

Real time GNSS spoofing detection and cancellation on embedded systems using Software Defined Radio

J.-M. Friedt*, W. Feng[†], D. Rabus*, G. Goavec-Merou*

*FEMTO-ST/Time & Frequency, Besançon, France, jmfriedt@femto-st.fr

[†]Xidian University, National Laboratory of Radar Signal Processing, Xi'an, China

Abstract—Global Navigation Satellite Systems have become ubiquitous to most daily activities requiring Positioning, Navigation and Timing and yet have become increasingly subject to spoofing and jamming, partly due to the availability of affordable software defined radio platforms allowing such functionalities. Despite novel modulation schemes and broader frequency bands, GPS L1 at 1575.42 MHz remains the main signal source for most consumer grade receivers. We address here real time spoofing and jamming mitigation using a software defined radio approach in which the raw (I, Q) coefficients collected by the radiofrequency frontend are analyzed for spoofing detection by assessing the phase difference of the GPS signals collected by different antennas. These signals are possibly cleaned from the interfering sources by null-steering when spoofing or jamming is detected, and the cleaned signal are used for real time Position and Navigation information extraction using the opensource `gnss-sdr` framework. The application to other frequency bands is considered for redundancy and detecting spoofing attacks. Timing information is under consideration as well.

Index Terms—software defined radio, spoofing cancellation, jamming cancellation

I. INTRODUCTION: SOFTWARE DEFINED RADIO BASED CRPA

Software Defined Radio (SDR) provides the means for widespread spoofing capability with minimum financial investment, while the ubiquity of Global Navigation Satellite Systems (GNSS) leads to increasing impact of such threat [1]. Despite the advent of new constellations with advanced security on the digital messages, legacy receivers are expected to be in use for the coming years. Thus, mitigation of spoofing and jamming threats on the GPS L1 band is addressed using SDR receivers [2] and more specifically the opensource `gnss-sdr` SDR GNSS decoding software running on top of the opensource GNU Radio framework.

CRPA (Controlled Radiation Pattern Receiver) is a well known null-steering approach to jammer and spoofer cancellation in GNSS prone to such attacks considering the weak signals reaching the ground from satellites over 20000 km away from the receiver, actually below thermal noise. Signal processing techniques require on the one hand to identify the characteristics of the spoofer or jammer, and on the other hand to tune the phase between various antenna elements to cancel this contribution and allow for recovering the genuine signal. While classically performed in the analog domain (e.g. radiofrequency phase shifters), software defined radio GNSS receivers are well suited to such a task since providing access

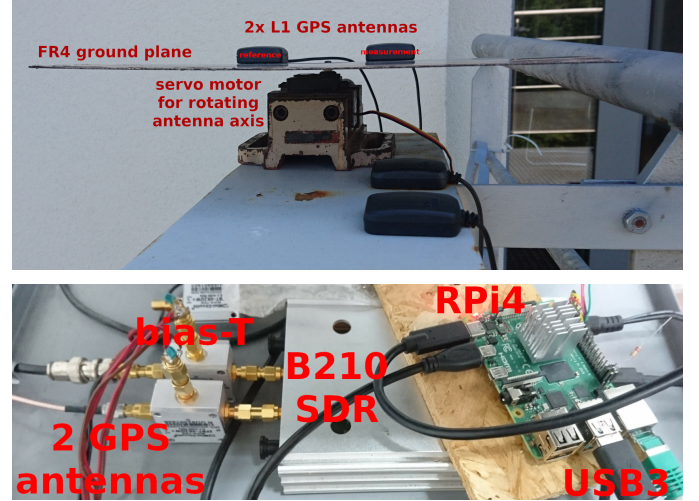


Fig. 1. Experimental setup: an Ettus Research B210 Software Defined Radio platform is fed through bias-T polarization circuits by the signal collected by active antennas in clear view of the sky. The resulting datastream is transmitted through the USB3 bus to a Raspberry Pi4 (RPI4) single board computer. The antennas are attached to a rotating, FR4 copper-coated printed circuit board, ground plane to simulate the motion of the spoofing or jamming source with respect to the CRPA array.

to the raw (I, Q) samples and hence the physical characteristics of the incoming electromagnetic waves. In this paper, we demonstrate real time jamming and spoofing cancellation using a codeless demodulation technique implemented at the signal acquisition level of `gnss-sdr` to process the datastream and provide Navigation and Positioning information from the genuine constellation despite interfering sources. All experimental demonstrations are performed with two antennas in clear sky view of the genuine GPS constellation with spoofing and jamming signals generated nearby and transmitted wirelessly in a scenario representative of practical attacks (Fig. 1), weak enough for this illegal emission demonstration to hardly disturb legal receivers beyond the university building. The extension to other frequency bands is addressed and the current limitation of SDR is discussed in the context of Commercial, Off The Shelf (COTS) hardware.

II. SPOOFING DETECTION AND CANCELLATION

The benefit of a SDR approach to GNSS signal processing is the access to the raw radiofrequency datastream allowing to characterize the electromagnetic wave propagation properties.

The (I,Q) datastream generated after radiofrequency frequency transposition to baseband and sampling by the analog to digital converters contains the sum of the contributions of all satellite signals. Spoofing attack detection, assuming a single spoofing source, will rely on analyzing direction of arrival (DoA) of the various contributions after sampling with multiple antennas the signal (Fig. 2). In our demonstration, an Ettus Research B210 dual-channel receiver is used, sampling at 1.123 MS/s the L1 band centered on 1575.42 MHz with 12-bit resolution. The AD9361 radiofrequency frontend fitted on this SDR platform clocks both receiver input channels with the same local oscillator, allowing for phase analysis to extract DoA information.

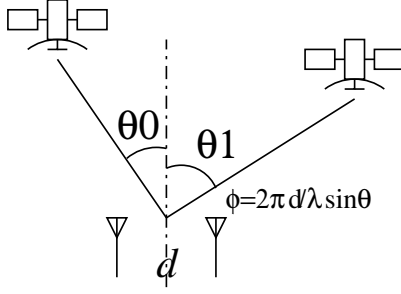


Fig. 2. Basic principle of the CRPA approach: a genuine constellation will exhibit a diversity of directions of arrival measured as a diversity of phases between two antennas collecting GNSS signals. A unique spoofer might mimic the Doppler shift, code and navigation messages of the constellation but the phase difference between antennas, defined by electromagnetic wave propagation physics, cannot be spoofed. d is the distance between antennas inducing a phase difference φ between the two antennas illuminated by the signals at angle θ which is practically a combination of azimuth and elevation.

Since GNSS Code Division Multiple Access (CDMA) encoded Binary Phase Shift Keying (BPSK) modulation spreads power below thermal noise, DoA measurement requires removing the CDMA modulation to bring the relevant information above thermal noise. The two general approaches to spoofing detection by analyzing the radiofrequency wave characteristics involve pre- and post-despreading computation, where either the full GNSS correlation can be performed in the latter case or where compression is computed prior to correlation with no knowledge of the CDMA characteristics. The former approach, also known as codeless analysis, is considered here for its computational efficiency. Indeed, BPSK modulation is canceled by squaring the signal, so that the modulated phase equal to 0 or π doubles as the argument of the squared complex $(I + jQ)$ become 0 modulo 2π and the energy is concentrated in the carrier raising above the thermal noise. While the Pseudo Random Number (PRN) sequence encoding which Space Vehicle signal was received has been lost in the process, the Doppler shift still allows for differentiating the various satellite contribution to the signal. Even a properly spoofed signal will introduce realistic Doppler shifts for each satellite signal, consistent with its azimuth and elevation. However, the phase difference between antennas is only determined by plane wave propagation characteristics and

cannot be spoofed. Thus, observing the phase at the various frequency offsets of the discrete peaks in the Fourier transform at double the Doppler shift (due to the squaring process) allows for assessing spoofing. If all phases are close, despite satellites being distributed in azimuth and elevation as would be expected from a genuine constellation, then spoofing is identified. Sorting the phases and analyzing their standard deviation is used for automating the spoofing detection.

Formally, considering that antenna a receives satellite i signal as

$$s_a(t) = A_a(t) \exp(j(\underbrace{\delta\omega_i t}_{\text{Doppler}} + \underbrace{\varphi_{PRN,i}}_{\text{BPSK}} + \underbrace{\varphi_{a,i}}_{\text{geometric}})) \quad (1)$$

with Doppler shift $\delta\omega_i$, BPSK modulated code $\varphi_{PRN,i} \in [0, \pi]$, and geometrical phase $\varphi_{a,i}$, then squaring the signal cancels the PRN modulation and the associated energy spreading as

$$s_a^2(t) = A_a^2(t) \exp(j(2\delta\omega_i t + 2\varphi_{a,i})) \quad (2)$$

and the contributions of the various satellites are separated by their different Doppler shifts in the Fourier transform of the squared signals. The weight of the spoofing signal is deduced from the ratio of these (complex) coefficients

$$\frac{FFT(s_1^2(t))}{FFT(s_2^2(t))} = \frac{A_1^2(t)}{A_2^2(t)} \exp(2j(\varphi_{1,i} - \varphi_{2,i})) \quad (3)$$

computed at bin $\delta\omega_i$ of the Fourier transform.

If all $\varphi_{1,i} - \varphi_{2,i} \forall i$ are close, a spoofing attack is detected through a threshold on the standard deviation analysis on $\varphi_1 - \varphi_2$ (Fig. 3).

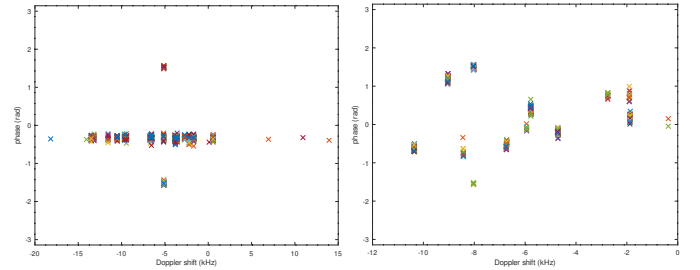


Fig. 3. Left: spoofing of the GPS constellation in the L1 frequency band with the antennas facing the sky: most phases are the same with only a couple of genuine satellites detected, indicative of a spoofing attack. Right: genuine constellation exhibiting the diversity of phases representative of the diversity of the directions of arrival.

As adjacent antenna phase and relative magnitude is computed as argument and module of each Fourier transform of the squared signal spectral component, identifying spoofed contributions as the signals with close phases allows for identifying the DoA and hence for null-steering by using destructive interference in this direction to cancel the spoofing signal. Applying this processing *after* analog-to-digital conversion requires a high resolution sampling as the genuine signal must remain above the least significant bit quantization level while avoiding saturation of the received signal including the possibly strong spoofing contribution. Thus, classical low-resolution

(1- or 2-bit resolution as provided for example by Maxim IC MAX2771 receiver) sampling techniques classically used for GNSS reception might not be suitable for spoofing (and jamming) cancellation as post-processing steps.

III. COMPUTATIONALLY EFFICIENT ALGORITHMS IMPLEMENTATION IN `gnss-sdr`

These concepts are implemented in the early data collection of `gnss-sdr` for real time processing and decoding. While `gnss-sdr` is organized in a strict hierarchy of processing planes from Signal Source to Position, Velocity and Time extraction with intermediate processing steps including Signal Conditioning, Acquisition, Tracking, and Decoding, we have included the jamming and spoofing cancellation in the Signal Source acquisition in order to accept data streaming from multiple sources. Indeed, CRPA requires multiple antennas to identify and cancel the interfering signal, in our case the datastream from the two channels of the B210 receiver.

TABLE I

COMPARISON OF THE WEIGHT COMPUTATION USING INVERSE FILTERING (IF AS INTEGRAL OF THE RATIO OF THE FOURIER TRANSFORMS AS 0-DELAY CORRELATION) AND THE STOCHASTIC GRADIENT LEAST SQUARE (LS) METHOD. NOTICE THE CONSISTENCY OF THE COMPLEX WEIGHT WITH A LARGE MODULE IN CASE OF JAMMING (LEFT) AND THE NEGLIGIBLE WEIGHT IN THE ABSENCE OF JAMMING (RIGHT): A THRESHOLD IS USED FOR JAMMING DETECTION AND APPLYING THE CANCELLATION BY SUBTRACTING THE WEIGHTED MEASUREMENT FROM ONE ANTENNA TO THE SECOND ANTENNA SIGNAL AS JAMMING LEADS TO 1000-FOLD STRONGER WEIGHTS.

With jamming	No jamming
IF 0.1809+i*0.3856	IF 0.0606+i*-0.0125
LS (0.2191,0.4710)	LS (0.00027,0.00011)
LS (0.2196,0.4684)	LS (0.00037,0.00014)
IF 0.1779+i*0.3678	LS (0.00046,0.00018)
LS (0.2125,0.4629)	IF 0.06623+i*0.00309
LS (0.2127,0.4668)	LS (0.00064,0.00026)
IF 0.1781+i*0.3618	LS (0.00073,0.00029)
LS (0.2121,0.4662)	LS (0.00082,0.00033)
LS (0.2129,0.4649)	LS (0.00092,0.00036)
LS (0.2138,0.4657)	IF 0.06576+i*0.01101

Running efficiently on an embedded board requires cross-compiling `gnss-sdr` to the embedded General Purpose Central Processing Unit (GP-CPU) with maximum performance: `gnss-sdr` is included in the Buildroot framework allowing the use of the SIMD instruction set of the processor fitted on the Raspberry Pi4 single board computer. These SIMD instruction are heavily used by the Vector Optimized Library of Kernels (VOLK) developed as part of the GNU Radio framework with 3 to 7-fold speed improvement over the generic function implementation [3]. As the handled quantities are best represented as vectors, using the VOLK implementations such as `volk_32fc_x2_multiply_32fc()` for squaring complex vectors or `volk_32fc_x2_divide_32fc()` for computing the ratio of the Fourier transforms of the two squared channels samples provides significant computational speed benefit. Jamming cancellation cannot benefit from the known structure of the interfering signal and a least square (LS) approach is used to identify the contribution of the

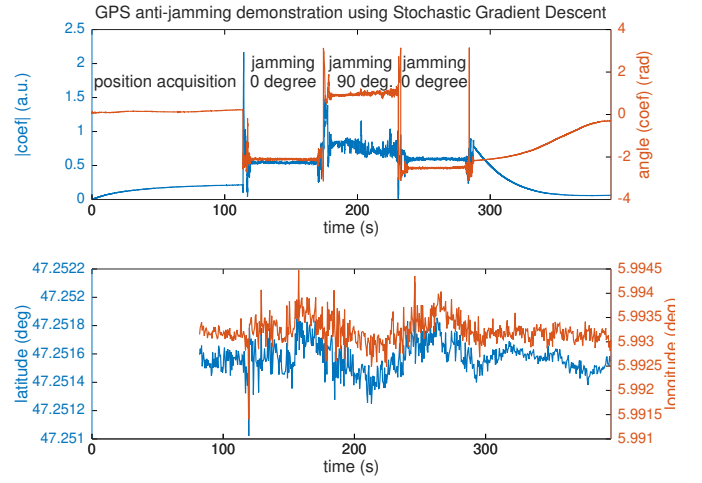


Fig. 4. Moving jammer cancellation: the set of antennas is positioned on a rotating stage in clear view of a sky. A nearby jammer prevents the signal acquisition if no cancellation occurs. After initial position acquisition, the jammer is switched on at date 110 s, the antenna rotated by 90° at date 180 s and back to its initial orientation at date 220 s, and finally the jamming source is switched off at 290 s.

jamming signal on one antenna and subtract it from the second antenna: rather than implement a matrix pseudo-inverse, a stochastic gradient descent algorithm has been implemented to iteratively converge towards the complex weight identification. Alternatively, the 0-delay coefficient of the cross-correlation function computed as the ratio of the Fourier transforms (rather than the product of the complex conjugate since here the ratio of the magnitudes is required to identify the weight) followed by an integration as an efficient computation of the 0-delay inverse Fourier transform coefficient is implemented as jamming cancellation algorithm (Tab. I): this inverse filtering approach has been used for demonstration on a moving jammer (Fig. 4).

IV. MULTIBAND APPLICATION

One protection against spoofing or jamming is redundancy by analyzing the information transmitted on multiple frequency bands. While the civilian L1 band around 1575.42 MHz is most commonly used, the multiple constellations (GLONASS, Beidou, Galileo) will allow to address spoofing attacks by assessing consistency of the signals, and each one of these constellations is transmitting on multiple frequency bands. Nevertheless, a careful enough attacker might generate spoofing signals in all such frequency bands, and extending the CRPA approach to all bands is desirable. One limitation of SDR is the signal bandwidth limited by digital communication bandwidth: with GNSS bands separated by more than 400 MHz, multiple receivers are needed to address all bands.

We consider the L5 band around 1176.45 MHz as a complement to L1 reception (Tab. II), despite fewer satellite currently emitting this signal (Fig. 5). L5 uses a 10-times longer PRN code than L1 C/A so that the bandwidth is increased 10-fold.

Lat: 47.2516269° Time: 13:25:06
Long: 5.9932088° TTFF: 2 sec
Alt: 357.0 m E H Acc: 15.2 m
Alt (MSL): 309.0 m # Sats: 10/22/30
Speed: 0.0 m/s Bearing:
PDOP: 1.7 H/V DOP: 1.4/0.9

ID	GNSS	C/N0	Flags	Elev	Azim
1		13.8	AE	37°	136°
3		17.8	AEU	69°	53°
4			A	64°	178°
6		22.8	AEU	25°	307°
9		14.2	A	29°	210°
11			A	6°	156°
12			A		
17		18.4	AEU	40°	265°
19		20.3	AEU	36°	289°
22		21.6	AEU	48°	78°
31		16.4	A	18°	50°
1		14.4	A	10°	52°

Fig. 5. GPS constellation configuration during the L5 acquisition experiment: the useful satellites have been highlighted in red in the edited screenshot of GPSTest software running on a Sony Z5 mobile phone.

Furthermore, the Binary Offset Carrier (BOC) modulation leads to a poorer signal to noise ratio when applying a basic codeless processing technique [4], [5], and hence requires longer integration time to raise the signal above noise in a codeless decoding approach (Fig. 6).

TABLE II
L1 SIGNAL SAMPLED WITH 8-BIT RESOLUTION AT 11.23 MS/S AND
DECODED USING gnss-sdr WITH THE CONTRIBUTION OF SPACE
VEHICLES CONSISTENT WITH THE LIST SHOWN IN FIG. 5.

```
New GPS NAV message received in channel 2: subframe
3 from satellite GPS PRN 04 (Block Unknown)
New GPS NAV message received in channel 4: subframe
3 from satellite GPS PRN 09 (Block IIF)
New GPS NAV message received in channel 8: subframe
3 from satellite GPS PRN 19 (Block IIR)
New GPS NAV message received in channel 6: subframe
3 from satellite GPS PRN 17 (Block IIR-M)
New GPS NAV message received in channel 1: subframe
3 from satellite GPS PRN 03 (Block IIF)
Current receiver time: 1 min 19 s
First position fix at 2020-Oct-10 11:29:30.300000 UTC
is Lat = 47.2516 [deg], Long = 5.99321 [deg], Height=
338.448 [m]
Position at 2020-Oct-10 11:29:30.500000 UTC using 4
observations is Lat = 47.251578218 [deg], Long =
5.993222004 [deg], Height = 336.211
Velocity: East: -0.890 [m/s], North: -1.676 [m/s],
Up = 3.507
Position at 2020-Oct-10 11:29:31.000000 UTC using 4
observations is Lat = 47.251630849 [deg], Long =
5.993326694 [deg], Height = 299.172
```

Nevertheless, the underlying BPSK modulation remains cancelled by squaring and the same processing technique can be used as was demonstrated with L1 (Fig. 7). Similarly, L2 around 1227.6 MHz now transmits a civilian signal which is

considered as a complement to L1 and L5, with a narrower bandwidth better suited for SDR investigations. All these signals are collected by feeding one input channel of the B210 receiver with the output of a Septentrio PolaNt-x MF broadband antenna. Samples were collected either with a Dell Precision M6500 laptop or a Raspberry Pi4, in both cases using the USB3 port.

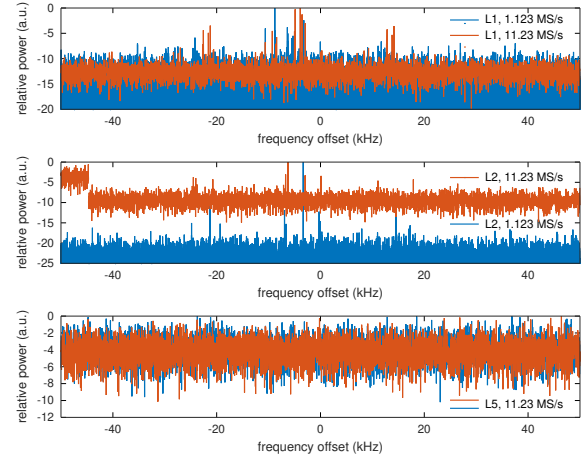


Fig. 6. Codeless analysis of the L1 (top), L2 (middle) and L5 (bottom) signals sampled at 1.123 MS/s (L1 and L2) or 11.23 MS/s (L1, L2 and L5 twice) sequentially. The various satellites are visible as different Doppler shifts (frequency offsets) for L1 and L2 BPSK modulation but the signal to noise ratio is insufficient for the L5 modulation in these 1-second integration durations. Notice that the abscissa is twice the Doppler shift due to squaring the signal.

As was done with L1, we consider a 10% margin when selecting the sampling rate and 11.23 MS/s is used to record L5 I/Q data for post-processing. Indeed, we have observed that real time processing is beyond the current GP-CPU fitted in consumer electronics computers and post-processing is used in this demonstration. The B210 frontend, Analog Devices AD9361, samples I and Q coefficients with 12-bit resolution, leading to 16-bit complex data requiring 32-bit transfers for each sample. At a sampling rate of 11.23 MS/s, the resulting data-rate of 44.92 MS/s is observed to be beyond the bandwidth of the USB3 bus, and reducing the data resolution to 8-bit is mandatory to avoid sample loss.

The L5 signal quality was assessed by running a post-processing analysis using gnss-sdr. Indeed, the position was retrieved from the collected data

```
[...]
Current receiver time: 38 s
New GPS L5 CNAV message received in channel 0:
ephemeris from satellite GPS PRN 01 (Block IIF)
New GPS L5 CNAV message received in channel 1:
ephemeris from satellite GPS PRN 03 (Block IIF)
New GPS L5 CNAV message received in channel 2:
ephemeris from satellite GPS PRN 04 (Block Unknown)
New GPS L5 CNAV message received in channel 4:
ephemeris from satellite GPS PRN 09 (Block IIF)
First position fix at 2020-Oct-10 11:18:19.240000
UTC is Lat = 47.2513 [deg], Long = 5.99305 [deg],
Height= 431.628 [m]
```