Software Defined Radio (SDR) Passive Radar Implementations

Jean-Michel **Friedt**
FEMTO-ST, Besançon, France
Email: jmfriedt@femto-st.fr

Web: http://jmfriedt.free.fr

with invaluable support from Weike **Feng**
Air Force Engineering University, Xi'an, China
and Pr. Motoyuki **Sato**
CNEAS, Tohoku University,
Sendai, Japan

Software Defined Radio (SDR) for RADAR applications

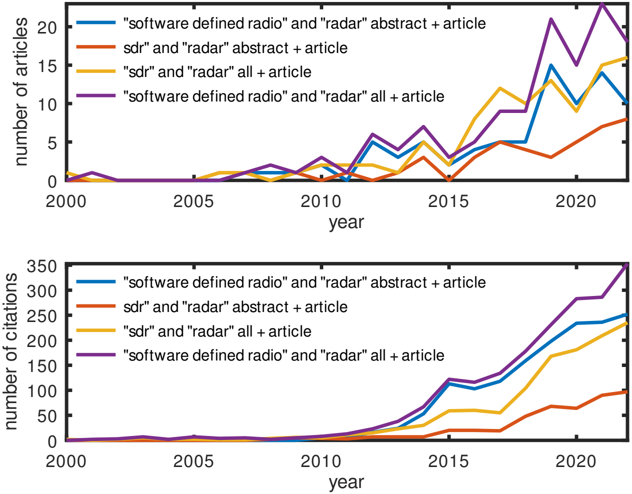
SDR architecture:

- SDR provides access to the raw radiofrequency data straight from the antenna (IQ stream)
- **flexible**: only a single frequency transposition from RF to baseband and sampling
- **stable**: fully digital signal processing
- **reconfigurable**: use one radiofrequency frontend to address all signals

SDR for **passive** RADAR:

- dual channel receiver
- ideally **coherent** (common LO), or characterize time delay and make sure it remains constant
- **synchronous** (common ADC clock)
- *N*: dynamic range
- post-processing for range (correlation) and velocity (Doppler shift) maps
- opensource framework: GNU Radio

\+ multipurpose RF platform (RADAR + communication + direction of arrival + ...)



Web Of Science statistics

Software Defined Radio (SDR) for RADAR applications

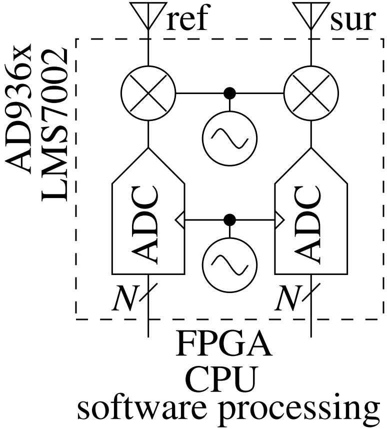
SDR architecture:

- SDR provides access to the raw radiofrequency data straight from the antenna (IQ stream)
- **flexible**: only a single frequency transposition from RF to baseband and sampling
- **stable**: fully digital signal processing
- **reconfigurable**: use one radiofrequency frontend to address all signals

SDR for **passive** RADAR:

- dual channel receiver
- ideally **coherent** (common LO), or characterize time delay and make sure it remains constant
- **synchronous** (common ADC clock)
- N: dynamic range
- post-processing for range (correlation) and velocity (Doppler shift) maps
- opensource framework: GNU Radio

+ multipurpose RF platform (RADAR + communication + direction of arrival + ...)



GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

GNU Radio: free opensource SDR framework running on PC or embedded board (cross-compiled with Buildroot)

Software Defined Radio (SDR) for RADAR applications

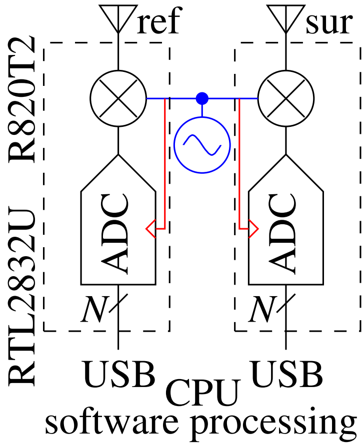
SDR architecture:

- SDR provides access to the raw radiofrequency data straight from the antenna (IQ stream)
- **flexible**: only a single frequency transposition from RF to baseband and sampling
- **stable**: fully digital signal processing
- **reconfigurable**: use one radiofrequency frontend to address all signals

SDR for **passive** RADAR:

- dual channel receiver
- ideally **coherent** (common LO), or characterize time delay and make sure it remains constant
- **synchronous** (common ADC clock)
- N: dynamic range
- post-processing for range (correlation) and velocity (Doppler shift) maps
- opensource framework: GNU Radio

+ multipurpose RF platform (RADAR + communication + direction of arrival + ...)



GNU Radio: free opensource SDR framework running on PC or embedded board (cross-compiled with Buildroot)

Passive RADAR using RTL-SDR receiver dongles and DVB-T source (Japan) [2] [3]

- R820T2 RF frontent: 50–1600 MHz LO, up to 2.4 Msamples/s, 8 bits/sample
- unknown **but constant** time delay between **multiple** USB peripherals
- **continuous** data stream from acquisition (GNU Radio) to processing (GNU/Octave, Matlab): Zero-MQ [1]PUB-SUB (UDP-like)
- periodically grab data for correlation and Doppler compensation
- compensate for limited bandwidth (2.4 MHz/RTL-SDR) by dupplicating the receivers operating at different carrier frequencies

$Map(\tau,\delta f)=\int s(t)\cdot m(t+\tau)\cdot \exp(j2\pi\delta f t)dt$ with $\delta f\simeq 2f_0\frac{v}{c}$ Doppler shift and $\tau=2\frac{d}{c}$

Bandwidth=2.4 MS/s $\Rightarrow \Delta R\simeq 62.5$ m

[1] https://github.com/jmfriedt/gnuradio_communication

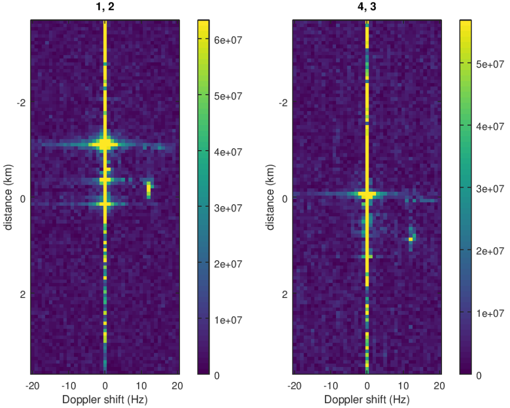
[2] https://github.com/jmfriedt/passive_radar

[3] W. Feng, J.-M. Friedt, G. Cherniak, M. Sato, *Passive bistatic radar using DVB-T receivers as general-purpose software-defined radio receivers*, Rev. Sci. Instrum. **89**, 104701 (Sept. 2018)

Passive RADAR using RTL-SDR receiver dongles and DVB-T source (Japan) [2] [3]

- R820T2 RF frontent: 50–1600 MHz LO, up to 2.4 Msamples/s, 8 bits/sample
- unknown **but constant** time delay between **multiple** USB peripherals
- **continuous** data stream from acquisition (GNU Radio) to processing (GNU/Octave, Matlab): Zero-MQ [1]PUB-SUB (UDP-like)
- periodically grab data for correlation and Doppler compensation
- compensate for limited bandwidth (2.4 MHz/RTL-SDR) by dupplicating the receivers operating at different carrier frequencies

$Map(\tau, \delta f) = \int s(t) \cdot m(t+\tau) \cdot \exp(j2\pi\delta f t)dt$ with $\delta f \simeq 2f_0 \frac{v}{c}$ Doppler shift and $\tau = 2\frac{d}{c}$



Uncalibrated delay between 1-2 and 3-4 (use direct-wave for calibration)

[1]https://github.com/jmfriedt/gnuradio_communication

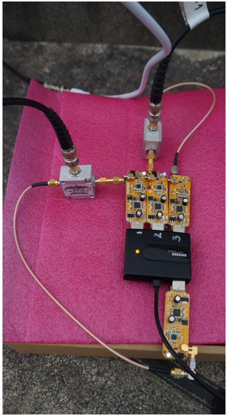
[2]https://github.com/jmfriedt/passive_radar

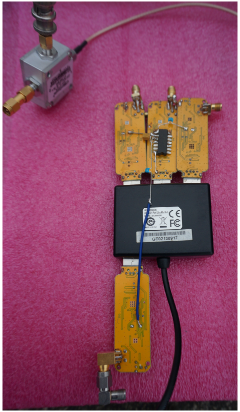
[3]W. Feng, J.-M. Friedt, G. Cherniak, M. Sato, *Passive bistatic radar using DVB-T receivers as general-purpose software-defined radio receivers*, Rev. Sci. Instrum. **89**, 104701 (Sept. 2018)

Passive RADAR using RTL-SDR receiver dongles and DVB-T source (Japan) [2] [3]

- R820T2 RF frontent: 50–1600 MHz LO, up to 2.4 Msamples/s, 8 bits/sample
- unknown **but constant** time delay between **multiple** USB peripherals
- **continuous** data stream from acquisition (GNU Radio) to processing (GNU/Octave, Matlab): Zero-MQ [1]PUB-SUB (UDP-like)
- periodically grab data for correlation and Doppler compensation
- compensate for limited bandwidth (2.4 MHz/RTL-SDR) by dupplicating the receivers operating at different carrier frequencies

$Map(\tau,\delta f)=\int s(t)\cdot m(t+\tau)\cdot \exp(j2\pi\delta ft)dt$ with $\delta f\simeq 2f_0\frac{v}{c}$ Doppler shift and $\tau=2\frac{d}{c}$



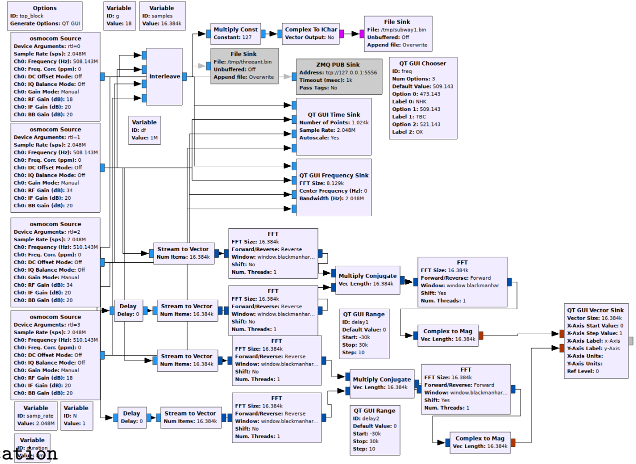


Limited range resolution (limited bandwidth) compensated for by stacking spectra $xcorr(m,s)(\tau)=iFFT(FFT(m)\cdot FFT^*(s))$ with FFT spectra accumulating adjacent carrier frequency measurements

Passive RADAR using RTL-SDR receiver dongles and DVB-T source (Japan) [2] [3]

- R820T2 RF frontent: 50–1600 MHz LO, up to 2.4 Msamples/s, 8 bits/sample
- unknown **but constant** time delay between **multiple** USB peripherals
- **continuous** data stream from acquisition (GNU Radio) to processing (GNU/Octave, Matlab): Zero-MQ [1]PUB-SUB (UDP-like)
- periodically grab data for correlation and Doppler compensation
- compensate for limited bandwidth (2.4 MHz/RTL-SDR) by dupplicating the receivers operating at different carrier frequencies

$Map(\tau,\delta f)=\int s(t)\cdot m(t+\tau)\cdot \exp(j2\pi\delta f t)dt$ with $\delta f \simeq 2f_0\frac{v}{c}$ Doppler shift and $\tau = 2\frac{d}{c}$



[1] https://github.com/jmfriedt/gnuradio_communication

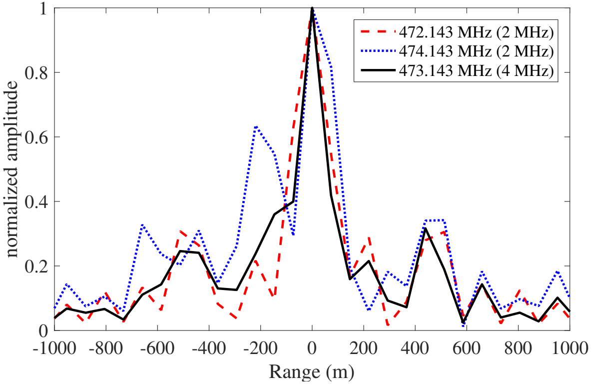
[2] https://github.com/jmfriedt/passive_radar

[3] W. Feng, J.-M. Friedt, G. Cherniak, M. Sato, *Passive bistatic radar using DVB-T receivers as general-purpose software-defined radio receivers*, Rev. Sci. Instrum. **89**, 104701 (Sept. 2018)

Passive RADAR using RTL-SDR receiver dongles and DVB-T source (Japan) [2] [3]

- R820T2 RF frontent: 50–1600 MHz LO, up to 2.4 Msamples/s, 8 bits/sample
- unknown **but constant** time delay between **multiple** USB peripherals
- **continuous** data stream from acquisition (GNU Radio) to processing (GNU/Octave, Matlab): Zero-MQ [1]PUB-SUB (UDP-like)
- periodically grab data for correlation and Doppler compensation
- compensate for limited bandwidth (2.4 MHz/RTL-SDR) by dupplicating the receivers operating at different carrier frequencies

$Map(\tau, \delta f) = \int s(t) \cdot m(t+\tau) \cdot \exp(j2\pi\delta f t)dt$ with $\delta f \simeq 2f_0\frac{v}{c}$ Doppler shift and $\tau = 2\frac{d}{c}$



---

[1] https://github.com/jmfriedt/gnuradio_communication

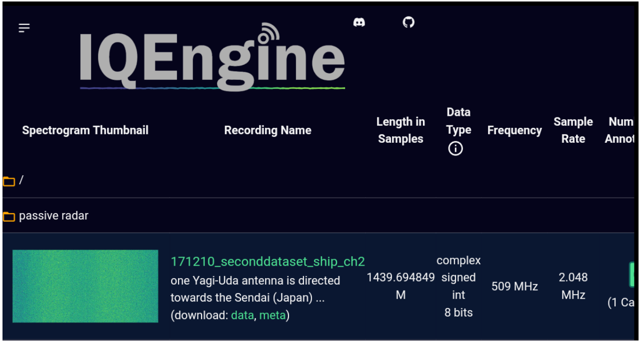
[2] https://github.com/jmfriedt/passive_radar

[3] W. Feng, J.-M. Friedt, G. Cherniak, M. Sato, *Passive bistatic radar using DVB-T receivers as general-purpose software-defined radio receivers*, Rev. Sci. Instrum. **89**, 104701 (Sept. 2018)

Passive RADAR using RTL-SDR receiver dongles and DVB-T source (Japan) [2] [3]

- R820T2 RF frontent: 50–1600 MHz LO, up to 2.4 Msamples/s, 8 bits/sample
- unknown **but constant** time delay between **multiple** USB peripherals
- **continuous** data stream from acquisition (GNU Radio) to processing (GNU/Octave, Matlab): Zero-MQ [1]PUB-SUB (UDP-like)
- periodically grab data for correlation and Doppler compensation
- compensate for limited bandwidth (2.4 MHz/RTL-SDR) by dupplicating the receivers operating at different carrier frequencies

$Map(\tau,\delta f)=\int s(t)\cdot m(t+\tau)\cdot \exp(j2\pi\delta f t)dt$ with $\delta f\simeq 2f_0\frac{v}{c}$ Doppler shift and $\tau=2\frac{d}{c}$



IQ Engine:
`iqengine.org` → GNU Radio SigMF → passive radar

[1] `https://github.com/jmfriedt/gnuradio_communication`

[2] `https://github.com/jmfriedt/passive_radar`

[3] W. Feng, J.-M. Friedt, G. Cherniak, M. Sato, *Passive bistatic radar using DVB-T receivers as general-purpose software-defined radio receivers*, Rev. Sci. Instrum. **89**, 104701 (Sept. 2018)

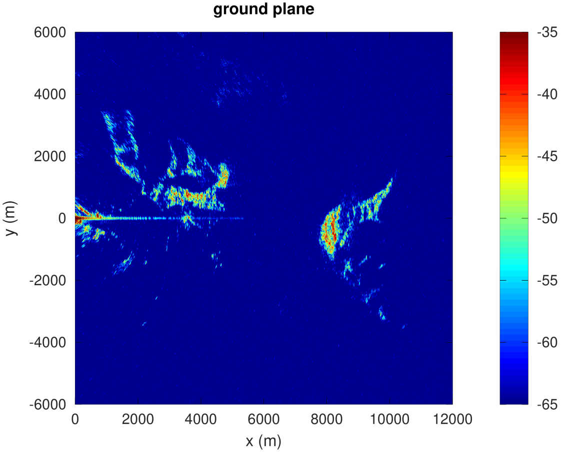
Passive RADAR using the B210 using Sentinel1 source (worldwide)

- Sentinel1: C-band spaceborne RADAR with **predictable** and **published** observation pattern
- 100 MHz wide chirp but only a fraction recorded by B210 SDR (limited by USB bandwidth)
- short (200 ms) illumination duration of a given location

- clock uncertainty: record ± 30 s around expected illumination time (60 s @ 8 MS/s for float-complex samples, dual channel is $8 \times 4 \times 2 \times 2 \times 60 = 7.68$ GB fitting in the RAMdisk of an 8-GB Raspberry Pi 4)
- portable solution using a USB battery pack to power Rasberry Pi 4 + B210, and stream (Ethernet) to laptop: tested in Europe and Arctic regions
- use satellite motion for SAR imaging: only satellite altitude (velocity) is needed for ground based azimuth/range mapping[4]

Passive RADAR using the B210 using Sentinel1 source (worldwide)

- Sentinel1: C-band spaceborne RADAR with **predictable** and **published** observation pattern
- 100 MHz wide chirp but only a fraction recorded by B210 SDR (limited by USB bandwidth)
- short (200 ms) illumination duration of a given location
- clock uncertainty: record ± 30 s around expected illumination time (60 s @ 8 MS/s for float-complex samples, dual channel is $8 \times 4 \times 2 \times 2 \times 60 = 7.68$ GB fitting in the RAMdisk of an 8-GB Raspberry Pi 4)
- portable solution using a USB battery pack to power Rasberry Pi 4 + B210, and stream (Ethernet) to laptop: tested in Europe and Arctic regions
- use satellite motion for SAR imaging: only satellite altitude (velocity) is needed for ground based azimuth/range mapping[4]



[4]W. Feng, J.-M. Friedt, P. Wan, *SDR-implemented passive bistatic SAR system using Sentinel-1 signal and itsexperiment results*, MDPI Remote Sensing **14** (1) pp.221- (2022) and `https://github.com/jmfriedt/sentinel1_pbr`

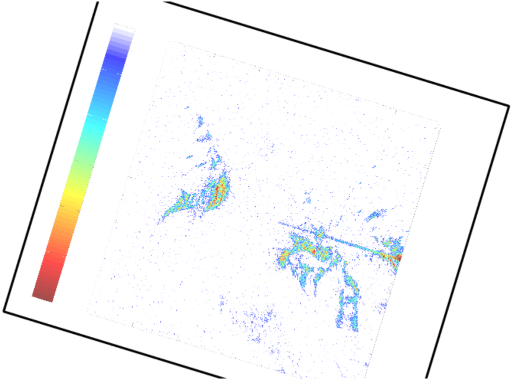
Passive RADAR using the B210 using Sentinel1 source (worldwide)

- Sentinel1: C-band spaceborne RADAR with **predictable** and **published** observation pattern
- 100 MHz wide chirp but only a fraction recorded by B210 SDR (limited by USB bandwidth)
- short (200 ms) illumination duration of a given location
- clock uncertainty: record ± 30 s around expected illumination time (60 s @ 8 MS/s for float-complex samples, dual channel is $8 \times 4 \times 2 \times 2 \times 60 = 7.68$ GB fitting in the RAMdisk of an 8-GB Raspberry Pi 4)
- portable solution using a USB battery pack to power Rasberry Pi 4 + B210, and stream (Ethernet) to laptop: tested in Europe and Arctic regions
- use satellite motion for SAR imaging: only satellite altitude (velocity) is needed for ground based azimuth/range mapping[4]

[4]W. Feng, J.-M. Friedt, P. Wan, *SDR-implemented passive bistatic SAR system using Sentinel-1 signal and itsexperiment results*, MDPI Remote Sensing **14** (1) pp.221- (2022) and `https://github.com/jmfriedt/sentinel1_pbr`

Passive RADAR using the B210 using Sentinel1 source (worldwide)

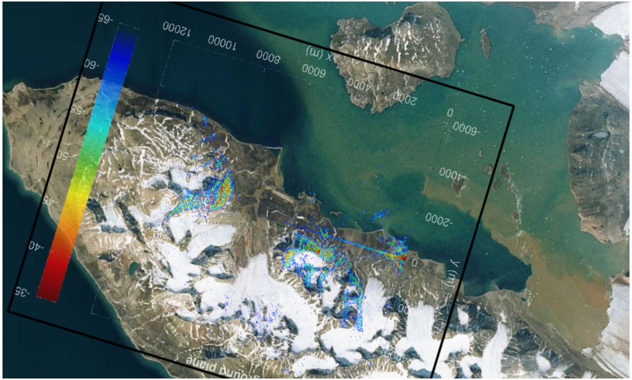
- Sentinel1: C-band spaceborne RADAR with **predictable** and **published** observation pattern
- 100 MHz wide chirp but only a fraction recorded by B210 SDR (limited by USB bandwidth)
- short (200 ms) illumination duration of a given location
- clock uncertainty: record ±30 s around expected illumination time (60 s @ 8 MS/s for float-complex samples, dual channel is $8 \times 4 \times 2 \times 2 \times 60 = 7.68$ GB fitting in the RAMdisk of an 8-GB Raspberry Pi 4)
- portable solution using a USB battery pack to power Rasberry Pi 4 + B210, and stream (Ethernet) to laptop: tested in Europe and Arctic regions
- use satellite motion for SAR imaging: only satellite altitude (velocity) is needed for ground based azimuth/range mapping[4]



[4]W. Feng, J.-M. Friedt, P. Wan, *SDR-implemented passive bistatic SAR system using Sentinel-1 signal and itsexperiment results*, MDPI Remote Sensing **14** (1) pp.221- (2022) and `https://github.com/jmfriedt/sentinel1_pbr`

Passive RADAR using the B210 using Sentinel1 source (worldwide)

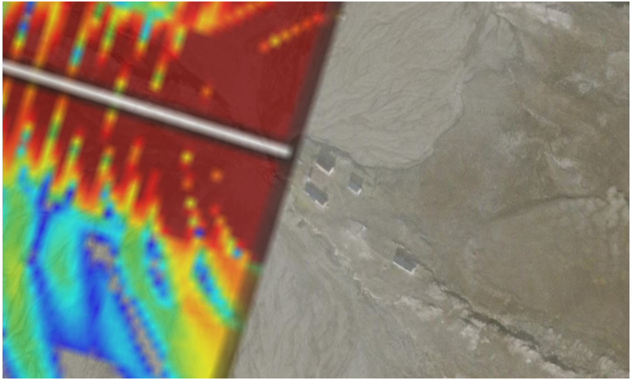
- Sentinel1: C-band spaceborne RADAR with **predictable** and **published** observation pattern
- 100 MHz wide chirp but only a fraction recorded by B210 SDR (limited by USB bandwidth)
- short (200 ms) illumination duration of a given location
- clock uncertainty: record ± 30 s around expected illumination time (60 s @ 8 MS/s for float-complex samples, dual channel is $8 \times 4 \times 2 \times 2 \times 60 = 7.68$ GB fitting in the RAMdisk of an 8-GB Raspberry Pi 4)
- portable solution using a USB battery pack to power Rasberry Pi 4 + B210, and stream (Ethernet) to laptop: tested in Europe and Arctic regions
- use satellite motion for SAR imaging: only satellite altitude (velocity) is needed for ground based azimuth/range mapping[4]



[4] W. Feng, J.-M. Friedt, P. Wan, *SDR-implemented passive bistatic SAR system using Sentinel-1 signal and itsexperiment results*, MDPI Remote Sensing **14** (1) pp.221- (2022) and `https://github.com/jmfriedt/sentinel1_pbr`

Passive RADAR using the B210 using Sentinel1 source (worldwide)

- Sentinel1: C-band spaceborne RADAR with **predictable** and **published** observation pattern
- 100 MHz wide chirp but only a fraction recorded by B210 SDR (limited by USB bandwidth)
- short (200 ms) illumination duration of a given location
- clock uncertainty: record ±30 s around expected illumination time (60 s @ 8 MS/s for float-complex samples, dual channel is $8 \times 4 \times 2 \times 2 \times 60 = 7.68$ GB fitting in the RAMdisk of an 8-GB Raspberry Pi 4)
- portable solution using a USB battery pack to power Rasberry Pi 4 + B210, and stream (Ethernet) to laptop: tested in Europe and Arctic regions
- use satellite motion for SAR imaging: only satellite altitude (velocity) is needed for ground based azimuth/range mapping[4]



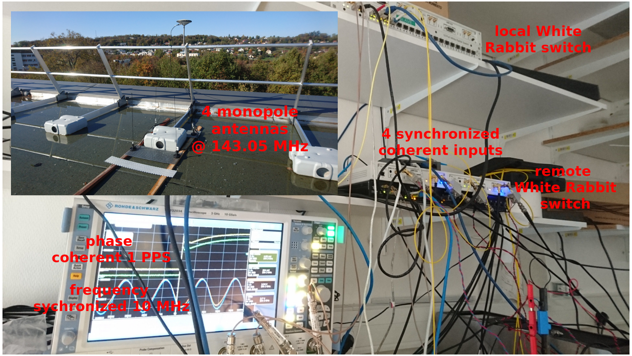
[4]W. Feng, J.-M. Friedt, P. Wan, *SDR-implemented passive bistatic SAR system using Sentinel-1 signal and itsexperiment results*, MDPI Remote Sensing **14** (1) pp.221- (2022) and `https://github.com/jmfriedt/sentinel1_pbr`

Distributed passive RADAR using the X310 synchronized using White Rabbit (GRAVES)

Widely distributed receivers:

- GRAVES: CW space surveillance RADAR emitter located 30 km from our laboratory location in France
- replace ranging (no range resolution from CW) with angle of arrival (phase) measurement on a long baseline for plane detection
- synchronize X310 SDR receivers with White Rabbit 10 MHz and 1-PPS reference signal broadcast over Gb Ethernet
- use aliasing (second Nyquist zone) to sample the 143.05 MHz signal with the 200 MS/s ADC

2×X310 SDR: 200 MS/s $\Rightarrow$ use aliasing to record 143.05 MHz signal (@ 56.95 MHz)



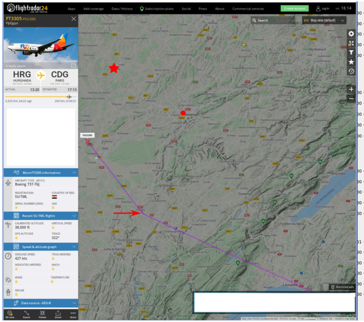
White Rabbit=$\sigma_\tau \simeq 60$ ps synchronization over Gb Ethernet network (60 ps = 3° @ 143.05 MHz)

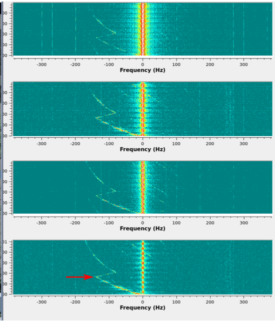
Distributed passive RADAR using the X310 synchronized using White Rabbit (GRAVES)

Widely distributed receivers:

- GRAVES: CW space surveillance RADAR emitter located 30 km from our laboratory location in France
- replace ranging (no range resolution from CW) with angle of arrival (phase) measurement on a long baseline for plane detection
- synchronize X310 SDR receivers with White Rabbit 10 MHz and 1-PPS reference signal broadcast over Gb Ethernet
- use aliasing (second Nyquist zone) to sample the 143.05 MHz signal with the 200 MS/s ADC

2×X310 SDR: 200 MS/s ⇒ use aliasing to record 143.05 MHz signal (@ 56.95 MHz)





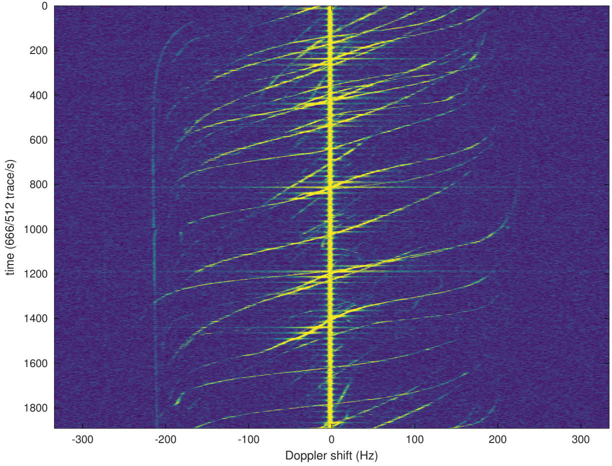
CW RADAR: Doppler shift only, no range information... unless AoA

Distributed passive RADAR using the X310 synchronized using White Rabbit (GRAVES)

Widely distributed receivers:

- GRAVES: CW space surveillance RADAR emitter located 30 km from our laboratory location in France
- replace ranging (no range resolution from CW) with angle of arrival (phase) measurement on a long baseline for plane detection
- synchronize X310 SDR receivers with White Rabbit 10 MHz and 1-PPS reference signal broadcast over Gb Ethernet
- use aliasing (second Nyquist zone) to sample the 143.05 MHz signal with the 200 MS/s ADC

2×X310 SDR: 200 MS/s ⇒ use aliasing to record 143.05 MHz signal (@ 56.95 MHz)

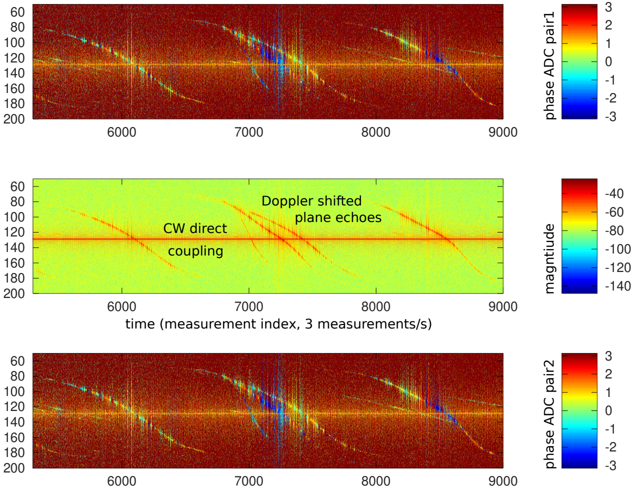


Distributed passive RADAR using the X310 synchronized using White Rabbit (GRAVES)

Widely distributed receivers:

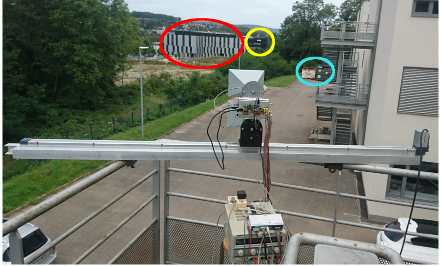
- GRAVES: CW space surveillance RADAR emitter located 30 km from our laboratory location in France
- replace ranging (no range resolution from CW) with angle of arrival (phase) measurement on a long baseline for plane detection
- synchronize X310 SDR receivers with White Rabbit 10 MHz and 1-PPS reference signal broadcast over Gb Ethernet
- use aliasing (second Nyquist zone) to sample the 143.05 MHz signal with the 200 MS/s ADC

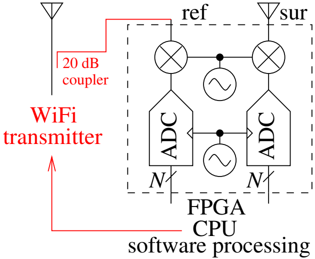
2×X310 SDR: 200 MS/s ⇒ use aliasing to record 143.05 MHz signal (@ 56.95 MHz)

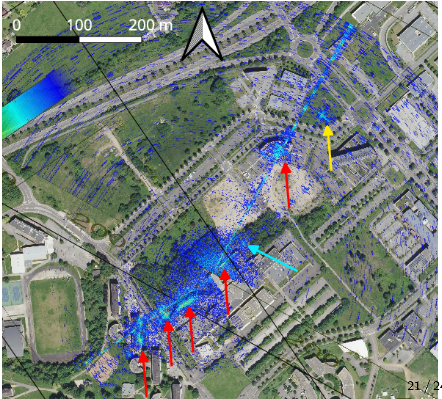


Covert SDR-GB-SAR using WiFi

- Challenge of passive RADAR geometry: help with a non-cooperative emitter colocated with receiver [a]
- record loopback signal and correlate for ranging
- limited bandwidth (ADC sampling rate, communication and storage) ⇒ frequency **stacking** (200 MHz on 5.8 GHz WiFi)
- repeat for each new antenna position, possibly with pseudo-random channel generator instead of linear sweep
- Raspberry Pi4 used for both data acquisition, rail control and processing



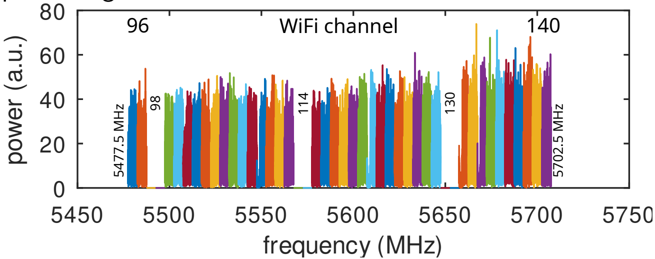


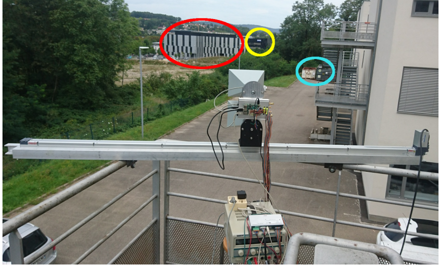


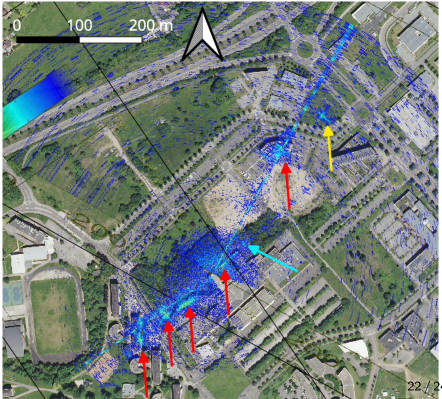
[a] https://github.com/jmfriedt/SDR-GB-SAR

Covert SDR-GB-SAR using WiFi

- Challenge of passive RADAR geometry: help with a non-cooperative emitter colocated with receiver [a]
- record loopback signal and correlate for ranging
- limited bandwidth (ADC sampling rate, communication and storage) ⇒ frequency **stacking** (200 MHz on 5.8 GHz WiFi)
- repeat for each new antenna position, possibly with pseudo-random channel generator instead of linear sweep
- Raspberry Pi4 used for both data acquisition, rail control and processing







[a] https://github.com/jmfriedt/SDR-GB-SAR

Conclusion

- Use of surrounding electromagnetic smog for target mapping
- Add non-cooperative source for controlled but covert emissions
- Developing (SAR) passive-RADAR has never been easier and more accessible

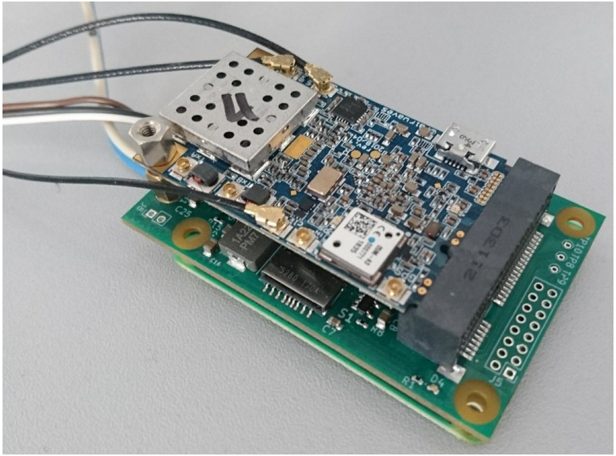
Work in progress:

- UAV mounted passive RADAR (XTRX SDR receiver) $\longrightarrow$
  (heating problems = local oscillator drift !)
- merge 2.45 GHz WiFi with 5.8 GHz WiFi when antenna with sufficient bandwidth is available (A-Info LB-2060-H-SF is 2 to 6 GHz horn antenna with 15 dBi gain)

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

`http://jmfriedt.free.fr`

Lime XTRX + Compute Module 4 (OEM version of RPi4): 60 MS/s dual-channel 12-bit IQ in 62.5 × 40 mm & 55 g



Conclusion

- Use of surrounding electromagnetic smog for target mapping
- Add non-cooperative source for controlled but covert emissions
- Developing (SAR) passive-RADAR has never been easier and more accessible

Work in progress:

- UAV mounted passive RADAR (XTRX SDR receiver) $\longrightarrow$ (heating problems = local oscillator drift !)
- merge 2.45 GHz WiFi with 5.8 GHz WiFi when antenna with sufficient bandwidth is available (A-Info LB-2060-H-SF is 2 to 6 GHz horn antenna with 15 dBi gain)

GNU Radio THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

`http://jmfriedt.free.fr`