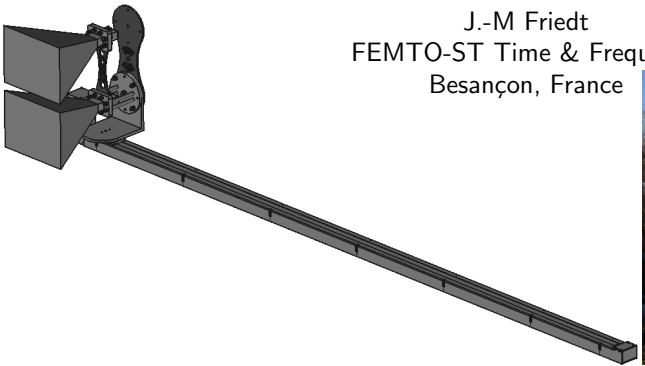
Covert Ground Based Synthetic Aperture RADAR using a Wi-Fi emitter and SDR receiver



J.-M Friedt
FEMTO-ST Time & Frequency
Besançon, France

February 4, 2024

femto-st
sciences & technologies

What is GB-SAR?

Ground Based-Synthetic Aperture RADAR

Active remote sensing technique for fine displacement mapping using **RADAR**

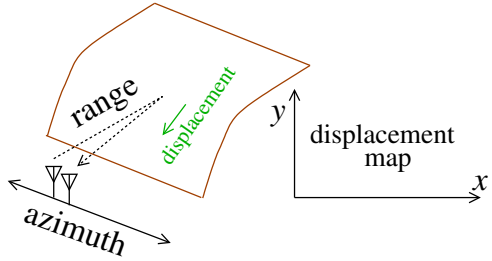
- **Active** $\Rightarrow$ no illumination dependence ($\neq$ optical passive remote sensing, e.g. satellite imagery or photogrammetry)
- **RADAR** $\Rightarrow$ no fog/rain dependence (unlike LiDAR)

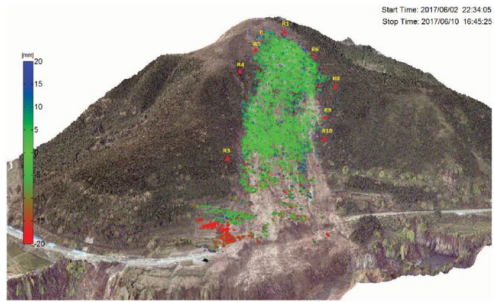
Commercial availabilty:

IDS Ibis [a] , Metasensing FastGBSAR [b]

but active means obtaining a license for emitting.

Covert GB-SAR using existing, licensed radio frequency emitters and SDR receiver?





A. Karunathilake, L. Zou, K. Kikuta, M. Sato, *Implementation and configuration of GB-SAR for landslide monitoring: Case study in Minami-Aso, Kumamoto*, Exploration Geophysics **50**(2) pp.210–220 (2019)

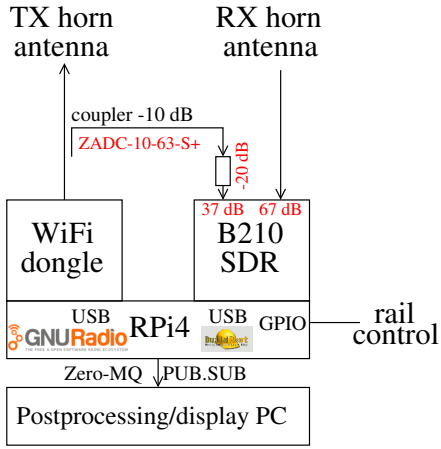
[a] https://idsgeoradar.com/products/interferometric-radar/ibis-fl

[b] https://metasensing.com/product/fastgbsar/

Requirements

- **bandwidth**: $\Delta R = c/(2B)$ for separating voxels along depth
- **increasing carrier frequency**:
  - easier to have high bandwidth at high frequency (2.4 GHz Wi-Fi: 80 MHz wide ; 5.8 GHz Wi-Fi: 200 MHz wide)
  - smaller antenna/higher gain with lower mechanical constraint
  - azimuth resolution $\simeq \frac{\lambda}{L}$ with antenna size (SAR motion) L
- **power**: returned power decays as 4th power of distance
- **spatial diversity** for azimuth compression: synthetic aperture by **moving** the TX+RX with $\lambda/4$ steps[a] ULA[b]

  At 5600 MHz, $\lambda \simeq 5.36$ cm $\Rightarrow \lambda/4 \simeq 1.34$ cm or 170 cm with 128 steps $<$ 2 m long rail



G. Goavec-Merou, J.-M Friedt, *Porting GNU Radio to Buildroot: application to an embedded digital network analyzer*, FOSDEM 2021

[a] matching the sampling theorem since both TX and RX are moving $\Rightarrow$ two-way path $< \lambda/2$

[b] Uniform Linear Array $\Rightarrow$ **azimuth compression = FFT**

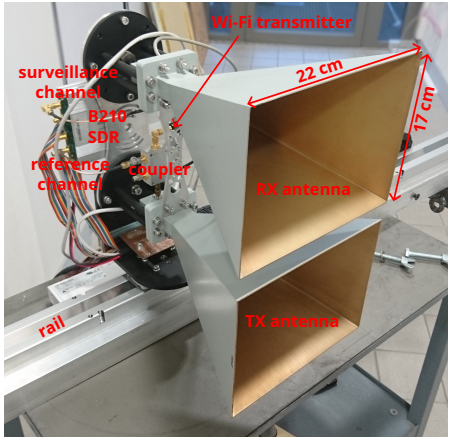
$\rightarrow$ **Covert** radiofrequency signal: use of Wi-Fi emitter

$\rightarrow$ **Unknown waveform** $\Rightarrow$ record on reference channel the emitted signal and record on second coherent channel the signal backscattered by illuminated targets

Requirements

- **bandwidth**: $\Delta R = c/(2B)$ for separating voxels along depth
- **increasing carrier frequency**:
  - easier to have high bandwidth at high frequency (2.4 GHz Wi-Fi: 80 MHz wide ; 5.8 GHz Wi-Fi: 200 MHz wide)
  - smaller antenna/higher gain with lower mechanical constraint
  - azimuth resolution $\simeq \frac{\lambda}{L}$ with antenna size (SAR motion) L
- **power**: returned power decays as 4th power of distance
- **spatial diversity** for azimuth compression: synthetic aperture by **moving** the TX+RX with $\lambda/4$ steps[a] ULA[b]

  At 5600 MHz, $\lambda \simeq 5.36$ cm $\Rightarrow \lambda/4 \simeq 1.34$ cm or 170 cm with 128 steps $<$ 2 m long rail



[a] matching the sampling theorem since both TX and RX are moving $\Rightarrow$ two-way path $< \lambda/2$

[b] Uniform Linear Array $\Rightarrow$ **azimuth compression = FFT**

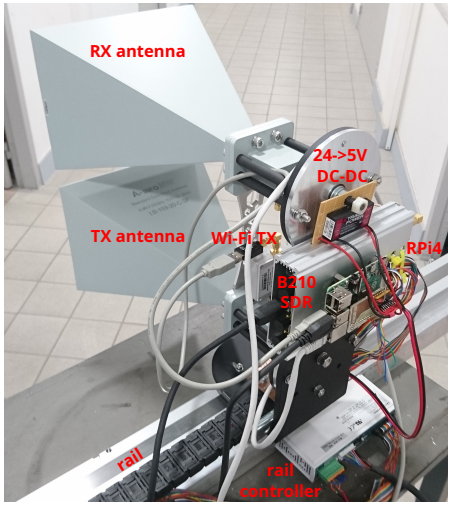
$\rightarrow$ **Covert** radiofrequency signal: use of Wi-Fi emitter

$\rightarrow$ **Unknown waveform** $\Rightarrow$ record on reference channel the emitted signal and record on second coherent channel the signal backscattered by illuminated targets

Requirements

- **bandwidth**: $\Delta R = c/(2B)$ for separating voxels along depth
- **increasing carrier frequency**:
  - easier to have high bandwidth at high frequency (2.4 GHz Wi-Fi: 80 MHz wide ; 5.8 GHz Wi-Fi: 200 MHz wide)
  - smaller antenna/higher gain with lower mechanical constraint
  - azimuth resolution $\simeq \frac{\lambda}{L}$ with antenna size (SAR motion) L
- **power**: returned power decays as 4th power of distance
- **spatial diversity** for azimuth compression: synthetic aperture by **moving** the TX+RX with $\lambda/4$ steps[a] ULA[b]

  At 5600 MHz, $\lambda \simeq 5.36$ cm $\Rightarrow \lambda/4 \simeq 1.34$ cm or 170 cm with 128 steps $<$ 2 m long rail

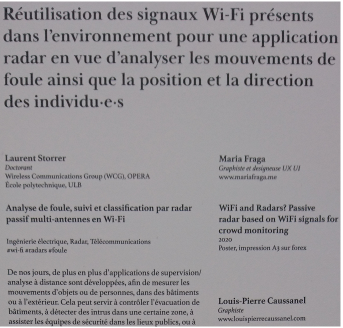


[a] matching the sampling theorem since both TX and RX are moving $\Rightarrow$ two-way path $< \lambda/2$

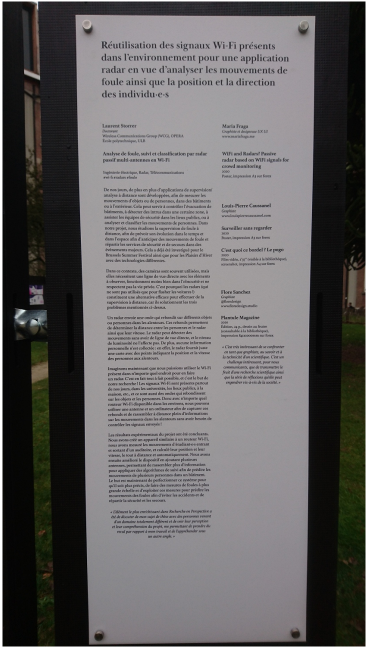
[b] Uniform Linear Array $\Rightarrow$ **azimuth compression = FFT**

$\rightarrow$ **Covert** radiofrequency signal: use of Wi-Fi emitter

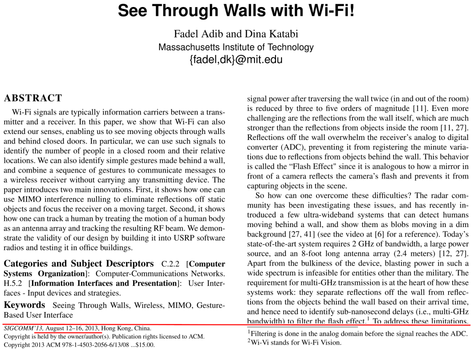
$\rightarrow$ **Unknown waveform** $\Rightarrow$ record on reference channel the emitted signal and record on second coherent channel the signal backscattered by illuminated targets


Réutilisation des signaux Wi-Fi présents dans l'environnement pour une application radar en vue d'analyser les mouvements de foule ainsi que la position et la direction des individu·e·s
Laurent Storrer
Doctorant
Wireless Communications Group (WCG), OPERA
École polytechnique, ULB
Maria Fraga
Graphiste et designeuse UX UI
www.mariafraga.me
Analyse de foule, suivi et classification par radar passif multi-antennes en Wi-Fi
WiFi and Radars? Passive radar based on WiFi signals for crowd monitoring
Ingénierie électrique, Radar, Télécommunications
#wi-fi #radars #foule
2020
Poster, impression A3 sur forex
De nos jours, de plus en plus d'applications de supervision/analyse à distance sont développées, afin de mesurer les mouvements d'objets ou de personnes, dans des bâtiments ou à l'extérieur. Cela peut servir à contrôler l'évacuation de bâtiments, à détecter des intrus dans une certaine zone, à assister les équipes de sécurité dans les lieux publics, ou à
Louis-Pierre Caussanel
Graphiste
www.louispierrecaussanel.com


PROJET RECHERCHE EN PERSPECTIVE
LOUIS-PIERRE CAUSSANEL
Surveiller sans regarder
Protéger la foule grâce à l'utilisation d'un radar basé sur les signaux Wi-Fi.
Prévenir les dangers de la foule
En 1989, 96 personnes sont tués lors d'un mouvement de foule durant un match de football à Sheffield en Angleterre.
En 2010, 21 personnes meurent par suffocation lors d'un festival de musique à Duisburg en Allemagne.
Pour éviter ces drames qui peuvent survenir lors de grands rassemblements, l'objectif est de développer un outil capable d'analyser les mouvements à l'intérieur d'une foule afin d'anticiper les situations potentiellement dangereuses.
D'ordinaire, les services de sécurité utilisent la surveillance par caméra, mais elle présente plusieurs défauts majeurs. Elle est aveugle la nuit et face à un obstacle, et elle est très impopulaire car intrusive et oppressante.
Utiliser la wi-fi comme un radar
Un radar est un système de detecte la position et la vitesse des objets qui l'entoure. Il est donc un outil efficace pour analyser les mouvements à l'intérieur d'une foule et prévenir des dangers.
De la même manière qu'une antenne radar, les bornes Wi-FI envoient des ondes dans toutes les directions et peuvent ainsi être détournées de leur usage premier en servant d'outil de supervision de foules.



Wi-Fi as **non-cooperative** signal source / passive RADAR has been widely investigated (MIT: 2013)



See Through Walls with Wi-Fi!

Fadel Adib and Dina Katabi
Massachusetts Institute of Technology
{fadel,dk}@mit.edu

ABSTRACT

Wi-Fi signals are typically information carriers between a transmitter and a receiver. In this paper, we show that Wi-Fi can also extend our senses, enabling us to see moving objects through walls and behind closed doors. In particular, we can use such signals to identify the number of people in a closed room and their relative locations. We can also identify simple gestures made behind a wall, and combine a sequence of gestures to communicate messages to a wireless receiver without carrying any transmitting device. The paper introduces two main innovations. First, it shows how one can use MIMO interference nulling to eliminate reflections off static objects and focus the receiver on a moving target. Second, it shows how one can track a human by treating the motion of a human body as an antenna array and tracking the resulting RF beam. We demonstrate the validity of our design by building it into USRP software radios and testing it in office buildings.

Categories and Subject Descriptors C.2.2 [**Computer Systems Organization**]: Computer-Communications Networks. H.5.2 [**Information Interfaces and Presentation**]: User Interfaces - Input devices and strategies.

Keywords Seeing Through Walls, Wireless, MIMO, Gesture-Based User Interface

SIGCOMM'13, August 12–16, 2013, Hong Kong, China.

signal power after traversing the wall twice (in and out of the room) is reduced by three to five orders of magnitude [11]. Even more challenging are the reflections from the wall itself, which are much stronger than the reflections from objects inside the room [11, 27]. Reflections off the wall overwhelm the receiver's analog to digital converter (ADC), preventing it from registering the minute variations due to reflections from objects behind the wall. This behavior is called the "Flash Effect" since it is analogous to how a mirror in front of a camera reflects the camera's flash and prevents it from capturing objects in the scene.

So how can one overcome these difficulties? The radar community has been investigating these issues, and has recently introduced a few ultra-wideband systems that can detect humans moving behind a wall, and show them as blobs moving in a dim background [27, 41] (see the video at [6] for a reference). Today's state-of-the-art system requires 2 GHz of bandwidth, a large power source, and an 8-foot long antenna array (2.4 meters) [12, 27]. Apart from the bulkiness of the device, blasting power in such a wide spectrum is infeasible for entities other than the military. The requirement for multi-GHz transmission is at the heart of how these systems work: they separate reflections off the wall from reflections from the objects behind the wall based on their arrival time, and hence need to identify sub-nanosecond delays (i.e., multi-GHz bandwidth) to filter the flash effect.[1] To address these limitations,

[1] Filtering is done in the analog domain before the signal reaches the ADC.
[2] Wi-Vi stands for Wi-Fi Vision.

Here: Wi-Fi as **covert** source

← building U park poster

Transmitter/receiver architecture

- Continuously broadcast Wi-Fi messages (either streaming or B. Bloessl's `packetspammer` [1])
- Unknown broadcast signal must be recorded on **reference** channel while surveillance channel monitors reflections from targets
- Non-cooperative source: detect periods of silence and repeat emission until enough signal is accumulated,

But ...

- Limited bandwidth from emitter (Wi-Fi channel width) and receiver (B210 to RPi4) $\Rightarrow$ **frequency stacking** [2] by sweeping frequency, assuming the scene remains static during the acquisition
- **Cross correlation** ($\int f(t)f(\tau - t)dt \rightarrow \int f(t)f(\tau + t)dt$) as

$$iFFT\{FFT(surveillance) \cdot FFT^*(reference)\}$$

  so that frequency stacking is naturally performed by accumulating spectra in the frequency domain prior to iFFT
- Cross correlation as

$$iFFT\{FFT(surveillance)/FFT(reference)\}$$

  to get rid of spectrum **envelope fluctuations** (ratio of amplitude but still phase subtraction)

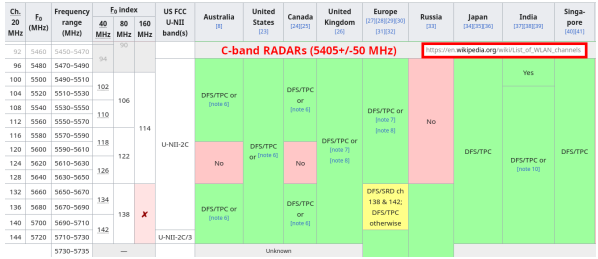
[1] `https://github.com/bastibl/gr-ieee802-11/tree/maint-3.10/utils/packetspammer`

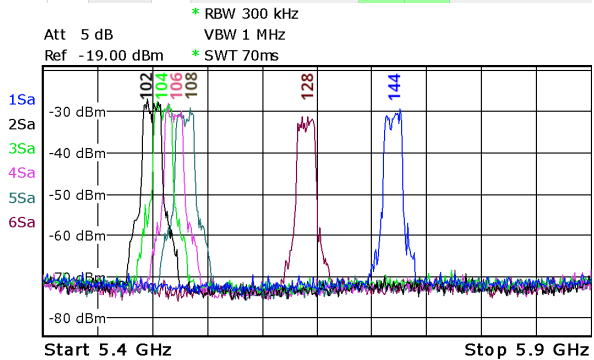
[2] S. Prager *& al.*, *Ultrawideband synthesis for high-range-resolution software-defined radar*, IEEE Transactions on Instrumentation and Measurement **69**(6) 3789–3803 (2019)

Frequency stacking for improved range resolution

- Broadcast starts above C-band RADAR range (> 5455 MHz)
- 20 MHz wide signal for each channel ...
- ... recorded as two 10-MHz wide sub-spectra with the B210 (USB/RPi4 limitation) centered on channel-5 MHz and channel$+5$ MHz
- run through all channel indexes from 96 to 144
- gaps in some channels (be careful when dividing $FFT(surveillance)/FFT(ref)$ to avoid division by 0)
- Streaming (0-MQ) from the B210 to control software for processing (would greatly benefit from Raspberry Pi GPU[a] !)

[a] S. Azarian, *Using GPU for real-time SDR Signal processing*, FOSDEM 2024

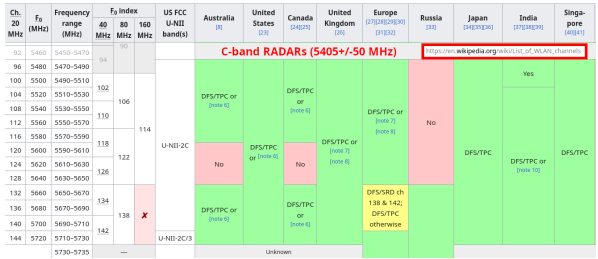


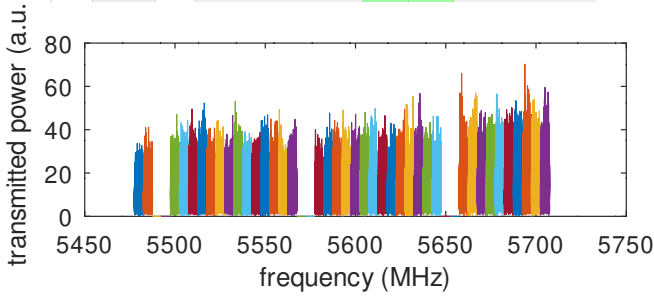


Frequency stacking for improved range resolution

- Broadcast starts above C-band RADAR range (> 5455 MHz)
- 20 MHz wide signal for each channel ...
- ... recorded as two 10-MHz wide sub-spectra with the B210 (USB/RPi4 limitation) centered on channel-5 MHz and channel$+5$ MHz
- run through all channel indexes from 96 to 144
- gaps in some channels (be careful when dividing $FFT(surveillance)/FFT(ref)$ to avoid division by 0)
- Streaming (0-MQ) from the B210 to control software for processing (would greatly benefit from Raspberry Pi GPU[a] !)

[a] S. Azarian, *Using GPU for real-time SDR Signal processing*, FOSDEM 2024



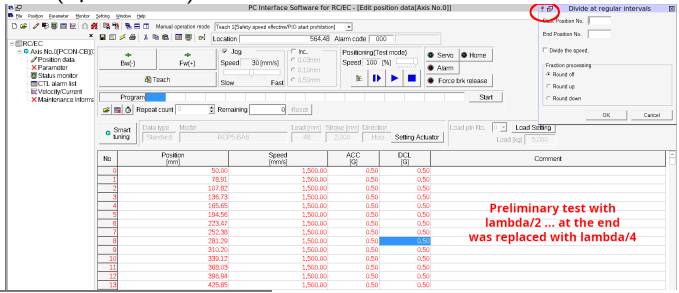


Rail control

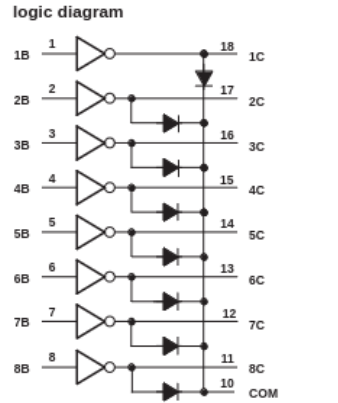
24 V GPIO from Raspberry Pi (Industrial PLC[a] standard):

- pre-record up to 128 locations on the rail (proprietary software running under Wine)
- set location at $N \times \lambda/4$, $N \in \mathbb{N}$
- set the 7-bit GPIO to the position index
- toggle enable signal

2× ULN2803A Darlington transistor array as opencollector driving circuit (up to 50 V)



[a]Programmable Logic Controller

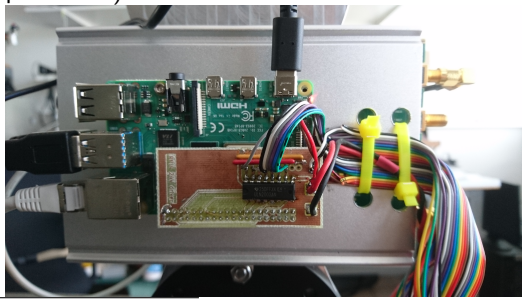


Rail control

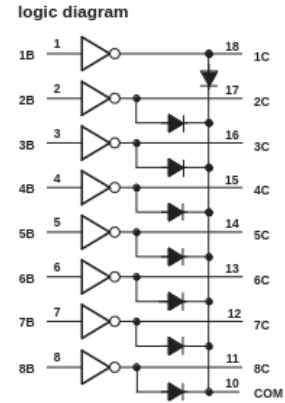
24 V GPIO from Raspberry Pi (Industrial PLC[a] standard):

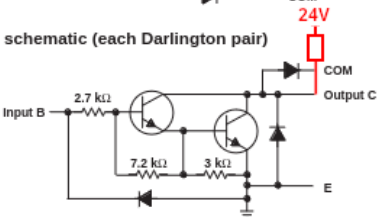
- pre-record up to 128 locations on the rail (proprietary software running under Wine)
- set location at $N \times \lambda/4$, $N \in \mathbb{N}$
- set the 7-bit GPIO to the position index
- toggle enable signal

2× ULN2803A Darlington transistor array as opencollector driving circuit (up to 50 V)



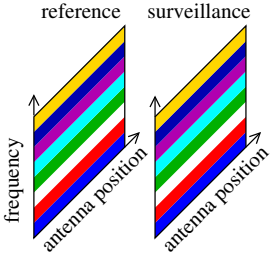
[a]Programmable Logic Controller

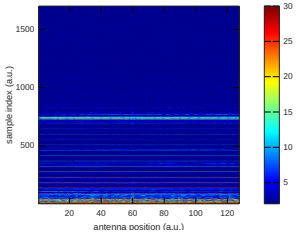


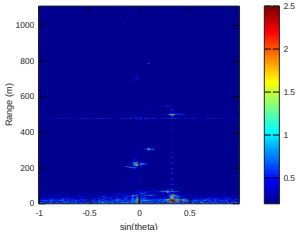


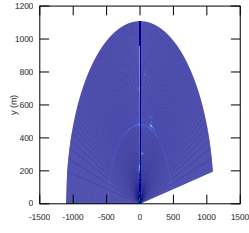
SAR processing [4]

$$(time - antenna\ position) \underbrace{\rightarrow}_{FFT_t/FFT_t} (range - antenna\ position) \underbrace{\rightarrow}_{FFT_x} (range - azimuth) \underbrace{\rightarrow}_{map} (X, Y)$$









FFT along time (correlation) and FFT along antenna position [3] are orthogonal and combined in 2D-FFT

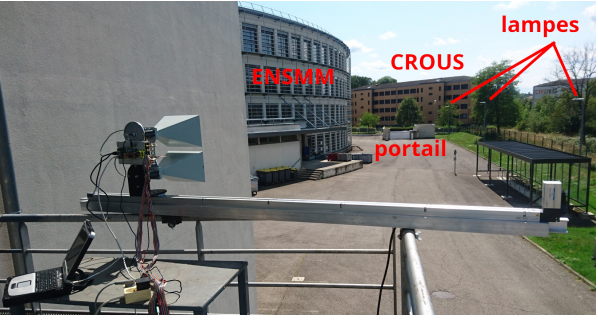
No degree of freedom other than direction adjustement, all scales are determined by sampling rate (range) and antenna step/wavelength (azimuth)

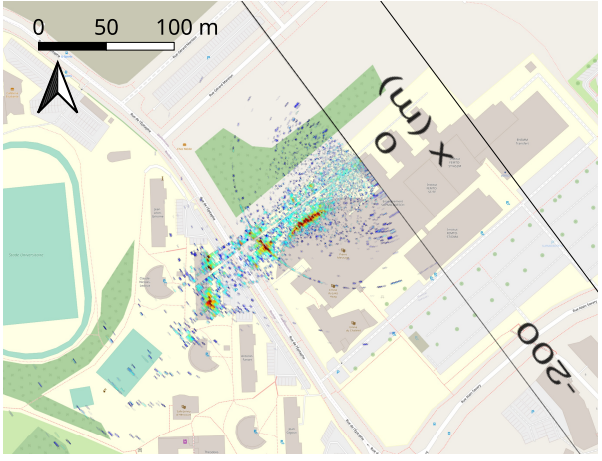
[3] J.-M Friedt, W. Feng, *Software defined radio based Synthetic Aperture noise and OFDM (WiFi) RADAR mapping*, 10th GNU Radio Conference 2020 at `https://pubs.gnuradio.org/index.php/grcon/article/view/71`

[4] Acknowledgement: Weike Feng, Air force Engineering University, Xi'an, China for providing range-azimuth to XY migration script

Results: amplitude analysis (Westward)

- overlay with OpenStreetMap background in QGis [a] after scaling to match distances (XY), origin at **known** SDR-GB-SAR location
- only **degree of freedom**: rotation
- "circular" shape of the left building
- portal and lamps visible as is the building blocking further view (150 m range)

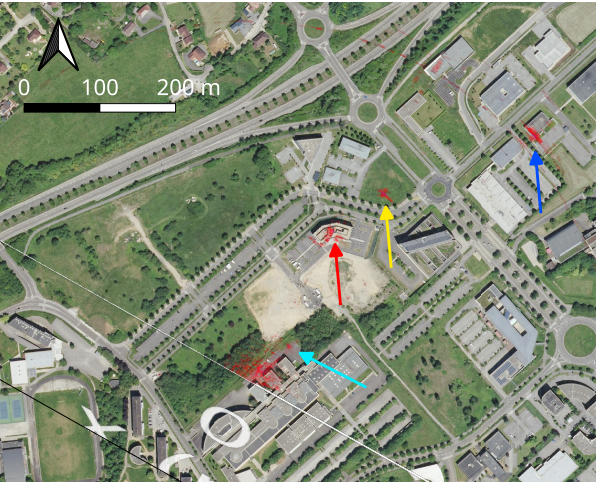




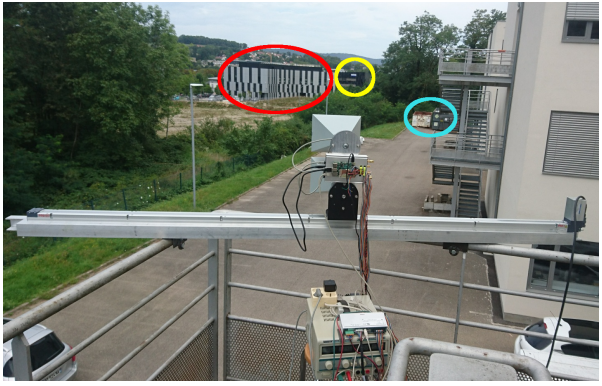
Threshold backscattered power to make background transparent

[a] "Freehand raster georeferencer" plugin

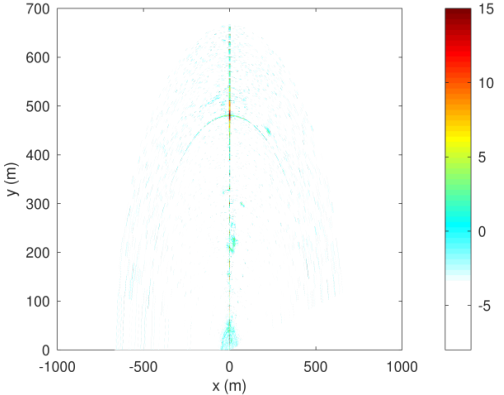
Results: amplitude analysis (Eastward)

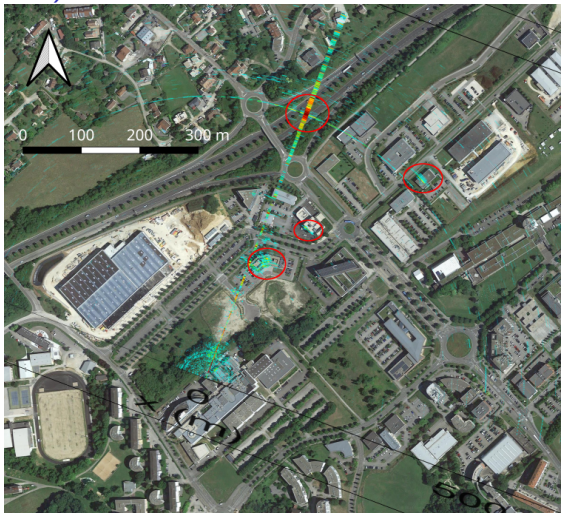


- Some trees to the left blocking the view, but antenna beam is only 18° wide anyway (20 dBi antenna)
- measurement at > 500 m range
- nearby metallic container (cyan), newly built building not yet visible on Google Maps (yellow)



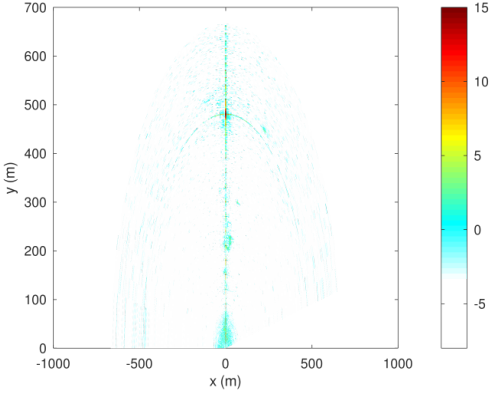
Results: amplitude analysis (Eastward)

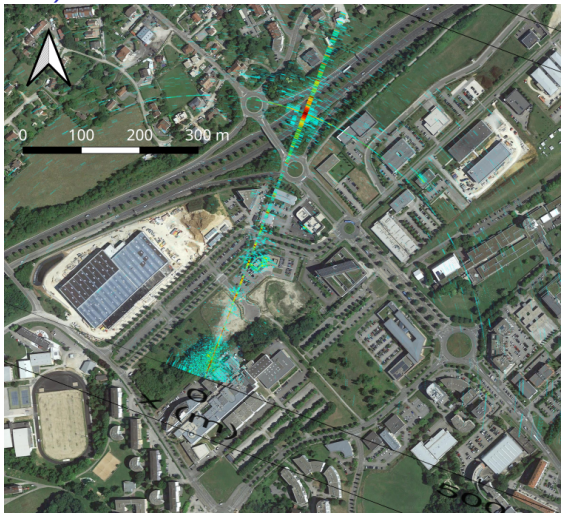




Background: Google Maps

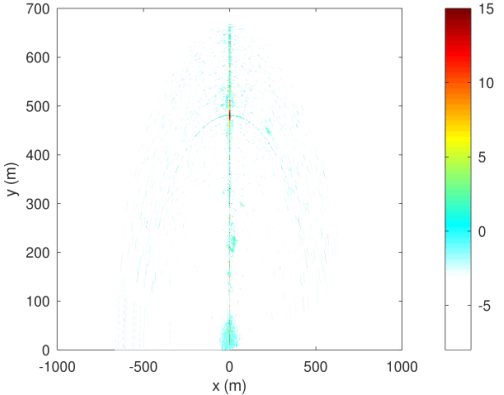
Results: amplitude analysis (Eastward)

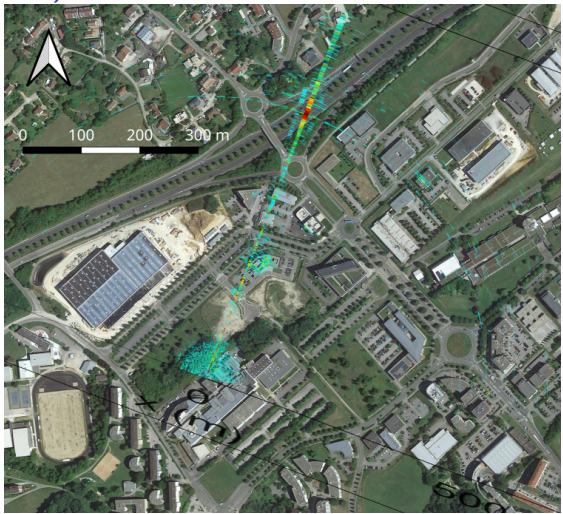




Background: Google Maps

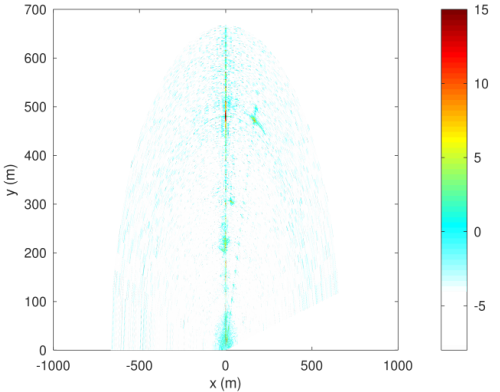
Results: amplitude analysis (Eastward)

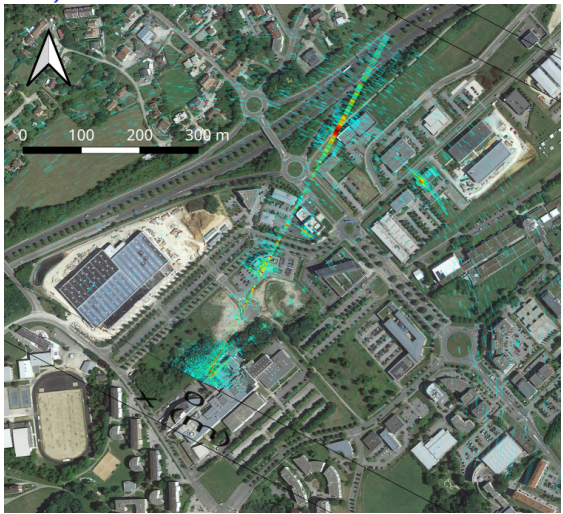




Background: Google Maps

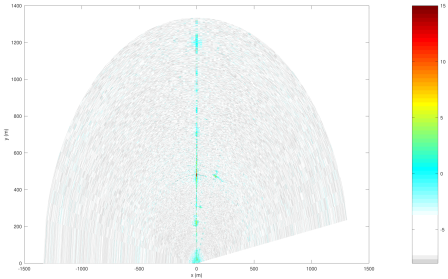
Results: amplitude analysis (Eastward)

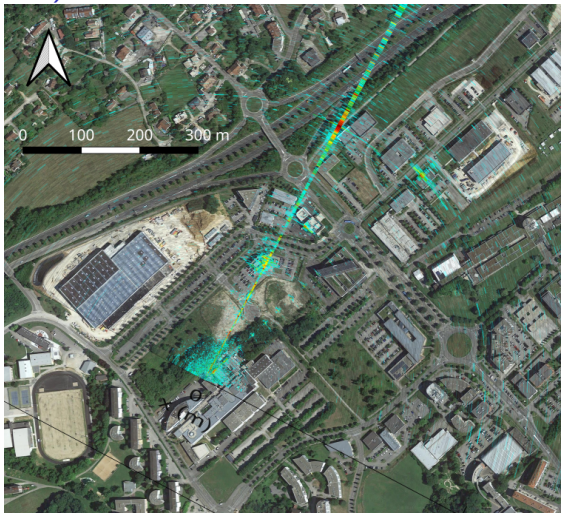




Background: Google Maps

Results: amplitude analysis (Eastward)



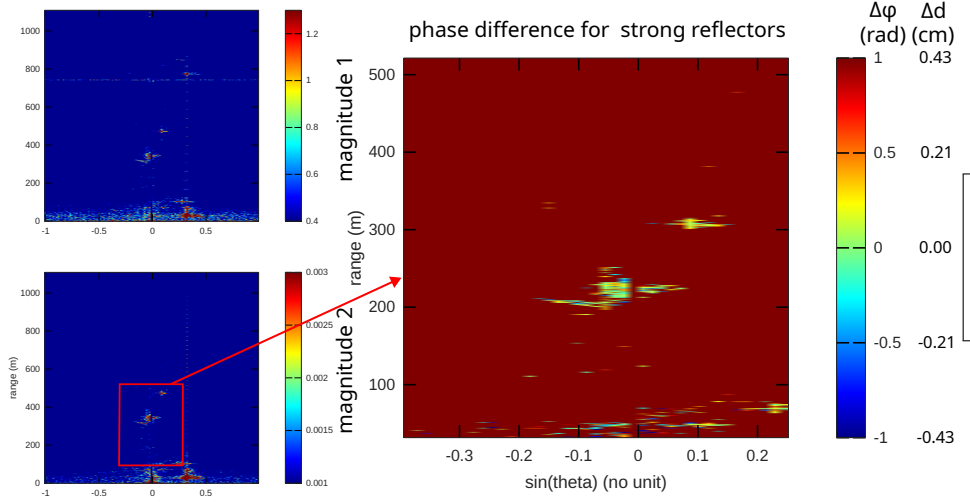


Longer range (more samples in the time domain, less averages)
Measurement duration $\simeq$ 15 minutes/image

Background: Google Maps

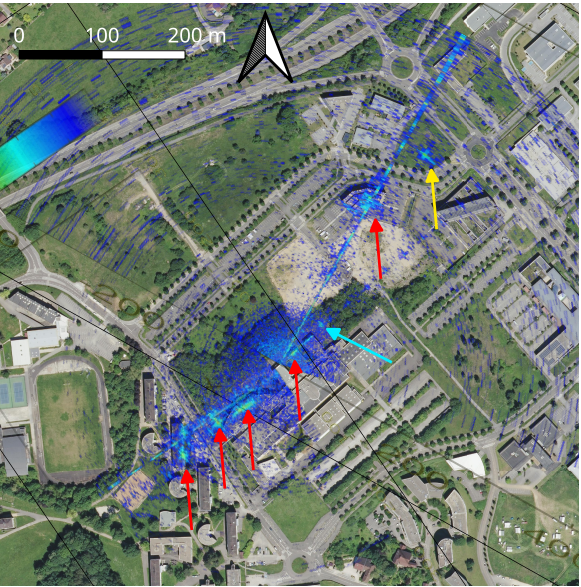
Results: phase analysis (Eastward) between two successive measurements

- InSAR (Interferometric Synthetic Aperture RADAR): phase analysis **but with $\lambda/2$** uncertainty
- Phase rotates by 2π for every λ path difference in the two-way trip $\Rightarrow \Delta d = \frac{\lambda}{2} \times \frac{\Delta\varphi}{2\pi}$
- known $\lambda \Rightarrow$ known Δd for a measured $\Delta\varphi$



Results (no movement):
$\langle\Delta\varphi\rangle \simeq 7 \cdot 10^{-4}$ m
$\sigma_{\Delta\varphi} \simeq 1.5 \cdot 10^{-3}$ m
$\Rightarrow 0.7 \pm 1.5$ mm=0

Conclusion



- Demonstrated a functional opensource, openhardware SDR-GB-SAR with 500 m range
- Covert emission using COTS 5.8 GHz Wi-Fi emitter
- ... and a dual channel coherent SDR receiver
- SAR and InSAR signal processing
- Cost estimate:

Item	Supplier/reference	Price (euros)
Antennas	A-Info LB-159-20-C-SF	2×807
Accessories	A-Info LB-159-10-C-MBL	2×202
B210	Ettus Research/NI	2160
Pluto+	Aliexpress	302
Rail	IAI[a]	1965+395
Wi-Fi[b]	Amazon	30
Passive RF	MiniCircuits	100
RPi4	Radiospares	100
Total		6768

- `https://github.com/jmfriedt/SDR-GB-SAR/`

[a] RCP5-BA6-WA-42P-48-2000-P3-S-CJT
[b] Alfa Network AWUS036ACS (RTL8812AU based)

Acknowledgements: Philippe Abbé and Vincent Tissot – FEMTO-ST mechanical workshop – for mechanical part manufacturing