(Yet another) DVB-T based passive radar demonstration using Software Defined Radio on low-cost DVB-T receivers

W. Feng[1], G. Cherniak[1], J.-M Friedt[1,2], M. Sato[1]

[1] CNEAS, Tohoku University, Sendai, Japan
[2] FEMTO-ST Time & Frequency, Besançon, France

References at `http://jmfriedt.free.fr`
manuscript at `jmfriedt.free.fr/URSI.pdf`

February 4, 2018

Why passive RADAR

- Emitting is strongly regulated
- The radiofrequency spectrum is already congested
- RADAR range resolution $\Delta R = c_0/(2B)$ requires broadband (B) signals
- returned power $\propto d^{-4}$

$\Rightarrow$ use existing radiofrequency emissions and analyze their reflections on targets

Aller Funkverkehr ist Landesverrat
All radio traffic is high treason
A. Price, Instruments of Darkness – The History of Electronic Warfare

GRAVES RADAR, France (47.3480° N, 5.5151° E), 143.05 MHz CW, 0.4 MW

Demonstrated:
broadcast FM station [1], Wifi[2], GSM[3], analog TV[4], DAB[5], **Digital TV**

Question: can it be done with low-cost DVB-T receivers used as general purpose SDR ?

[1] C.L. Zoeller & al., *Passive coherent location radar demonstration*, Proc. 34th Southeastern Symp. on System Theory, pp. 358–362 (2002), or J. Zhu & al., *Adaptive beamforming passive radar based on FM radio transmitter*, (2007): 13-13

[2] K. Chetty & al., *Through-the-wall sensing of personnel using passive bistatic wifi radar at standoff distances*, IEEE Trans. on Geosci. & Remote Sensing 50.4 (2012): 1218-1226

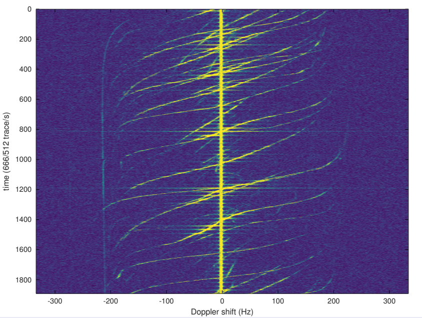
[3] R. Zemmari & al., *GSM passive radar for medium range surveillance* IEEE EuRAD (2009)

[4] P.E. Howland & al., *Target tracking using television-based bistatic radar*, IEE Proc. Radar Sonar Navig., 1999, 146, pp. 166–174

[5] M. Daun & al., *Tracking in multistatic passive radar systems using DAB/DVB-T illumination*, Signal Processing, 2012, 92(6), 1365-1386.

Why passive RADAR

- Emitting is strongly regulated
- The radiofrequency spectrum is already congested
- RADAR range resolution $\Delta R = c_0/(2B)$ requires broadband (B) signals
- returned power $\propto d^{-4}$



GRAVES RADAR, France (47.3480°N, 5.5151°E), 143.05 MHz CW, 0.4 MW

$\Rightarrow$ use existing radiofrequency emissions and analyze their reflections on targets

Demonstrated: broadcast FM station [1], Wifi[2], GSM[3], analog TV[4], DAB[5], **Digital TV**

Question: can it be done with low-cost DVB-T receivers used as general purpose SDR ?

[1] C.L. Zoeller & *al.*, *Passive coherent location radar demonstration*, Proc. 34th Southeastern Symp. on System Theory, pp. 358–362 (2002), or J. Zhu & *al.*, *Adaptive beamforming passive radar based on FM radio transmitter*, (2007): 13-13

[2] K. Chetty & *al.*, *Through-the-wall sensing of personnel using passive bistatic wifi radar at standoff distances*, IEEE Trans. on Geosci. & Remote Sensing 50.4 (2012): 1218-1226

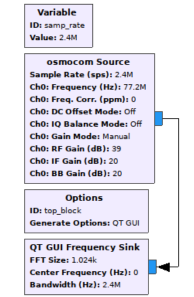
[3] R. Zemmari & *al.*, *GSM passive radar for medium range surveillance* IEEE EuRAD (2009)

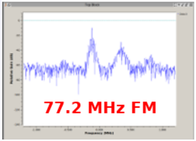
[4] P.E. Howland & al., *Target tracking using television-based bistatic radar*, IEE Proc. Radar Sonar Navig., 1999, 146, pp. 166–174

[5] M. Daun & al., *Tracking in multistatic passive radar systems using DAB/DVB-T illumination*, Signal Processing, 2012, 92(6), 1365-1386.

Low cost DVB-T receivers for SDR

- low-cost DVB-T receivers (10.38 US$=1165 yens)
- Linux driver port discovered that RTL2832U-based DVB-T receivers are general purpose software defined radio (SDR) receivers
- various RF frontends, now R820T2 (50–1600 MHz, 35 dB RF gain)
- 8-bit I and Q output on USB at max 2.4 MS/s
- GNURadio real time processing framework [6]

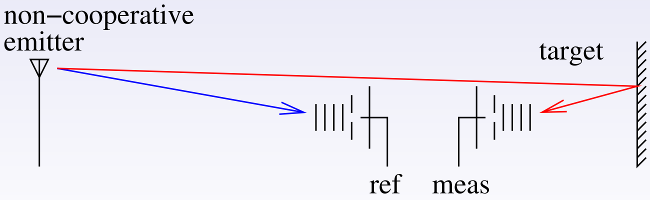




[6] E4k and RTL2832U based SDR @ `http://jmfriedt.free.fr/en_sdr.pdf`

Basics

- A "random" signal is emitted, e.g. by DVB-T tower [7] [8]
- This signal is recorded on a reference channel (direct path from emitter to reference receiver)
- A measurement channel, ideally hidden from the direct wave, records reflections.
- Search of the reference pattern in the measurement signal (time delayed) will give distance to target
- Matched filter: cross-correlation will give the strongest probability that a delayed copy of the reference is found in the signal.



[7] J. Raout *& al.*, *Passive bistatic noise radar using DVB-T signals* IET radar, sonar & navigation 4.3 (2010): 403-411

[8] J.E. Palmer *& al.*, *DVB-T passive radar signal processing*, IEEE Trans. Signal Proc. 61.8 (2013): 2116-2126

Real time correlation computation in GNURadio

From convolution to correlation:

- Convolution:

$$conv(s,r)(\tau) = \int s(t)r(\tau - t)dt$$

- Practical computation of convolution:

$$FT(conv(s,r)) = FT(s) \cdot FT(r)$$

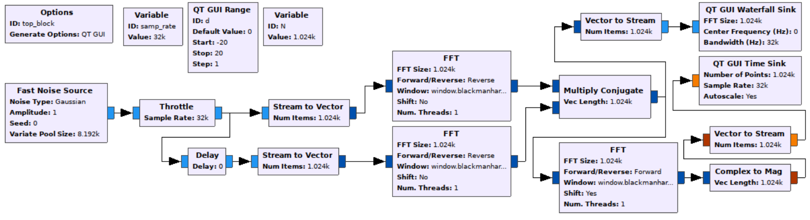
- Correlation:

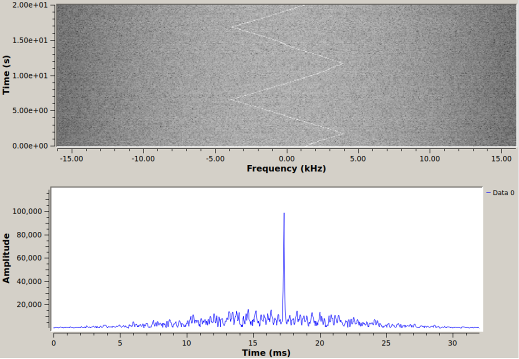
$$corr(s,r)(\tau) = \int s(t)r(t+\tau)dt$$

- Convolution $\rightarrow$ correlation: time reversal
- since $\exp(j\omega t)^* = \exp(-j\omega t)$, we conclude

$$FT(corr(s,r)) = FT(s) \cdot FT^*(r)$$

Real time correlation computation in GNURadio



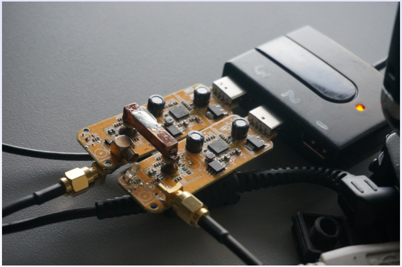


GNURadio:

- collect N-sample long vectors
- compute (i)FFT,
- multiply with complex conjugate,
- and iFFT with fftshift to get 0-delay correlation at center of graph
- *or* use waterfall sink for last iFFT

Challenge of DVB-T data collection

- each DVB-T dongle is clocked by its own quartz oscillator
- each DVB-T dongle communicates on the USB-bus at its own rate
- each DVB-T dongle generates LO with its own (oscillator-locked) PLL
- How can we make sure the datastream is **continuous**, the sampling rate equal and the phase coherent on the two dongles ?
- Same clock solves the clock reference issue, but **dithering must be deactivated** + **thermal coupling** of PLL multipliers generating LO.
- For RADAR application, phase coherence is only needed for the duration of the measurement (=maximum range)

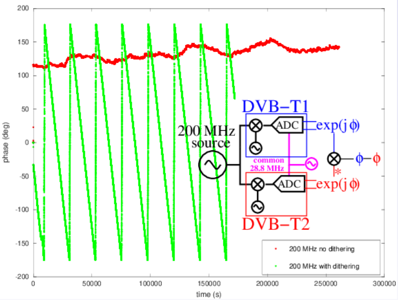


Experimental setup

Challenge of DVB-T data collection

- each DVB-T dongle is clocked by its own quartz oscillator
- each DVB-T dongle communicates on the USB-bus at its own rate
- each DVB-T dongle generates LO with its own (oscillator-locked) PLL

- How can we make sure the datastream is **continuous**, the sampling rate equal and the phase coherent on the two dongles ?
- Same clock solves the clock reference issue, but **dithering must be deactivated + thermal coupling** of PLL multipliers generating LO.
- For RADAR application, phase coherence is only needed for the duration of the measurement (=maximum range)

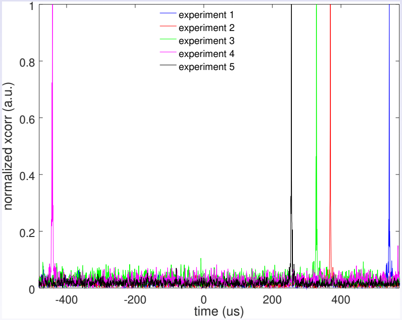


Need to de-activate PLL dithering in `librtlsdr` (`superkuh.com/rtlsdr.html`)

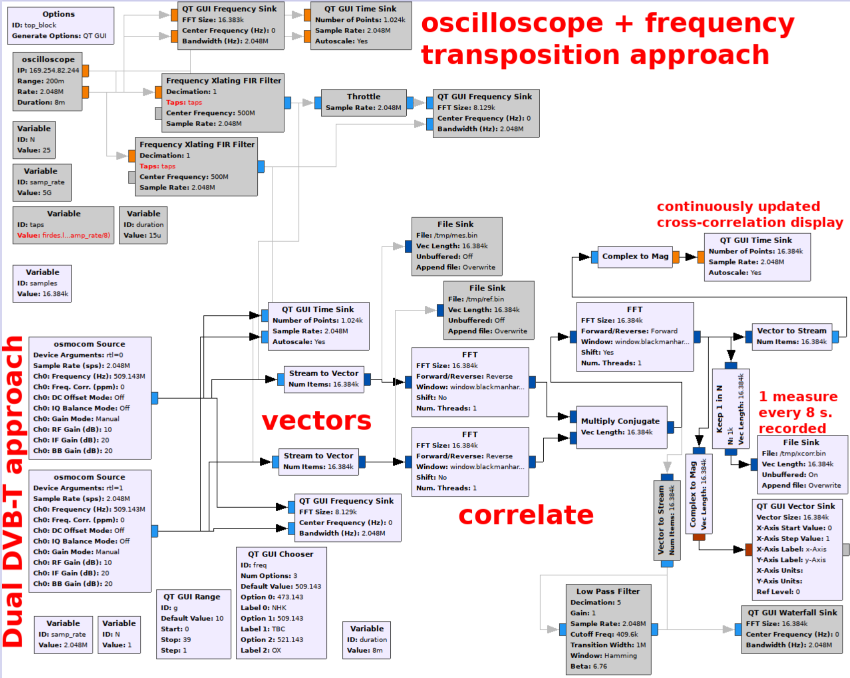
Challenge of DVB-T data collection

- each DVB-T dongle is clocked by its own quartz oscillator
- each DVB-T dongle communicates on the USB-bus at its own rate
- each DVB-T dongle generates LO with its own (oscillator-locked) PLL

- How can we make sure the datastream is **continuous**, the sampling rate equal and the phase coherent on the two dongles ?
- Same clock solves the clock reference issue, but **dithering must be deactivated** + **thermal coupling** of PLL multipliers generating LO.
- For RADAR application, phase coherence is only needed for the duration of the measurement (=maximum range)



Cross-correlation peak position for 5 experiments (400 μs @ 2 MS/s=800 sample offset)

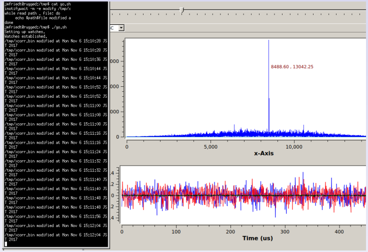


github.com/jmfriedt/gr-oscilloscope

Experimental setup

Reference antenna

GNURadio output:



Initial calibration by connecting the reference antenna to the measurement channel, and then keep the system running.

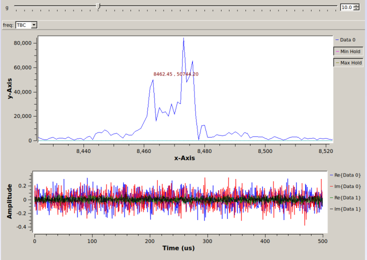
Measurement antenna

- **Never stop the data stream** since the time delay is unknown at first, but constant
- Slow down datarate so as to capture one cross-correlation curve every 8 seconds, enough time to move the antenna

Experimental setup

Reference antenna

GNURadio output:



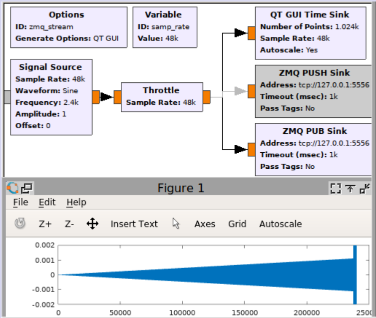
Real time time-domain signal and cross-correlation display for assessing signal quality

Measurement antenna

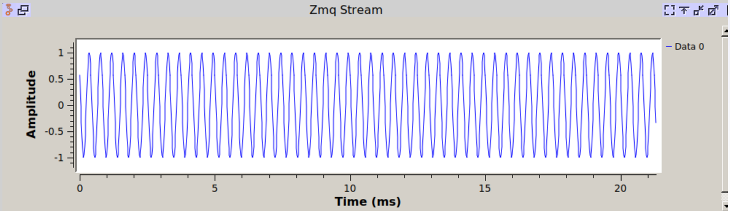
- **Never stop the data stream** since the time delay is unknown at first, but constant
- Better: stream data to external application which grabs measurements when needed (ZeroMQ pipe)

ZeroMQ

- Stream from data recorder to signal processing tool (e.g. Matlab)
- Separate recording from processing: intermadiate step between offline prototyping and integrated GNURadio processing




```
pkg load zeromq
% sock = zmq_socket(ZMQ_PULL);
sock = zmq_socket(ZMQ_SUB);
zmq_connect   (sock,"tcp://127.0.0.1:5556");
% case of SUB socket: register all services
zmq_setsockopt(sock, ZMQ_SUBSCRIBE, "");
fs=48000; f=fs/20; total_length=5*fs;
vector=zeros(total_length,1);
total=1;
while (total<total_length)
  recv=zmq_recv(sock, fs, 0);
  value=typecast(recv,"single"); % char -> float
  if (total+length(value)-1<total_length)
     vector(total:total+length(value)-1)=value;
  end
  total=total+length(value);
end
t=[0:1/fs:(length(vector)-1)/fs]';
ref=sin(2*pi*f*(t)); plot(vector-ref);
ylim([-0.002 0.002])
zmq_close (sock);
```

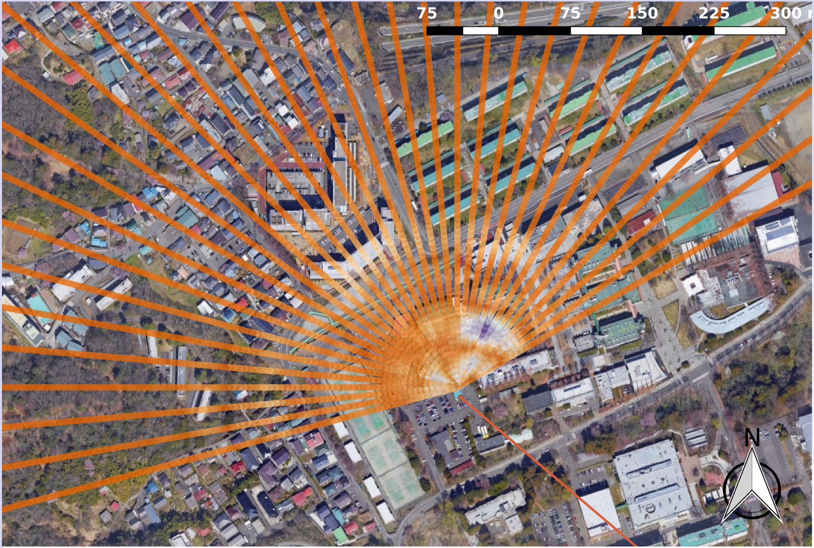


Result

DVB-T: 2 MHz bandwidth = 1 sample every 500 ns or 150 m

Result

oscilloscope: 200 MHz bandwidth = 1 sample every 5 ns or 1.5 m



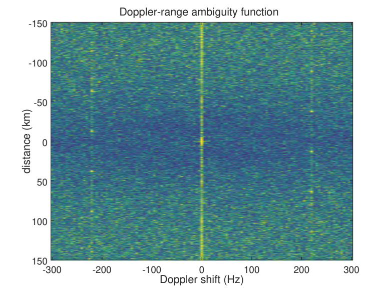
(200 ns wide autocorrelation peak)

Moving target: planes

- Range measurement feasibility study demonstrated
- Range-Doppler: for a moving target, try all possible

$$xcorr(\tau, f_D) = \int r(t) \cdot s(t+\tau) \cdot \exp(j2\pi f_D t)dt$$

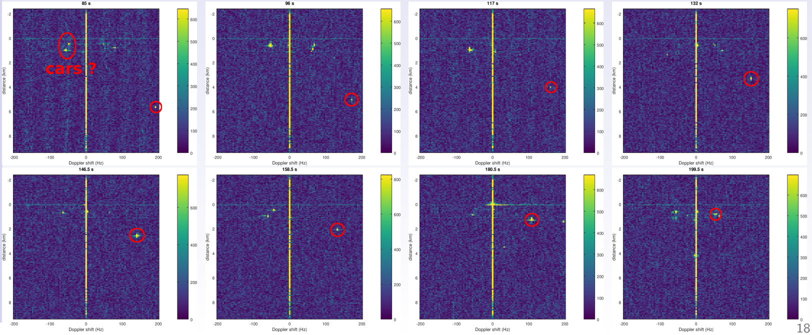
- Measurement duration ?
  - pulse compression ratio (SNR gain) given by the number of samples ($B \times T = N$ if whole bandwidth $B = 1/f_s$ is used)
  - Doppler resolution is $1/T$
  - plane flying at 360 km/h =100 m/s introduces $f_D = f \times 2v/c_0 = 333$ Hz @ 500 MHz ⇒ analyze 250 ms-long chunks of data (4 Hz Doppler resolution =9 km/h velocity resolution)
  - 250 ms=25 m @ 100 m/s
  - use of DVB-T receiver for continuous data-stream & post-process: 2 MHz bandwidth=75 m range resolution [9]



[9] kaira.sgo.fi/2013/09/passive-radar-with-16-dual-coherent.html

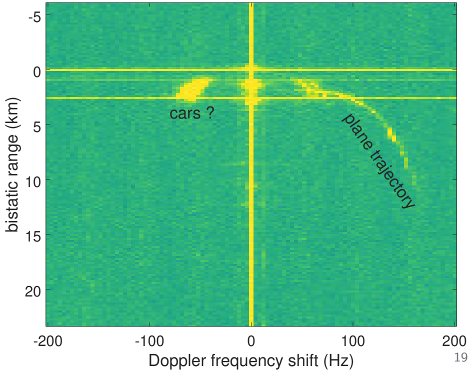
Moving target: planes

- Continuous stream: 32 MB/s=1.92 GB/min
  2 channels$\times$I/Q$\times$4 bytes/measurement$\times$2 MS/s
- Planes landing at Sendai airport, using the DVB-T emission at 473 MHz (NHK, 3 kW)
- range-Doppler map: 3 minute acquisition requires several hours processing time on general purpose CPU/interpreted language (GNU/Octave)



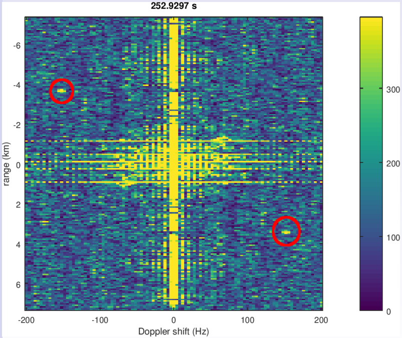
Moving target: planes

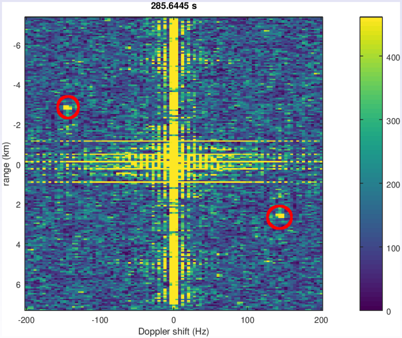
- Continuous stream: 32 MB/s=1.92 GB/min
  2 channels×I/Q×4 bytes/measurement×2 MS/s
- Planes landing at Sendai airport, using the DVB-T emission at 473 MHz (NHK, 3 kW)
- range-Doppler map: 3 minute acquisition requires several hours processing time on general purpose CPU/interpreted language (GNU/Octave)



Autocorrelation

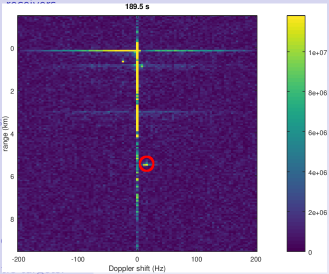
- Since some of the reference signal is in the measurement signal, autocorrelation will also identify Doppler shifted targets
- All targets will match some resemblance with all others: in our case only 1 target
- Avoids synchronizing two receivers, but lower signal to noise ratio due to the weak reference signal

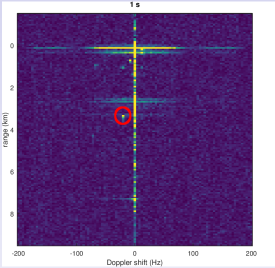


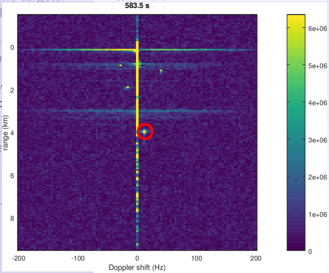


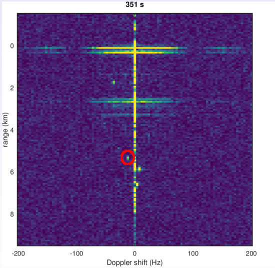
Passive RADAR on ships

Measurement from the sea shore near the port of Sendai









$f_D \simeq 12$ Hz$\simeq 3.6$ m/s$\simeq 13$ km/h$\simeq$ 7 knot, consistent with AIS transmissions ($\simeq$12 knot max. speed)

Passive RADAR on cars

$$x(\tau, f_D) = \int_{\infty}^{+\infty} \underbrace{ref(t+\tau)}_{\tau=range} \cdot mes^*(t) \cdot \underbrace{\exp(j2\pi f_D \cdot t)}_{f_D=speed} \cdot dt$$

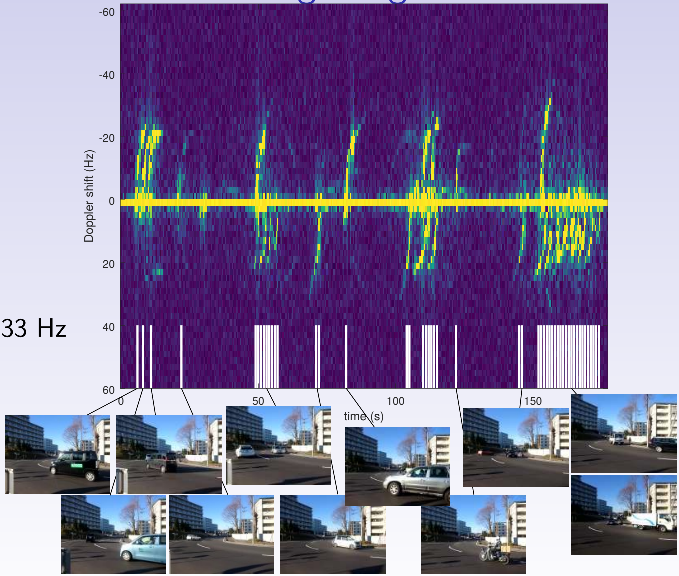
- No range resolution $\Rightarrow \tau = 0$ and compute $FFT(ref(t) \cdot mes(t)^*)$ providing the Doppler shift spectrum
- Data size: 2048 kS/s×4 bytes/S×I,Q×2 channels =33 MB/s=2 GB/min $\Rightarrow$ max record size is 3 min (6 GB RAMfs)
- Use first second of data to estimate (constant) time offset between ref. and meas. channels
- Apply this offset to all subsequent dataset (400 μs $\ll$0.5 s segment)

Short range targets: cars

Doppler consistent with car velocity at a corner:

$$f_D = 2 f_c \frac{v}{c_0} = 33 \text{ Hz}$$

@ 500 MHz & 10 m/s



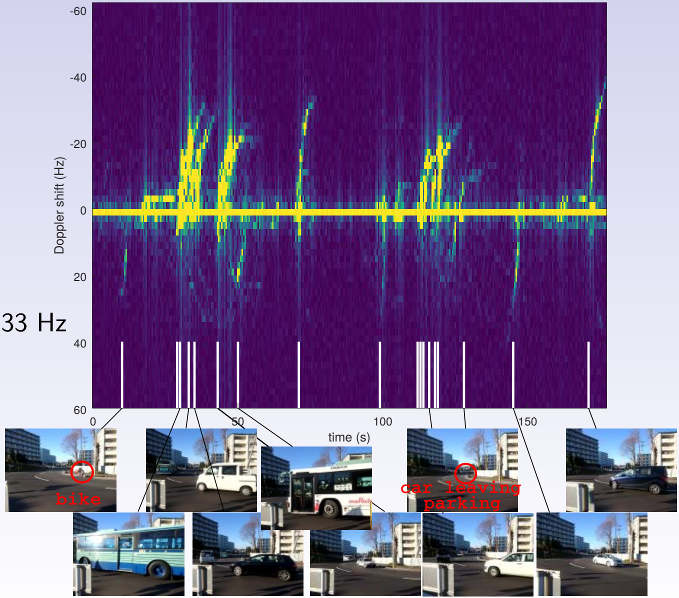
Movie → 1 picture/s, keep only pictures with cars and one white line for each time a picture appears

Short range targets: cars

Doppler consistent with car velocity at a corner:

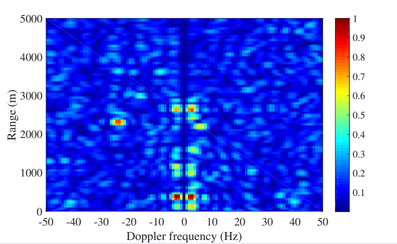
$$f_D = 2 f_c \frac{v}{c_0} = 33 \text{ Hz}$$

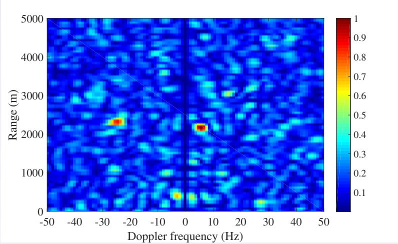
@ 500 MHz & 10 m/s

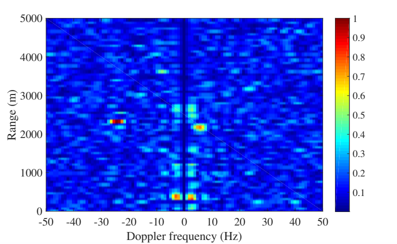


Doubling the bandwith

- Four DVB-T setup: two towards reference, two towards targets
- Each pair is set to two frequencies: adjacent frequencies = double bandwidth
- Challange: sub-sample resolution alignement of all datastreams
- Demonstration with ship detection

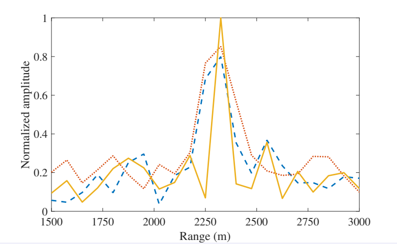




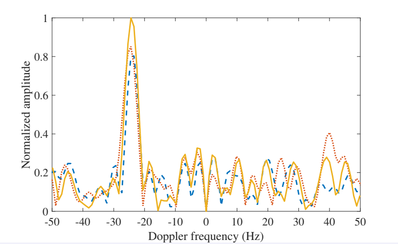


Doubling the bandwith

- Four DVB-T setup: two towards reference, two towards targets
- Each pair is set to two frequencies: adjacent frequencies = double bandwidth
- Challange: sub-sample resolution alignement of all datastreams
- Demonstration with ship detection



Range cross-section



Doppler cross-section

The two center frequencies can be widely separated: strong sidelobes but fringe period determined by center frequency difference

Conclusion and perspectives

- Demonstrated ability to detect static and moving targets using non-cooperative emitter ...
- using low-cost DVB-T receivers acting as general purpose SDR.
- GNURadio processing environment for fast prototyping and educational purposes (opensource)

What next ?

- array of DVB-T receivers for Direction of Arrival (DOA [10]) analysis (azimuth by exploiting the phase of the correlation)
- Real time correlation processing on the FPGA of the Redpitaya board ? (2× 125 MHz ADC for improved range resolution)

Resources:
Slides: `http://jmfriedt.free.fr/fosdem2018.pdf`
Manuscript: `http://jmfriedt.free.fr/URSI.pdf`
French article: GNU/Linux Magazine France **212** (Feb. 2018)
Ship movies: `http://jmfriedt.sequanux.org/ship6.mp4` (ship4..ship8)
Plane movies: `http://jmfriedt.sequanux.org/plane1.mp4` (plane1, plane2)

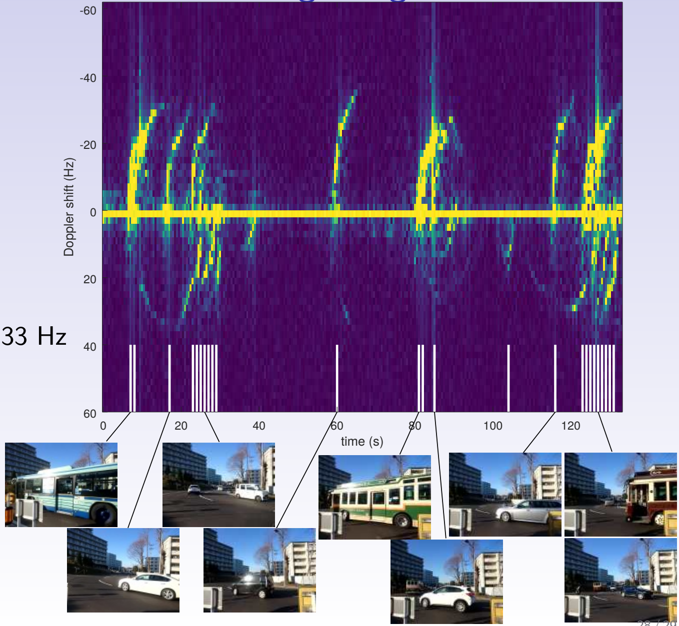
[10] GRCon2017 program @ `www.gnuradio.org/grcon-2017/program/grcon17-presentations/` and presentations @ `www.youtube.com/playlist?list=PLbBQHMnVMR43mM18y4r8L718bbYMgloFx`

Short range targets: cars

Doppler consistent with car velocity at a corner:

$$f_D = 2f_c\frac{v}{c_0} = 33 \text{ Hz}$$

@ 500 MHz & 10 m/s



Geographical settings