GPIO state)
    - As a result the led "software selectable bias_tee" must be switched on/off depending on the command
    - You do the same programmatically using the GPIO:
      // true – bias on; false – bias off
      setGPIOBit(handle, (byte) 0x01, true);
5. Switch the antenna switch between noise and antenna input; please see sections: "Antenna switch and noise generator card management" and "I2C and RTL2832U"

Communications with Coherent-Receiver.com

“I don’t think that the open sourcing will reduce the prices.

Initially, we developed this project for the commercial customer in order to improve the reception in the moving objects; the second idea was to use it in DRM30. Our public available realisation was made as flexible as possible incl. different components versions for various application scenarios, e.g. clock-card10 or clock-card 0.2/2. You can consider these products as development boards in order to test your ideas or make some research. These were not intended to be and are not the mass-market products.

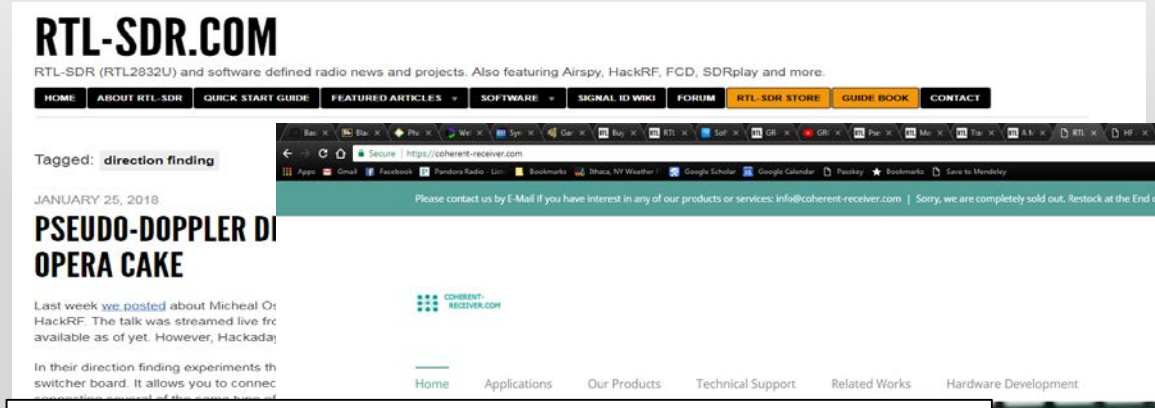
The design and realization for volume products (with cheaper prices) should be different. We designed such version for the above mentioned application scenario but cannot provide more details at the moment.

We provide the detailed description about the public available products. Moreover, you can ask the technical questions that we will try to answer.”

Resources to jump-start our project

1. www.RTL-SDR.com
2. www.coherent-receiver.com
3. www.radioreference.com
4. GitHub repositories:
   - RTL-Coherent
   - Multi-RTL
   - Gnuradio-doa (video)
   - Thrifty

System compatible with TDOA or TDOA/AOA-hybrid approaches



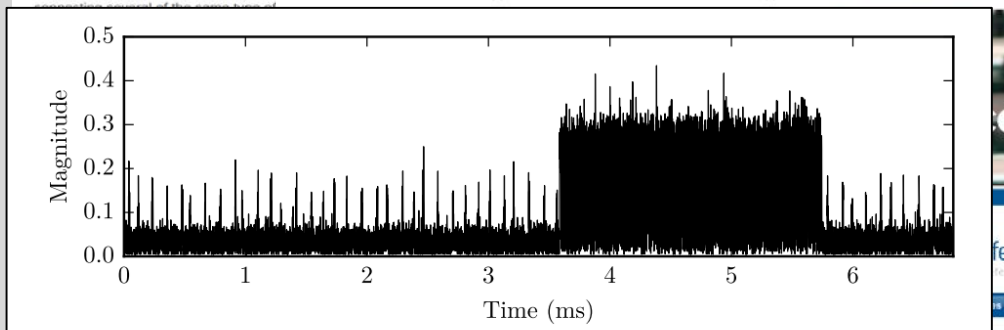


Figure 6.3: Magnitude of the time-domain samples after carrier frequency recovery.

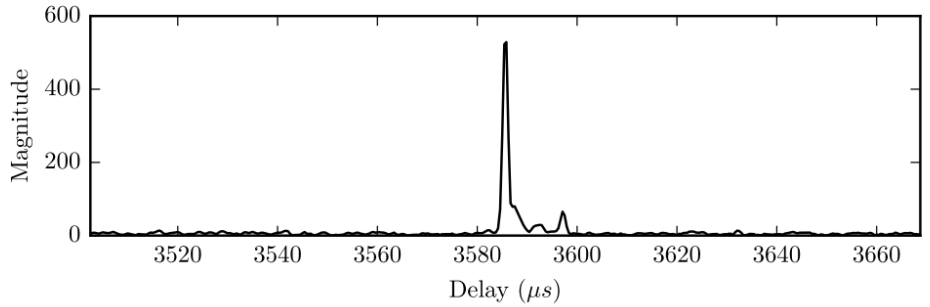
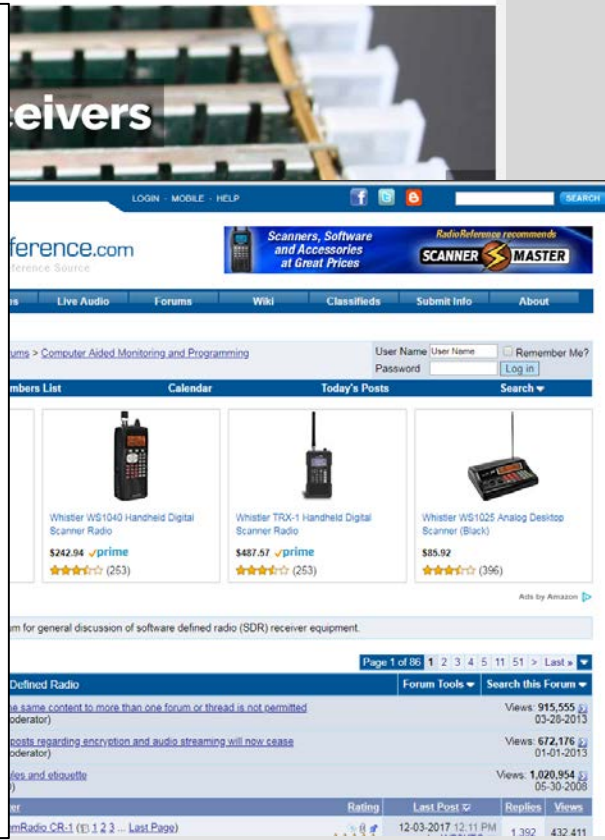


Figure 6.4: Extract from the correlator output showcasing the distinct correlation peak and a few multipath components.



Where to go from here?

- Review existing SDR DF designs
- Learn about (and test-drive) GNU Radio Companion
- Continue to formulate specific questions for Dr. Kan and his students for next week's meeting with him, focusing on evaluating the compatibility of SDRs with his approach
- Finish up proposal revisions, incorporating SDR approach

❑ Don't forget to update timeline with realistic milestones!

The RTL2832 SDR Dongle

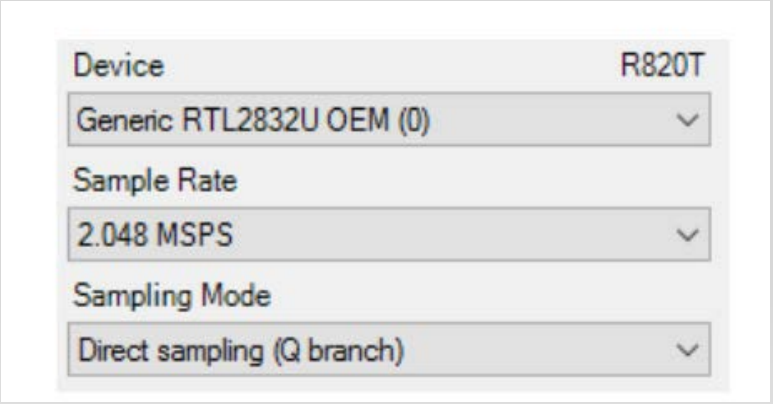
Russell Silva – AMRUPT, Spring ‘18

General Information

- “RTL-SDR is a very cheap software defined radio that uses a DVB-T TV tuner dongle based on the RTL2832U chipset. With the combined efforts of Antti Palosaari, Eric Fry and Osmocom it was found that the signal I/Q data could be accessed directly, which allowed the DVB-T TV tuner to be converted into a wideband software defined radio via a new software driver.” – rtl-sdr.com
- “The whole RTLSDR thing is fluke and not an intentional product. Basically 1.5 years ago someone discovered a stealth test mode on a commercial satellite TV receiver USB and it popped up on Reddit and the rest is history.” – Reddit Post
- The nature of the semiconductor and electronics industries in Asia is *highly competitive* so they are über paranoid about sharing information.” – Reddit Post
- “An enterprising hacker, Eric Fry, found that the device sends IQ data over the USB connection that can allow us to use it as an SDR. A lot of smart folks wrote code for linux, windows, etc and now we can use that IQ data as a means to listen to and view signals that the RTLSDR receives.” – Reddit Post

Concerns:

- Highest Safe Sampling Rate of the I/Q Extraction: 2.56 MS/s (Superkuh)
- Superheterodyne devices – Employs IF mixing; however, it is unclear whether I/Q signals can be taken after this stage
- No Formal Datasheet

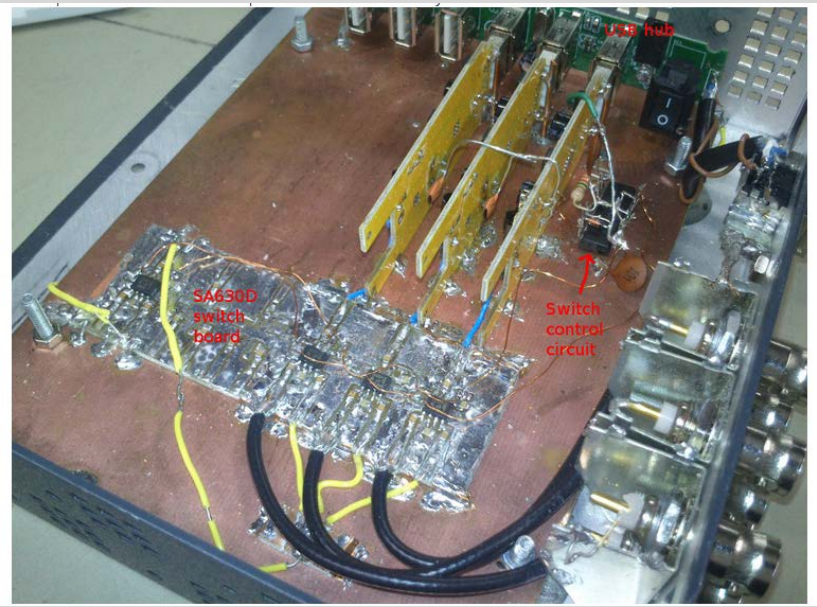


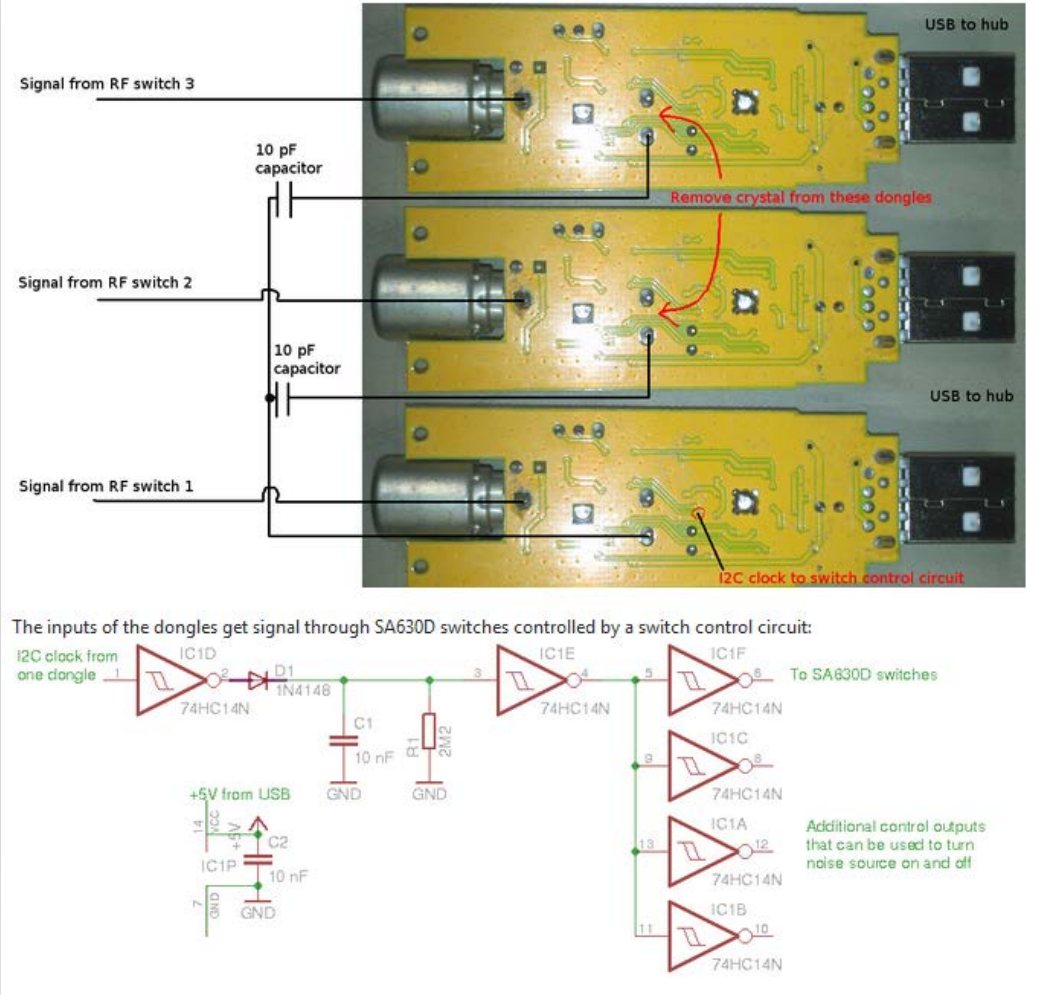
RTL-SDR Blog V3 Datasheet (rtl-sdr.com)

Clock selector jumper

- Clock selector jumper – “By soldering in a 4 pin 1.27mm pitch jumper header and removing the default 0 Ohm resistor, one can now easily select between the onboard clock, an external clock, or having the on board clock be the output for another dongle. This is for advanced users only who want to experiment with things like passive radar, and coherent receivers.” (RTL-SDR Blog V3 Datasheet – rtl-sdr.com)

Phase Interferometry Project using RTL SDRs (tejeez – Github)





GNU Radio Software:

```
Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tuner
Exact sample rate is: 2500000.107620 Hz
Sampling at 2500000 S/s.
Tuned to 100122000 Hz.
Tuner gain set to 40.20 dB.
Reading samples in async mode...
```

The raw, captured IQ data is saved in a file called *FMcapture1.dat*, which is stored in my home directory by default. You can download the file by clicking here:

FMcapature1.dat

The raw, captured IQ data is 8 bit unsigned data. Each I and Q value varies from 0 to 255 (since, 00000000_2 = 0 and 11111111_2 = 255). To get from the unsigned (0 to 255) range we need to subtract 127.5 from each I and Q value, which results in a new range from -127.5 to +127.5. Then the complex data is simply $y = I + jQ$. We perform this using Matlab by applying the following custom function *loadFile*, which is presented below. You can download this function by clicking here.

```
function y = loadFile(filename)
%  y = loadFile(filename)
%
% reads  complex samples from the rtlsdr file
%

fid = fopen(filename,'rb');
y = fread(fid,'uint8=>double');
```

"How to capture raw IQ data." (Dr. Aaron Scher, 2015)

Sources:

- http://superkuh.com/rtlsdr.html: “Central Hub” source for RTL SDR Information
- https://github.com/tejeez/rtl_coherent: Phase Interferometry Project using RTL SDRs
- https://www.reddit.com/r/RTLSDR/comments/6n9hdk/welcome_new_visitors_a_little_info_about_rtlsdr/ Reddit Post detailing how RTL SDRs became popular
- https://www.rtl-sdr.com/about-rtl-sdr/: General Information
- https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/: Buying Location
- aaronscher.com/wireless_com_SDR/RTL_SDR_AM_spectrum_demod.html “How to capture raw IQ data,” (Dr. Aaron Scher, 2015)

Keep in Mind: U.S. Frequency Allocation: