Software-Defined Radio Implemented GPS Spoofing and Its Computationally Efficient Detection and Suppression

Weike Feng, Jean-Michel Friedt, Gwenhaël Goavec-Merou, François Meyer

Software Defined Radio Implemented GPS Spoofing and Its Computationally Efficient Detection and Suppression

Weike Feng *Member, IEEE,* Jean-Michel Friedt, Gwenhael Goavec-Merou, François Meyer

***Abstract*—This paper demonstrates Global Positioning System (GPS) spoofing with a commercial, off the shelf software defined radio (SDR) emitter fitted with a local oscillator exhibiting a stability consistent with the medium term (0.01 to 1000 s) stability of atomic clocks on GPS satellite systems. Computationally efficient means of detecting spoofing is then addressed, namely codeless spoofing detection by phase difference measurement of the signals received from a two-antenna array. We conclude by using a simple and effective method to suppress spoofing to restore positioning and time transfer capabilities, and extend the demonstration to jamming cancellation. Experiment results demonstrate the performance of the proposed methods with an emphasis on computational efficiency for real time execution on embedded single board computers.**

***Index Terms*—GPS, Spoofing, Detection, Suppression.**

I. Introduction

Global Navigation Satellite Systems (GNSS) and most significantly the Global Positioning System (GPS) have become ubiquitous in most modern activities since Selective Availability (SA) was canceled [1], from positioning to time synchronization of networks. Initially developed as a military system, the wide civilian use of GPS makes it a target to jamming and spoofing attacks [2], [3], which have recently become affordable to any Software Defined Radio (SDR) user [4], [5], as has been reviewed in [6] with a focus on processing acceleration peripherals. While jamming is readily detected as a denial of service, spoofing is more subtle since introducing erroneous datastreams into the GPS receiver will not lead to loss of service but might allow the attacker to shift the receiver position or synchronization time (1-Pulse Per Second output) at will [7].

Recently, anti-spoofing techniques have been extensively reported in the literature based on various feature differences between spoofing and authentic signals [8], [9]. In general, these techniques can be divided into two main categories in the literature: spoofing detection and spoofing suppression. Spoofing detection techniques[10]–[15], e.g., signal strength monitoring, spatial processing discrimination, time of arrival measurement[16], consistency cross-check, signal quality monitoring, and cryptographic authentication, try to detect the presence of spoofing attacks. Spoofing suppression techniques[17], [18] aim to mitigate the influences of spoofing signal to recover the positioning and time synchronization capabilities of a GPS receiver.

With the fact that authentic signals are coming from spatially distributed satellites and the assumption that spoofing signals are coming from the same direction (i.e., several pseudo random noise (PRN) codes are transmitted by a single spoofer at a specific location), multiple antenna based spatial processing has become one of the most powerful anti-spoofing techniques [19], [20]. Based on spatial beamforming technique and by properly combining signals from different antennas, spoofing signals can be mitigated by steering a deep null toward the direction of the spoofer. Similarly, jamming can be cancelled by beamforming, requiring a more generic signal processing approach to identify the steering vector of the jamming signal since no assumption can be made on its structure.

As indicated by [20], spatial processing techniques can be implemented at either the pre-correlation or the post-correlation stages of a GPS receiver. One of the classical methods that work at the pre-correlation stage is proposed in [17]. Assuming spoofing signals are received at a stronger power than authentic signals, this method cross-correlates the received signals from different antennas to estimate the phase term of the steering vector of spoofing signals. Then, with the assumption that the gains of the uncalibrated antennas keep unchanged for all spoofing and authentic signals from different directions, and by exploiting the inherent periodicity of PRN codes, the amplitude term of the steering vector has been estimated. This method has a low computational complexity and can be employed as a simple additional block before a conventional GPS receiver. Nevertheless, this method may not work well when the spoofing power is low as the phase term of the steering vector cannot be accurately estimated in such a case. Besides, the assumption of unchanged gains for different incoming signal directions may not be well satisfied in practice, and the integration for amplitude estimation may not accumulate coherently based on the periodicity of PRN when the navigation data bit changes, resulting in inaccurate amplitude estimation of the steering vector. On the contrary, the post-correlation spatial processing methods, such as the one proposed in [18], can avoid these problems as they can

This work was partly funded by the FAST-LAB ANR grant, and motivated by the FIRST-TF and Oscillator Instability Measurement Platform (IMP) PIA ANR grants.

J.-M. Friedt is an associate professor at Franche-Comté University with his research activities hosted by the Time & Frequency department of the FEMTO-ST Institute in Besançon, France. G.G.M and J.-M. F are with the FEMTO-ST institute, Time & Frequency department, Besançon, France. W.F is with Xidian University, Xian, China. F.M is with the OSU THETA, Besançon, France. D. Rabus (FEMTO-ST & FAST-LAB, France) assisted in tuning the `gnss-sdr` processing parameters for real time processing and in performing the mobile spoofing experiment. E-mail: jmfriedt@femto-st.fr.

work effectively in both low and high spoofing power cases and no antenna gain assumption or PRN periodicity has been used to estimate the steering vector. However, compared to the pre-correlation method, the computational load of the post-correlation methods is much increased and some modifications of the acquisition/tracking procedure are normally needed for a GPS receiver.

In this work, we propose an alternative spatial processing method to detect and suppress spoofing signals, where we also assume a single spoofing emitter since keeping synchronization of multiple spoofing sources is beyond the capability of a basic spoofing attack. Firstly, the codeless decoding approach [21] squares the received signal to get rid of the Binary Phase Shift Keying (BPSK) of GPS L1 C/A (or L2C although only the former will be tackled here) PRN codes and navigation messages, and the Doppler frequencies of the squared authentic and spoofing signals of different antennas (to be simplified, two antennas are used in this paper) are estimated by fast Fourier transform (FFT). Secondly, all the frequency peaks identified above the noise floor are extracted to measure their phase differences between two antennas. The phase differences are used to detect the spoofing phenomenon and to classify the frequency peaks into two groups to distinguish the authentic and spoofing signals for spoofing suppression purpose. At last, with the help of the method proposed by [17] or a stochastic gradient descent (SGD) based iterative least squares (LS) algorithm [22], which is also applicable to strong spoofing and jamming suppression, the steering vector of spoofing signals is formed and the orthogonal projection based beamforming technique [17] is used to suppress spoofing signals and restore authentic signals. The proposed method makes a trade-off between existing pre-correlation and post-correlation methods: it works well in low and high spoofing power cases, the gains of the uncalibrated antennas are assumed to be different for different incoming signal directions, the periodicity of PRN codes is not necessary to be used, and its performance can be improved in low SNR situations by increasing the integration time; it is computationally efficient and can be achieved by a compact, low cost microcontroller before the GPS receiver without running the full acquisition procedure.

The outline of the paper is as follows: in the first section, we demonstrate the ability to spoof GPS using Commercial, Off The Shelf (COTS) SDR hardware fitted with a sufficiently stable quartz oscillator to properly mimic medium (0.01-1000 s) term stability of atomic clocks. In the second section, we detect spoofing by using a codeless decoding approach to analyse the phase of the signals collected by a two-antenna array. In the third section, we demonstrate the suppression of the spoofing signal to allow for recovering the authentic signals by steering a null towards the spoofing source. Finally, in the last section, we show various experiment results to illustrate GPS spoofing suppression performance of the presented methods and their extension to jamming cancellation.

II. GPS SPOOFING DEMONSTRATION

This sections focuses on demonstrating the ability to spoof a GPS receiver using commonly available hardware. The Analog Devices Inc. PlutoSDR fitted with the AD9363 radiofrequency front-end appears suitable, in terms of carrier frequency and data-rate bandwidth, for spoofing GPS. Throughout this paper, the output power of the PlutoSDR is provided in dBm, while the software configuration parameter is an attenuation: we have calibrated the 0-dB attenuation of a continuous wave to be 0 dBm. However, a low-grade Temperature Controlled Crystal Oscillator (TCXO) exhibits too poor a medium (0.01-1000 s) term stability, when the phase noise offset from carrier is lower than 100 Hz, to provide a credible spoofing signal: phase tracking loops in GPS receivers are tuned to track stable frequency sources as found on spaceborne atomic clocks whose frequency mainly shifts due to the Doppler shift introduced by the relative movement between space vehicles and GPS receivers. Therefore, we investigate how to replace the low-grade TCXO with a high-grade Oven Controlled Crystal Oscillator (OCXO) for both short term and long term stability compatible with atomic clock short term stability characteristics. Indeed, atomic clock microwave feedback loop is only used for long term (> 1000 s [23]) stabilization of the quartz local oscillator which defines the short term stability of atomic clocks: clocking the PlutoSDR with a double-ovenized OCXO will provide a source with sufficient stability to spoof all tested single-frequency GPS receivers.

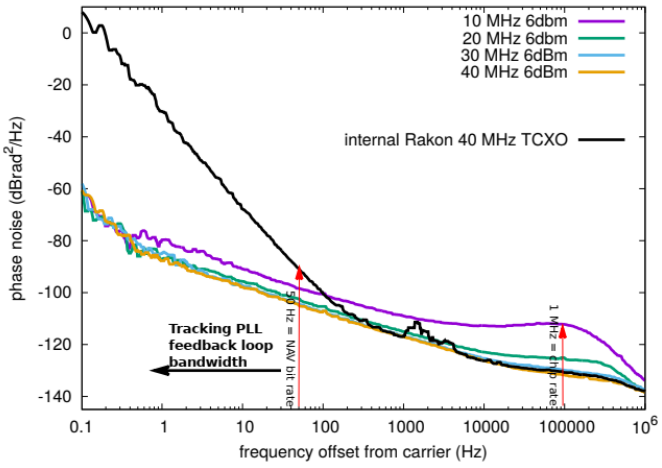

Fig. 1. 100 MHz output phase noise as a function of input clock frequency. All references are generated by a Rohde & Schwarz SMA100A synthesizer. The phase noise is degraded if the local oscillator clocking the AD9363 is below 40 MHz. All phase noises overlap for local oscillators of 40, 50 or 60 MHz and only the 40 MHz curve is shown. The black curve of the original TCXO exhibits excellent far-from-carrier phase noise but large drift close to carrier (low frequency offset), hence the poor spoofing capability since receiver PLL are unable to track such fast phase fluctuations.

As shown in Fig. 1, the original Rakon 40 MHz TCXO fitted in the PlutoSDR circuit exhibits large phase drift below 100 Hz from carrier, within the tracking loop of the GPS receiver decoding the 50 bps navigation messages transmitted by the satellites. Replacing the TCXO with an OCXO improves by more than 60 dB the phase noise fluctuations at 0.1 Hz from carrier, i.e. during measurements durations of 10 seconds. However, the 10 MHz OCXO output will degrade the PlutoSDR 1.57542 GHz output signal far from carrier, at frequency offsets above 100 Hz, and degrade the ability of

the receiver of detecting the BPSK modulated PRN codes. It is observed that increasing the reference clock frequency driving the AD9363 radiofrequency frontend fitted on the PlutoSDR is mandatory to recover the TCXO noise floor at frequency offsets above 100 Hz, as described below. Since the radiofrequency power driving the resonator defines the oscillator noise floor, all measurements are completed with the highest power level admitted by the PlutoSDR clock input, namely 6 dBm.

Most OCXOs output 10 or 100 MHz signals. The 100 MHz version is above the documented characteristics of the input clock signal of the AD9363 radiofrequency front-end, while the 10 MHz version exhibits excessive far-from-carrier phase noise, as shown in Fig. 1. Indeed, based on the PlutoSDR initial 40 MHz oscillator, it appears that an optimum clock frequency should be above 30 MHz. Such a clock frequency is achieved by doubling twice (MiniCircuits MK-2) a 10-MHz Hewlett Packard 10811-60111 OCXO. A low noise ZFL-1000LN+ amplifies the radiofrequency signal at the output of the first doubler to feed the second stage with sufficient power. Refurbished units were selected on purpose since they were already aged and no longer exhibit long-term drift as would be expected from new units. Phase noise spectra given in Fig. 1 demonstrate the need to raise the OCXO output frequency to 40 MHz to keep the excellent far-from-carrier phase noise of the AD9363 phase locked loop (PLL).

Using a local oscillator with stability representative of the short and medium term stability of an atomic clock, as provided by an OCXO, is mandatory for generating realistic spoofing signals. Actually, the TCXO was observed to generate a signal only randomly spoofing mobile phones and always failing with car navigation systems. However, when clocking the PlutoSDR with the OCXO, such GPS receivers have been spoofed to exhibit any location in a radius of a few hundred kilometers around the actual location, as long as the spoofing signal hides the authentic GPS constellation by selecting locations and dates not too far from the real constellation geometry. In this experimental setup, the PlutoSDR output is -30 dBm, leading to an attack range predicted by the Free Space Propagation Loss link budget analysis of less than 100 m around the spoofing emitter as the receiver is also exposed to the authentic genuine signal from the GPS constellation. Similarly, u-blox (Thalwil, Switzerland) NEO/LEA-6T GPS receivers [24] with timing capability thanks to the 1-Pulse Per Second (1-PPS) output have been spoofed to offset their 1-PPS timing signal with hardly any visible impact on the location even though the timing signal was delayed with discrete steps by introducing erroneous AF0 messages [25] for all satellite navigation messages, yielding stable position but varying 1-PPS time, as shown in Fig. 2. In all cases, the commercial receivers were running and had acquired the authentic constellation before being spoofed to the new location or time.

Therefore, it is demonstrated that, by using a single antenna, a properly clocked spoofing emitter will generate the 2 MHz wide GPS signal which cannot be distinguished from the authentic signal: as opposed to jamming in which the user immediately detects a loss of service, the spoofing signal will introduce erroneous position or timing signal, a dramatic impact if this GPS signal for example feeds a Network Time Protocol (NTP) or Precision Time Protocol (PTP) server for time dissemination in a network assumed to be synchronized with the GPS time.

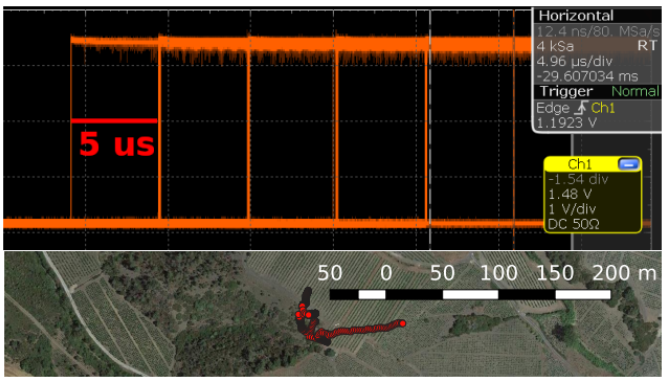

Fig. 2. Top: 1-PPS output from a spoofed u-blox GPS receiver. Bottom: relative position output of the spoofed receiver. Despite the 1-PPS shifting by 25 μs or the time needed for an electromagnetic signal to travel 7.5 km, the actual receiver position hardly varies in a sub-50 m range since the same time offset is introduced in the AF0 parameter of the spoofing message of all satellites. The spoofed location is south of France while the actual experiment location is in the north-eastern location of France in Besançon.

III. GPS SPOOFING DETECTION

In this Section, we propose a computationally efficient spoofing detection method by using a codeless decoding approach to measure the phase difference of different satellites and different antennas. Firstly, assuming there are M authentic satellites and N spoofing satellites, the complex baseband representation (I & Q) of the time-varying signal received by the k-th antennas ($k = 1, 2$, *i.e.*, two antennas are used in our analysis) can be expressed as [18]

$$\begin{aligned} s(k,t) = &\sum_{m=1}^{M} \alpha_m^A(k,t)\beta_m^A(k,t)e^{j\varphi_m^A(k,t)}s_m^A(k,t) \\ &+ \sum_{n=1}^{N} \alpha_n^S(k,t)\beta_n^S(k,t)e^{j\varphi_n^S(k,t)}s_n^S(k,t) + \varepsilon(k,t) \end{aligned} \tag{1}$$

with

$$\begin{cases} s_m^A(k,t) = d_m^A[t-\tau_m^A(k,t)]c_m^A[t-\tau_m^A(k,t)]e^{j2\pi f_m^A(k,t)t} \\ s_n^S(k,t) = d_n^S[t-\tau_n^S(k,t)]c_n^S[t-\tau_n^S(k,t)]e^{j2\pi f_n^S(k,t)t} \end{cases} \tag{2}$$

where the superscripts "A" and "S" denote "authentic" and "spoofing", t denotes time, $\alpha(k,t)$ denotes the complex gain of the k-th antenna, which is dependent on the antenna radiation pattern and the satellite signal direction, $\beta(k,t)$ denotes the real-value amplitude (i.e., the square root of the power) of the satellite signal, $\varphi(k,t)$ denotes the phase of the satellite signal, $\varepsilon(k,t)$ denotes the thermal noise, $d(t)$ and $c(t)$

denote the navigation message and the PRN code with BPSK modulations, $\tau(k,t)$ denotes the time delay of the satellite signal, and $f(k,t)$ denotes the Doppler shift as well as the frequency offset between the local oscillator and the received satellite signal, which is identical for all antennas in the context of a coherent receiver.

Given a short integration time T, during which the amplitude, phase, and Doppler shift of the satellite signals as well as the antenna gains are assumed to be constant (i.e., unchanged with time), and a limited antenna extent, for which the time delay, amplitude, and Doppler frequency of the satellite signal with respect to different antennas are assumed to be equivalent, the received signal can be approximated by

$$\begin{aligned} s(k,t) \simeq & \sum_{m=1}^{M} \alpha_m^A(k)\beta_m^A e^{j\varphi_m^G(k)} e^{j\varphi_m^A} s_m^A(t) \\ & + \alpha_0^S(k) e^{j\varphi_0^G(k)} \sum_{n=1}^{N} \beta_n^S e^{j\varphi_n^S} s_n^S(t) + \varepsilon(k,t) \end{aligned} \tag{3}$$

with

$$\begin{cases} s_m^A(t) \simeq d_m^A[t-\tau_m^A] c_m^A[t-\tau_m^A] e^{j2\pi f_m^A t} \\ s_n^S(t) \simeq d_n^S[t-\tau_n^S] c_n^S[t-\tau_n^S] e^{j2\pi f_n^S t} \end{cases} \tag{4}$$

where $\varphi_m^G(k)$ and $\varphi_0^G(k)$ denote the geometrical phase terms of the m-th authentic satellite signal and spoofing satellite signals from a single emitter with respect to the k-th antenna. We note that, since the complex gain of the k-th antenna with respect to the n-th spoofing satellite $\alpha_n^S(k)$ is only dependent on the antenna radiation pattern and the signal direction, we set $\alpha_1^S(k) = \alpha_2^S(k) = \cdots \alpha_N^S(k) \triangleq \alpha_0^S(k)$ in Eq. (3) under the assumption of a single spoofing source.

By using the first antenna as reference, the geometrical phase terms in Eq. (3) can be expressed as

$$\begin{cases} \varphi_m^G(k) = \varphi_m^G(1) + 2\pi(k-1)d\cos\psi_m/\lambda \\ \qquad\quad = \varphi_m^G(1) + 2\pi(k-1)d\cos\theta_m\cos\phi_m/\lambda \\ \varphi_0^G(k) = \varphi_0^G(1) + 2\pi(k-1)d\cos\psi_0/\lambda \\ \qquad\quad = \varphi_0^G(1) + 2\pi(k-1)d\cos\theta_0\cos\phi_0/\lambda \end{cases} \tag{5}$$

whose value depends on the angle of the satellite to the antenna array baseline, where d denotes the spacing between two antennas, λ denotes the GPS L1 carrier wavelength of 19 cm in this investigation, ψ, θ, and ϕ denote cone angle, azimuth angle, and elevation angle, respectively.

Then, assuming the phases of different satellites corresponding to different antennas can be obtained from the received signal, we get

$$\begin{cases} \varphi_m^A(k) = \angle\alpha_m^A(k) + \varphi_m^G(k) + \varphi_m^A \\ \varphi_n^S(k) = \angle\alpha_0^S(k) + \varphi_0^G(k) + \varphi_n^S \end{cases} \tag{6}$$

where $\angle$ denotes the phase of a complex value.

For a specific satellite, the phase difference between the two antennas is given by

$$\begin{cases} \Delta\varphi_m^A = \angle[\alpha_m^A(2)/\alpha_m^A(1)] + 2\pi d\cos\psi_m/\lambda \\ \Delta\varphi_n^S = \angle[\alpha_0^S(2)/\alpha_0^S(1)] + 2\pi d\cos\psi_0/\lambda \end{cases} \tag{7}$$

In Eq. (7), since $\Delta\varphi_n^S$ is not dependent on n, we can rewrite it as $\Delta\varphi_n^S = \Delta\varphi_0^S$. Besides, it can be learned from Eq. (7) that, computing the phase difference between two antennas cancels the satellite phase (φ_m^A and φ_n^S in Eq. (6)) common to both antennas, and only geometrical phase and intrinsic phase difference between two uncalibrated antennas remain. For an authentic constellation in which all satellites are located at different azimuths and elevations, the phase difference between two antennas would be different for different satellites. On the other hand, in the case of a spoofing constellation, assuming a single spoofing emitter, the phase difference between two antennas will be the same and defined only by the location of the spoofing emitter and the intrinsic phase difference between the two uncalibrated antennas.

The different characteristics between the authentic satellites and the spoofing satellites can be used for spoofing detection. The key point lies in measuring the phase differences corresponding to different satellites from the received signal with navigation message, PRN code, and Doppler shift, as given in Eq. (3). To this end, one solution is to run the full GPS acquisition procedure, as done by the post-correlation spatial processing method [18], which, however, is time-consuming in the context of an SDR implementation running on general purpose processors. With the assumption that the spoofing signals can accumulate higher power than the authentic signals, another solution, i.e., the pre-correlation spatial processing method proposed in [17], uses the approach shown in Eq. (8) to estimate the phase difference between two antennas.

$$\begin{aligned} & \int_0^T s(2,t)s^*(1,t)dt \\ & \simeq e^{j\Delta\varphi_0^S} \int_0^T \sum_{n=1}^{N} |\alpha_0^S(2)\alpha_0^S(1)|(\beta_n^S)^2 dt \\ & + \int_0^T \sum_{m=1}^{M} e^{j\Delta\varphi_m^A} |\alpha_m^A(2)\alpha_m^A(1)|(\beta_m^A)^2 dt \\ & \simeq e^{j\Delta\varphi_0^S} T \sum_{n=1}^{N} |\alpha_0^S(2)\alpha_0^S(1)|(\beta_n^S)^2 \\ & \Downarrow \\ & \Delta\varphi_0^S \simeq \angle \int_0^T s(2,t)s^*(1,t)dt \end{aligned} \tag{8}$$

where T denotes the integration time and $s^*(1,t)$ denotes the complex conjugate of the complex baseband signal $s(1,t)$. The method based on Eq. (8) is effective and can get accurate estimation when the spoofing power is much higher than the authentic power. Otherwise, the second approximation in Eq. (8) cannot hold, resulting in inaccurate estimation of the phase difference. To solve the limitations of the pre-correlation (i.e., potential performance loss) and post-correlation (i.e., high computational cost) spatial processing methods at the same time, a codeless decoding approach is proposed, as detailed in the following.

The BPSK modulation used to transmit the PRN code of each satellite spreads the carrier over the 2 MHz bandwidth

generated by the 1 Mb/s code transmission. The GPS regulation of receiving at least -130 dBm at ground level means that the signal is at least 19 dB below thermal noise: integrated over a 2 MHz bandwidth or 63 dB, the -174 dBm/Hz noise floor rises to -111 dBm, well above the -130 dBm standard. However, the BPSK modulation can be cancelled by squaring the received signal, as classically done for identifying the carrier frequency offset due to Doppler shift and local oscillator frequency difference in the Costas loop [21], since the phase of $[0;\pi]$ becomes $[0;2\pi] = 0 \pmod{2\pi}$ after squaring the signal. This pulse compression gets rid of the 2 MHz bandwidth modulation carrier spreading and brings the compressed signal back above the noise floor since a 1023 bit long code sequence rises the signal level by $10\log_{10}(1024) \simeq 30$ dB and $-130 + 30 = -100 > -111$ dBm. Thus, rather than running the full GPS acquisition sequence of correlating the local copies of the PRN code shifted by a Doppler frequency, we consider a computationally efficient codeless approach in which the received signal is squared and Fourier transformed. Although the actual message will be lost in the process of removing the digital communication modulation, this codeless processing technique will allow us to identify spoofing and the characteristics of the spoofing emitter.

Squaring the received complex baseband signal gets rid of the BPSK modulated navigation message and PRN code resulting in

$$\begin{aligned} s^2(k,t) &= s(k,t)s(k,t) \\ &= \sum_{m=1}^{M} \left(\beta_m^A\right)^2 |\alpha_m^A(k)|^2 e^{j2\varphi_m^A(k)} e^{j4\pi f_m^A t} \\ &+ \sum_{n=1}^{N} \left(\beta_n^S\right)^2 |\alpha_0^S(k)|^2 e^{j2\varphi_n^S(k)} e^{j4\pi f_n^S t} + s^{Inc}(k,t) \end{aligned} \tag{9}$$

where $s^{Inc}(k,t)$, including the square of noise and the multiplications among spoofing signal, authentic signal and noise, denotes the incoherent signal generated in the squaring process, which will not be coherently accumulated in the following Fourier transform, given by

$$S(k,f) = \int_0^T s^2(k,t) e^{-j2\pi f t} dt \tag{10}$$

When $f = 2f_m^A$ or $f = 2f_n^S$, we can obtain a frequency peak as

$$\begin{aligned} S(k,2f_m^A) &= \int_0^T s^2(k,t) e^{-j4\pi f_m^A t} dt \\ &\simeq T(\beta_m^A)^2 |\alpha_m^A(k)|^2 e^{j2\varphi_m^A(k)} \end{aligned} \tag{11}$$

or

$$\begin{aligned} S(k,2f_n^S) &= \int_0^T s^2(k,t) e^{-j4\pi f_n^S t} dt \\ &\simeq T(\beta_n^S)^2 |\alpha_0^S(k)|^2 e^{j2\varphi_n^S(k)} \end{aligned} \tag{12}$$

whose value will be much higher than those of other frequency bins generated by the incoherent signal component as observed by experiments. In Eqs. (11) and (12), the approximation comes from the fact that, when the frequency is twice that of the Doppler shift of a specific satellite (authentic one or spoofing one), its energy will be accumulated coherently thanks to the removal of the BPSK modulation and hence it becomes a single-tone signal as was demonstrated above in Eq. (9), while the relative power of other satellite signals with different Doppler shifts and incoherent signal component will be significantly reduced after integration.

After determining the frequency peaks that rise above the noise floor by thresholding, all the authentic and spoofing satellites can be detected. Then, we can calculate the intermediate phase difference between two antennas for each detected satellite as

$$\Delta\widetilde{\varphi}_m^A = \angle[S(2,2f_m^A)/S(1,2f_m^A)] \tag{13}$$

or

$$\Delta\widetilde{\varphi}_0^S = \angle[S(2,2f_n^S)/S(1,2f_n^S)] \tag{14}$$

Arising from the squaring process that doubles the phase term, the relationship between the intermediate phase difference $\Delta\widetilde{\varphi}$ in Eqs. (13) or (14) and the phase difference $\Delta\varphi$ in Eq. (7) is given by

$$\Delta\varphi = \begin{cases} \Delta\widetilde{\varphi}/2, |2\Delta\varphi| \le \pi \\ \Delta\widetilde{\varphi}/2 - \pi, \text{else} \end{cases} \tag{15}$$

Eq. (15) means that directly using $\Delta\widetilde{\varphi}/2$ to estimate $\Delta\varphi$ is ambiguous because, if $|2\Delta\varphi| > \pi$, then we have $\Delta\widetilde{\varphi}/2 = \angle e^{j2[\varphi(2)-\varphi(1)]}/2 = \angle e^{j2\Delta\varphi}/2 = \Delta\varphi + \pi$. Therefore, in order to well suppress the spoofing signals, ambiguity resolving is needed to get $\Delta\varphi$ based on Eq. (15). However, for the spoofing detection purpose, this step is not necessary since the ambiguity is the same for all spoofing satellites. In other words, we can simply use $\Delta\widetilde{\varphi}/2$ as a preliminary estimation of $\Delta\varphi$ in the spoofing detection step. Based on this, we can get an ascending phase difference vector as shown in Eq. (16) by sorting the phase differences of all the detected satellites.

$$\boldsymbol{\Delta}\varphi = [\Delta\varphi_1, \Delta\varphi_2, ..., \Delta\varphi_L] \tag{16}$$

where L is the number of detected satellites, i.e., the number of the determined frequency peaks.

Then, the successive differences of the phase difference vector $\boldsymbol{\Delta}\varphi$ can be computed to get the following vector

$$\boldsymbol{\Delta\Delta}\varphi = [\Delta\varphi_2 - \Delta\varphi_1, ..., \Delta\varphi_L - \Delta\varphi_{L-1}] \tag{17}$$

Since all the spoofing satellites have the same $\Delta\varphi_0^S$, the spoofing phenomenon can be detected if the minimum of $\boldsymbol{\Delta\Delta}\varphi$ is smaller than a detection threshold, expressed as

$$min[\boldsymbol{\Delta\Delta}\varphi] \le \xi \tag{18}$$

where ξ is the spoofing detection threshold, which can be set as a fixed value in advance or be determined by some adaptive

techniques in practical applications, e.g., the Constant False Alarm Rate (CFAR) detection technique [26].

We note that, for the proposed method, the spoofing detection is conducted discretely with an interval of T. In some cases, false detection alarms may be introduced by the noise, the authentic satellites that come from near the same direction, or the unexpected large phase differences among different spoofing satellites. A backward sliding-average based approach can be used to solve this problem, given by

$$\mathbf{\Delta\Delta}\overline{\varphi}^{o} = \frac{1}{W}\sum_{w=0}^{W-1}\mathbf{\Delta\Delta}\varphi^{o-w} \tag{19}$$

where W is the window size for average, $\mathbf{\Delta\Delta}\overline{\varphi}^{o}$ corresponds to the o-th spoofing detection point with time of $(o-1)T$, and $\mathbf{\Delta\Delta}\varphi^{o-w}$ corresponds to the $(o-w)$-th detection point. After sliding-average along time, the negative influences caused by the noise, authentic satellites from the close directions, and unexpected spoofing satellite phases can be reduced. Therefore, the spoofing detection in Eq. (18) can be conducted based on $\mathbf{\Delta\Delta}\overline{\varphi}$ instead of $\mathbf{\Delta\Delta}\varphi$.

Furthermore, when there is spoofing, since the element value of $\mathbf{\Delta}\varphi$ is continuously ascending, the spoofing satellites can also be distinguished from the authentic satellites by determining an index set including continuous indexes (from l_{first} to l_{last}) of $\mathbf{\Delta\Delta}\varphi$ with the corresponding elements smaller than the detection threshold. To make it clear, with a real-sampled GPS signal with spoofing, $\mathbf{\Delta}\varphi$ and $\mathbf{\Delta\Delta}\varphi$ are shown in Fig. 3. It can be seen from the top sub-figure that, given $l_{\text{first}} = 3$ and $l_{\text{last}} = 6$, $\mathbf{\Delta}\varphi(l_{\text{first}}), ..., \mathbf{\Delta}\varphi(l_{\text{last}}), \mathbf{\Delta}\varphi(l_{\text{last}}+1)$ are quite close to each other, which is a strong sign of spoofing attack occurring. Based on $\mathbf{\Delta\Delta}\varphi$ as shown in the bottom sub-figure, the spoofing phenomenon can be detected according to Eq. (18), while l_{first} and l_{last} can also be determined to distinguish the spoofing satellites.

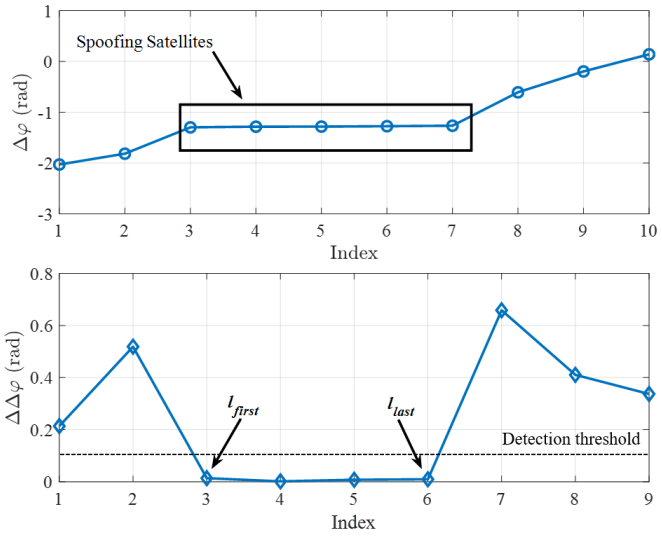

Fig. 3. $\mathbf{\Delta}\varphi$ (top) and $\mathbf{\Delta\Delta}\varphi$ (bottom) calculated from a real-sampled GPS signal with 5 spoofing satellites and 5 authentic satellites. Spoofing phenomenon and the corresponding spoofing satellites can be detected by thresholding $\mathbf{\Delta\Delta}\varphi$.

To summarize, Table I shows the proposed spoofing detection method. The proposed method is computationally efficient because it only requires squaring the raw radiofrequency signal collected by the receiver with two antennas, identifying the frequency offset characteristic of each satellite, computing the phase difference of each identified satellite between different antennas, and calculating the successive difference of the sorted ascending phase difference vector. This method is also applicable to L2, doubling the spoofing detection capability if L1 and L2 observed frequency offsets are inconsistent as would be expected from a spoofing attack on L1 only as most readily feasible with consumer-grade SDR emitters towards consumer-grade receivers.

TABLE I
PROCESSING FLOWCHART OF THE PROPOSED SPOOFING DETECTION METHOD.

Input: Complex baseband signal $s(k,t)$, where k = 1 and 2, and detection threshold ξ.
Procedure: 1) Square the received signal $s(k,t)$ to get $s^2(k,t)$ based on Eq. (9); 2) Perform Fourier transform of the squared signal $s^2(k,t)$ to get $S(k,f)$ based on Eq. (10) and extract the frequency peaks that rise above the noise floor; 3) Calculate and sort the phase differences of each frequency peak between two antennas to get an ascending phase difference vector $\mathbf{\Delta}\varphi$ based on Eq. (16); 4) Take the successive differences of the phase difference vector $\mathbf{\Delta}\varphi$ to get $\mathbf{\Delta\Delta}\varphi$ based on Eq. (17); 5) Compute the averaged successive difference vector $\mathbf{\Delta\Delta}\overline{\varphi}$ with the saved previous measurements based on Eq. (19); 6) If Eq. (18) is satisfied, then the spoofing phenomenon occurs, go to the spoofing suppression step. Otherwise, no spoofing, go to the normal processing steps. Output: $s(k,t)$, the decision to do or not to do spoofing suppression, and the indexes of spoofing satellites indicated by l_{first} and l_{last}.

IV. GPS SPOOFING SUPPRESSION

In this Section, the information obtained from the previous spoofing detection step is introduced into a null-steering processing for spoofing suppression.

A. Basic principle

As seen in Eq. (3), if the amplitude (antenna gain) ratio and phase (geometrical phase and intrinsic phase) difference between two uncalibrated antennas corresponding to the spoofing signal can be obtained, the spoofing signal can be canceled by the following process.

$$\begin{aligned} s(t) &= s(2,t) - \frac{\alpha_0^S(2)}{\alpha_0^S(1)} e^{j[\varphi_0^G(2)-\varphi_0^G(1)]} s(1,t) \\ &= s(2,t) - |\Delta\alpha_0^S| e^{j\Delta\varphi_0^S} s(1,t) \\ &= s(2,t) - w_0^S s(1,t) \end{aligned} \tag{20}$$

where $|\Delta\alpha_0^S|$, $\Delta\varphi_0^S$, and w_0^S are amplitude ratio, phase difference, and weight coefficient, respectively. Such a process allows for subtracting the spoofing signal from the signal measured on the second antenna. Actually, by defining the steering vector of the spoofing signal as $\mathbf{v}_0 = [1, |\Delta\alpha_0^S| e^{j\Delta\varphi_0^S}]^{\mathrm{T}}$ with

$[\cdot]^{\mathrm{T}}$ as the transpose, Eq. (20) is equivalent to the orthogonal projection based beamforming process [17], [27], given by

$$s(t) = \mathbf{h}^H \mathbf{P}_\perp [s(1,t), s(2,t)]^{\mathrm{T}} \tag{21}$$

where $\mathbf{P}_\perp$ is the orthogonal projection matrix, expressed as

$$\mathbf{P}_\perp = \mathbf{I} - \mathbf{v}_0 (\mathbf{v}_0^H \mathbf{v}_0)^{-1} \mathbf{v}_0^H \tag{22}$$

with $\mathbf{I}$ as a 2×2 identity matrix and $[\cdot]^H$ as the conjugate transpose, and

$$\mathbf{h} = [-|\Delta\alpha_0^S| e^{-j\Delta\varphi_0^S}, 1]^T \tag{23}$$

is the vector used to combine the signals from two antennas. By orthogonally projecting the received signal to the spoofing subspace, a null can be formed towards the spoofer direction to remove the spoofing signal, resulting in

$$\begin{aligned} s(t) = \mathbf{h}^H \mathbf{P}_\perp \sum_{m=1}^{M} \alpha_m^A(1) \beta_m^A e^{j\varphi_m^G(1)} e^{j\varphi_m^A} s_m^A(t) \mathbf{v}_m \\ + \mathbf{h}^H \mathbf{P}_\perp [\varepsilon(1,t), \varepsilon(2,t)]^T \end{aligned} \tag{24}$$

with $\mathbf{v}_m = [1, |\alpha_m^A(2)/\alpha_m^A(1)| e^{j\Delta\varphi_m^A}]^{\mathrm{T}}$ as the steering vector of the m-th authentic satellite signal.

In order to estimate the weight coefficient w_0^S to steer the null for spoofing suppression, the key is to estimate the amplitude ratio $|\Delta\alpha_0^S|$ and the phase difference $\Delta\varphi_0^S$ between two antennas. According to the method in [18], Eq. (8) can be used to estimate $\Delta\varphi_0^S$ and the method shown in Eq. (25) can be used to estimate $|\Delta\alpha_0^S|$.

$$\begin{aligned} &\int_0^T s(k,t) s^*(k, t - T_0) dt \\ &\simeq \int_0^T \sum_{m=1}^{M} |\alpha_m^A(k)|^2 (\beta_m^A)^2 e^{j2\pi f_m^A T_0} \\ &\quad + |\alpha_0^S(k)|^2 \sum_{n=1}^{N} (\beta_n^S)^2 e^{j2\pi f_n^S T_0} dt \\ &\simeq |\alpha_0^S(k)|^2 [T \sum_{m=1}^{M} (\beta_m^A)^2 e^{j2\pi f_m^A T_0} \\ &\quad + T \sum_{n=1}^{N} (\beta_n^S)^2 e^{j2\pi f_n^S T_0}] \\ &\quad \Downarrow \\ &|\Delta\alpha_0^s| \simeq \left[\frac{\int_0^T s(2,t) s^*(2, t - T_0) dt}{\int_0^T s(1,t) s^*(1, t - T_0) dt} \right]^{1/2} \end{aligned} \tag{25}$$

where T_0 denotes the period of PRN codes.

However, when the navigation data changes, the first approximation in Eq. (25) cannot hold, and when the assumption $|\alpha_m^A(k)| = |\alpha_0^S(k)|$ is not satisfied, the second approximation in Eq. (25) cannot hold, resulting in a poor estimation of $|\Delta\alpha_0^S|$. Besides, as mentioned above, the estimation method based on Eq. (8) cannot get accurate estimation of $\Delta\varphi_0^S$ when the spoofing power is not much higher than the authentic power. Actually, based on the proposed codeless spoofing detection method, $|\Delta\alpha_0^S|$ can be estimated by

$$|\Delta\alpha_0^S| = \frac{1}{N} \sum\nolimits_{n=1}^{N} \sqrt{|S(2, 2f_n^S)/S(1, 2f_n^S)|} \tag{26}$$

where the average over N detected spoofing satellites is conducted to improve the estimation accuracy.

Then, based on Eq. (12), we can get the intermediate phase difference estimation as

$$\Delta\widetilde{\varphi}_0^S = \frac{1}{N} \sum_{n=1}^{N} \angle [\frac{S(2, 2f_n^S)}{S(1, 2f_n^S)}] \tag{27}$$

The relationship between the intermediate phase difference $\Delta\widetilde{\varphi}_0^S$ in Eq. (27) and the phase difference $\Delta\varphi_0^S$ is given by

$$\Delta\varphi_0^S = \begin{cases} \Delta\widetilde{\varphi}_0^S/2, |2\Delta\varphi_0^S| \leq \pi \\ \Delta\widetilde{\varphi}_0^S/2 - \pi, \text{else} \end{cases} \tag{28}$$

Based on Eq. (28), we can try both possible solutions of $\Delta\varphi_0^S$ for spoofing suppression to get the authentic satellites with a continuous double-check process, while, in a more general manner, we can try to resolve the ambiguity of Eq. (28) to get the actual $\Delta\varphi_0^S$ for effective spoofing suppression, which will be addressed in the next sub-Section.

B. Ambiguity resolving

To solve the ambiguity problem for phase difference estimation, i.e., to get $\Delta\varphi_0^S$ based on $\Delta\widetilde{\varphi}_0^S$, the proposed method is to use a rough estimation of $\Delta\varphi_0^S$ as the reference.

A simple method to get a rough estimation of $\Delta\varphi_0^S$ is based on Eq. (8). Although Eq. (8) may not provide accurate phase difference estimation when the spoofing power is low, its estimated value will not be too far from the exact value. Therefore, we can get the estimation of $\Delta\varphi_0^S$ as

$$\Delta\varphi_0^S = \begin{cases} \Delta\widetilde{\varphi}_0^S/2, |\Delta\widetilde{\varphi}_0^S/2 - \Delta\varphi_0^{ref}| \leq \frac{\pi}{2} \\ \Delta\widetilde{\varphi}_0^S/2 - \pi, |\Delta\widetilde{\varphi}_0^S/2 - \Delta\varphi_0^{ref}| > \frac{\pi}{2} \end{cases} \tag{29}$$

where $\Delta\varphi_0^{ref} = \angle \int_0^T s_2(t) s_1^*(t) dt$, acting as the reference, and the threshold $\pi/2$ is determined by half of the ambiguity value. Depending on the spoofing power, this threshold can either be relaxed to a bigger value or be tightened to a smaller value than $\pi/2$. Eq. (29) indicates that, if $|\Delta\widetilde{\varphi}_0^S/2 - \Delta\varphi_0^{ref}| \leq \frac{\pi}{2}$, there is no ambiguity of the estimation given by $\Delta\widetilde{\varphi}_0^S/2$. Otherwise, ambiguity happens, the estimation given by $\Delta\widetilde{\varphi}_0^S/2$ should be corrected by subtracting π.

An alternative method to get the reference for estimating $\Delta\varphi_0^S$, which can directly be used for strong spoofing and jamming signal suppression, is further proposed.

Actually, to find the spoofing signal component in the signal vector $\mathbf{s}_2 \in C^{I \times 1}$ received by the second antenna, with I as the number of samples in an integration time T, the following Least Squares (LS) method can be used.

$$w_{LS} \leftarrow \min_{w_{LS} \in C} ||\mathbf{s}_2 - \mathbf{w}_{LS} \mathbf{s}_{sp}||_2^2 / 2 \tag{30}$$

whose solution is given by

$$w_{LS} = (\mathbf{s}_{sp})^\dagger \mathbf{s}_2 = (\mathbf{s}_{sp}^H \mathbf{s}_{sp})^{-1} \mathbf{s}_{sp}^H \mathbf{s}_2 \tag{31}$$

where w_{LS} is the weight coefficient of the spoofing component in the received signal, $(\cdot)^\dagger$ denotes pseudo-inversion, and $\mathbf{s}_{sp} \in C^{I \times 1}$ is the spoofing signal vector. Since the spoofing signal vector is unknown in practice, the signal vector $\mathbf{s}_1 \in C^{I \times 1}$

received by the first antenna can be used to make a replacement of $\mathbf{s}_{sp} \in C^{I\times 1}$ to minimize the power of the combination of $\mathbf{s}_1$ and $\mathbf{s}_2$ as:

$$\begin{cases} w_{LS} \leftarrow \min\limits_{w_{LS}\in C} ||\mathbf{s}_2 - w_{LS}\mathbf{s}_1||_2^2/2 \\ w_{LS} = (\mathbf{s}_1)^{\dagger}\mathbf{s}_2 = (\mathbf{s}_1^H\mathbf{s}_1)^{-1}\mathbf{s}_1^H\mathbf{s}_2 \end{cases} \tag{32}$$

Based on Eq. (32), the spoofing signal contribution can be subtracted from the signal measured on the second antenna, expressed as

$$s(t) = s_2(t) - w_{LS}s_1(t) = [\mathbf{I}_{I\times I} - s_1(s_1^H s_1)^{-1}s_1^H]s_2 \tag{33}$$

By comparing Eq. (33) with Eq. (20), it is clear that w_{LS} is an approximation of w_0, which can help us to estimate $\Delta\varphi_0^S$ based on $\Delta\widetilde{\varphi}_0^S$ as

$$\Delta\varphi_0^S = \begin{cases} \Delta\widetilde{\varphi}_0^S/2, |\Delta\widetilde{\varphi}_0^S/2 - \angle w_{LS}| \le \frac{\pi}{2} \\ \Delta\widetilde{\varphi}_0^S/2 - \pi, |\Delta\widetilde{\varphi}_0^S/2 - \angle w_{LS}| > \frac{\pi}{2} \end{cases} \tag{34}$$

where $\angle w_{LS}$ is the phase of the LS weight coefficient, acting as the reference. Eq. (34) indicates that, if $|\Delta\widetilde{\varphi}_0^S/2 - \angle w_{LS}| \le \frac{\pi}{2}$, there is no ambiguity of the estimation given by $\Delta\widetilde{\varphi}_0^S/2$. Otherwise, ambiguity is determined to happen, the estimation given by $\Delta\widetilde{\varphi}_0^S/2$ should be corrected by subtracting π.

Besides, by comparing Eq. (32) with Eq. (8), it can be derived that $\angle w_{LS}$ in Eq. (34) is equivalent to $\Delta\varphi_0^{ref}$ in Eq. (29) due to the fact that $\angle w_{LS} = \angle[(\mathbf{s}_1^H\mathbf{s}_1)^{-1}\mathbf{s}_1^H\mathbf{s}_2] = \angle[\mathbf{s}_1^H\mathbf{s}_2] = \angle\int_0^T s_2(t)s_1^*(t)dt = \Delta\varphi_0^{ref}$. Therefore, Eq. (34) is actually the same as Eq. (29).

The problems of substituting s_{sp} with s_1 in Eq. (32) are: (a) the LS weight coefficient estimation may not be accurate at low spoofing power, as is the case for the method of Eq. (8) described in [17]; (b) the pseudo-inversion calculation is a computationally intensive operation, caused by the matrix inversion process, and challenging for real-time spoofing suppression.

However, no matter whether the spoofing power is high or low, the LS weight coefficient estimation obtained by Eq. (32) can always act as a reference for resolving the ambiguity of phase difference estimation as observed during various experiments. Besides, we have already addressed in the past the issue of iteratively identifying the LS weight coefficient and had identified Stochastic Gradient Descent (SGD) [22] as a means of avoiding the computing burden of matrix inversion, especially aimed at being implemented in Field Programmable Gate Arrays (FPGA) best suited for iterative processing as each new sample is collected and, due to strong memory constraints, poorly suited to matrix storage and processing. The SGD based LS weight coefficient calculation method is briefly presented as follows.

With the considerations that (a) the weight coefficient of spoofing component hardly varies from one sample to another and (b) data from two antennas are continuously streamed from two analog-to-digital (ADC) converters, the SGD method aims at solving the computationally intensive problem of pseudo-inversion calculation by using an iterative optimization scheme which avoids matrix inversions and can proceed incrementally, based on which the weight coefficient is updated at the p-th iteration by

$$w_{LS}^{p+1} = w_{LS}^p + \nu^p(s_1^i)^*(s_2^i - w_{LS}^p s_1^i) \tag{35}$$

where s_1^i and s_2^i are randomly selected from the already-received signal samples from the first and second antennas, and ν^p is the learning rate at the p-th iteration. As observed in experiments, the SGD method can always provide an accurate approximation to the LS weight coefficient directly computed by the pseudo-inversion process.

It should be noted that, to solve the ambiguity problem for phase difference estimation, i.e., to get $\Delta\varphi_0^S$ based on $\Delta\widetilde{\varphi}_0^S$, we have proposed three methods to provide the rough estimation of $\Delta\varphi_0^S$ as the reference, while, different from the method based on Eq. (8), when the spoofing power is high or when there exists a strong jamming signal, the LS method in Eq. (32) and the SGD method in Eq. (35) can both work effectively to directly suppress the spoofing and jamming signals according to Eq. (33), which will be demonstrated in the next Section.

To summarize, Table II shows the proposed spoofing suppression method.

TABLE II
PROCESSING FLOWCHART OF THE PROPOSED SPOOFING SUPPRESSION METHOD.

Input: Complex baseband signal $s(k,t)$ and the indexes of spoofing satellites obtained in the spoofing detection step.
Procedure: 1) Based on Eq. (26), estimate the amplitude of the weight coefficient; 2) Apply the method in Eq. (8), (32), or (35) to get a reference for phase difference estimation; 3) According to Eq. (29) or (34), obtain the phase estimation of the weight coefficient; 4) Suppress the spoofing component in the signal received by the second antenna based on Eq. (20). Output: $s(t)$ that can be directly feed into a conventional GPS receiver.

V. EXPERIMENT RESULTS

In this section, experiment results are shown to demonstrate the effectiveness of the proposed methods in practice, where the set-up is shown in Fig. 4. First the spoofing detection results are shown, then the spoofing suppression results, and at last the jamming rejection results. All data acquisitions are performed using Ettus Research B210 SDR platforms fitted with the Analog Devices Inc. AD9361 frontend with two low-cost COTS GPS antennas powered by MiniCircuits ZFBT-4R2GW+ bias tee. This dual-channel radiofrequency frontend uses the same oscillator to mix the input signals and transpose to baseband the resulting complex (I & Q) output stream coherently. The unmodulated carrier power emitted by the PlutoSDR AD9363 frontend was measured as 0 dBm, and this output is attenuated by various factors provided as parameters to the SDR, so that the integrated output power is the attenuation factor in dBm despite the spectrum spreading introduced by BPSK modulation. The two receiving patch antennas are located on a ground plane and separated by 10 cm with a clear view of the sky (Fig. 4). The emitting

antenna is a dipole antenna directly connected to the PlutoSDR output SMA connector. Despite being illegal in France, over the air spoofing signals were emitted with low enough power as not to affect users beyond the university campus building. At 80 m from the transmitter, the over the air spoofing signals were measured to be weaker than the genuine signals, in agreement with standard Free Space Propagation Loss. Hence, the spoofing signal should not affect the area beyond the university campus building where the experiments were conducted. The spoofing signal was emitted from a distance of 2.5 meters from the receiver array (fixed parameter adding another -45 dB to the provided emitted power when assessing the received spoofing power), and the jamming signal from a distance of 10 to 1 m from the receiver (varying parameter).

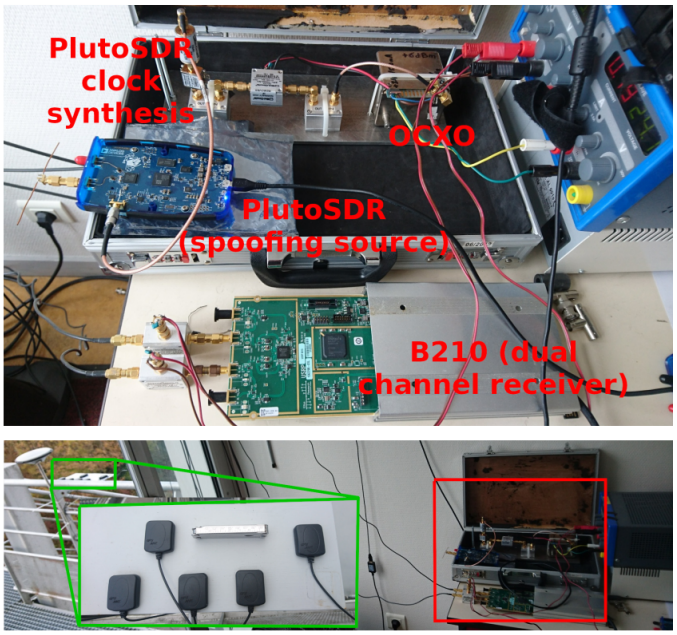

Fig. 4. Compact experimental set-up with a dual antenna measurement system for GPS spoofing/jamming suppression demonstration. Top sub-figure is zoomed from the red square highlighted area on the bottom picture, where the green inset exhibits the antenna array, with only the two bottom antennas separated by 10 cm connected to the Ettus Research B210 SDR receiver.

A. *Spoofing detection*

Two different experiments were conducted to show the performance of the proposed spoofing detection method. During the first experiment, the following experiment sequence is repeated with the spoofing signal power X ranging from -60 dBm to -35 dBm with a 5 dB step using a static spoofer: (a) Authentic constellation with the antennas facing to the sky; (b) Spoofing with International GNSS Service (IGS) orbital data derived constellation collected a couple of months prior to the experiment (inconsistent constellation geometry) with a signal power X for a duration of 10 s; (c) Authentic constellation with the antennas facing to the sky; (d) Spoofing with IGS-derived constellation collected an hour prior to the experiment (consistent constellation geometry) with a signal power X for a duration of 10 s. For each data sequence, the duration is about 30 s, resulting in a total data sampling duration of about 180 s, with (a) and (c) identical baseline conditions of measuring the authentic constellation signal.

Fig. 5 shows the phase difference-Doppler map of the authentic constellation (top) and the spoofing constellation (bottom). The integration time T is 100 ms and the noise floor is set to be 5 times the amplitude average of all frequency bins after Fourier transform. It can be observed that different satellites can be effectively detected as frequency peaks that rise above the noise floor. For both authentic and spoofing constellations, the Doppler shift (half of the detected frequency) is unique for each satellite. For different authentic satellites, their phase differences are dependent on their azimuth and elevation angles and hence are different. In case of the spoofing emitter located at a single point, all phase differences are the same, a signature characteristic for spoofing detection.

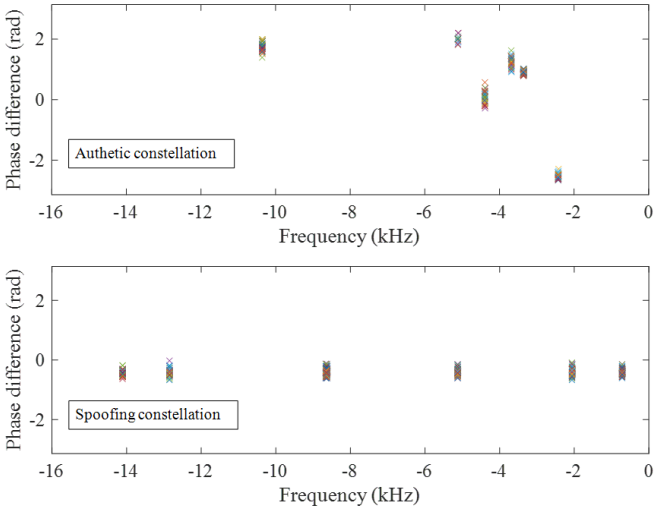

Fig. 5. Experimental phase difference-Doppler map of the authentic constellation (top) and the spoofing constellation (bottom), with the x-axis as the estimated frequency (twice the Doppler shift) and the y-axis as the phase difference measurement between two antennas. Only frequency peaks that rise above the noise floor are detected and extracted, corresponding to different satellites.

As described above, the power emitted from the static spoofing SDR ranged from -60 dBm to -35 dBm with a 5 dB step, alternating from spoofing to genuine constellation every 10 s. Fig. 6 shows the minimum value of the successive difference vector $\mathbf{\Delta\Delta}\varphi$ (top) computed by Eq. (17) and the minimum value of the averaged successive difference vector $\Delta\Delta\overline{\varphi}$ (bottom) computed by Eq. (19) with an interval of $T = 100$ ms. In order to calculate $\Delta\Delta\overline{\varphi}$, the window size W is set to 50, *i.e.*, the averaging time is 5 s. It can be seen from both sub-figures that, when spoofing occurs, the minimum phase difference is much lower than the case without spoofing. Therefore, the spoofing can be effectively detected given an experiential detection threshold of 0.04 rad, as denoted by the red lines in Fig. 6.

Then, a second experiment was conducted, where the spoofer emitting -40 dBm is moving on the campus along a straight path and emitting at constant power for a duration of 9 minutes and then is stopped to leave the receiver to sample the authentic satellite signals during 3 minutes. The

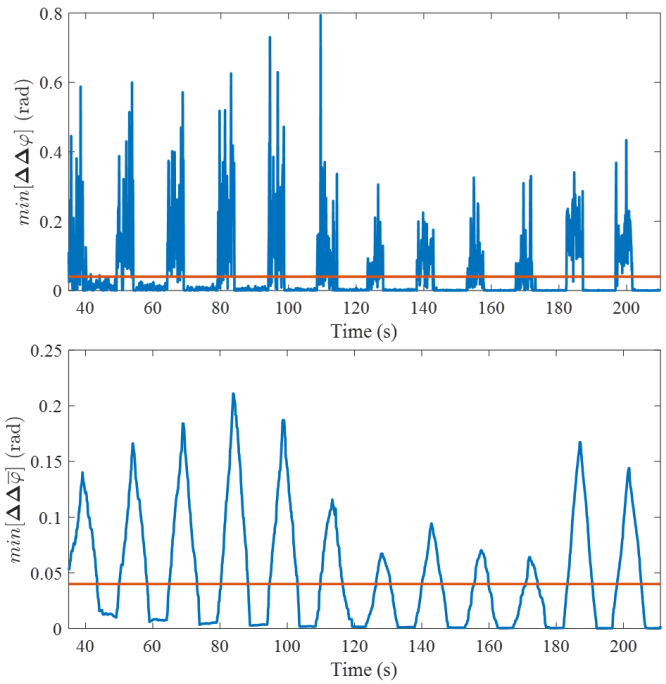

Fig. 6. Minimum phase difference between two antennas of the detected frequency peaks without (top) and with (bottom) backward sliding average process. Authentic and spoofing signals are alternately sampled with a duration of about 180 s. The red horizontal lines denote the spoofing detection threshold, different for top and bottom sub-figures, below which the spoofing is determined. On the contrary, above which there is no spoofing.

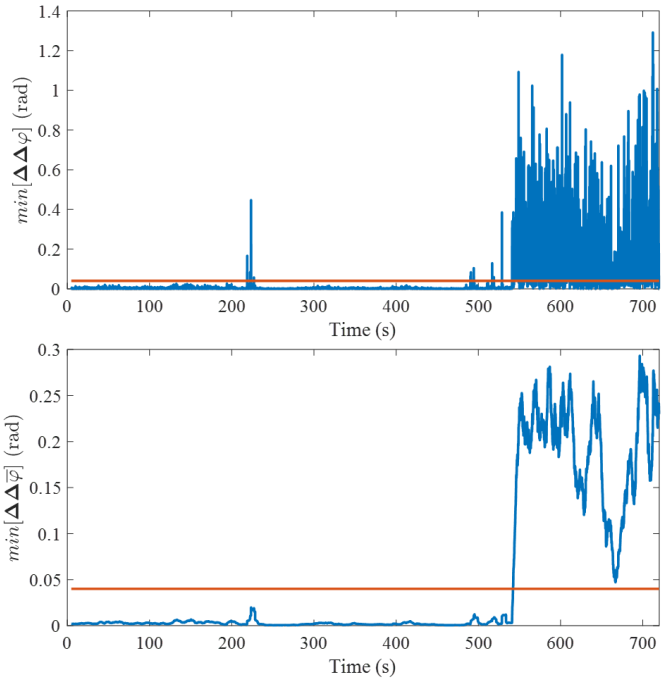

Fig. 7. Detection results with (top) and without (bottom) backward sliding average process for moving spoofer case. Spoofing is controlled to be started from the beginning and to be stopped at about 9 minutes. The authentic satellite signals are sampled from 9 to 12 minutes. The false alarms caused by the noise and the unexpected large phase differences among spoofing satellites can be avoided when sliding average process is applied.

spoofer transmitted at distances between 10 m to 25 m from the receiving array, resulting in a mix of open sky and spoofed signal. Similarly to the results shown in the static spoofer case, Fig. 7 shows the minimum value (top) and the averaged minimum value (bottom) of the successive difference vector with $T = 100$ ms and $W = 50$. It can be seen that the phase difference is continuously small in the beginning (from 0 to 540 seconds or 9 minutes) and then becomes big (from 540 to 720 seconds or 9 to 12 minutes). Therefore, the spoofing phenomenon can also be effectively detected when there is relative movement between the spoofer and the receiver with an experiential detection threshold of 0.04 rad. After performing backward sliding average process, the false alarms as observed from the top sub-figure (at about 220 s and 520 s) can be avoided, as shown in the bottom sub-figure. Since backward sliding approach is used, the causal average process is conducted only based on current and previous phase difference measurements, without next measurements, giving real-time spoofing detection capacity.

As mentioned in Section III, the spoofing detection threshold can be set at a fixed value in advance empirically as used for plotting Figs. 6 and 7, or adaptively determined by some techniques. For example, for each detection point, refered to as cells, based on reference cells, a CFAR technique can help to detect the spoofing phenomenon with a constant false alarm rate by dynamically setting a threshold on the parameter representative of spoofing, in our case $\Delta\Delta\varphi$. Therefore, by using the Smallest of CFAR (SO-CFAR) [28] with a false-alarm rate of 10^{-6}, a guard cell number of 50, and a reference cell number of 50, the detection result for moving spoofing case is shown in Fig. 8. In order to demonstrate the dynamic threshold selection, the dataset used to generate Fig. 7 has been time-reversed. According to the principle of CFAR, spoofing can be detected when the minimum of $\mathbf{\Delta\Delta}\overline{\varphi}$ (as denoted by the blue curve) is bigger than the CFAR threshold (as denoted by the purple curve). It can be seen that spoofing can be effectively detected in the time of 185 s, as indicated by the vertical black line. The spoofing detection threshold ξ in Eq. (18) can thus be adaptively determined by the corresponding value of the minimum of $\mathbf{\Delta\Delta}\overline{\varphi}$ when spoofing occurs, as denoted by the red dot and the red line: here the dynamic selection of the threshold of 0.06 rad matches the fixed empiric value selected 0.04 rad previously. Implementing CFAR involves a computational load comparable to a sliding average and is hence compatible with an implementation for real time processing on a general purpose processing unit.

B. *Spoofing suppression*

The spoofing suppression performance of the proposed method is validated in this sub-Section. Firstly, with spoofing power of -40 dBm and -60 dBm, the weight coefficients used to cancel the spoofing signal in the second antenna are calculated by the proposed method, the LS based method, and the classical method in [17].

Fig. 9 shows the weight estimation results with a spoofing power of -40 dBm for a duration of 10 s. It can be observed that, in such a case, the proposed method can get a close estimation accuracy to the classical method, both in amplitude

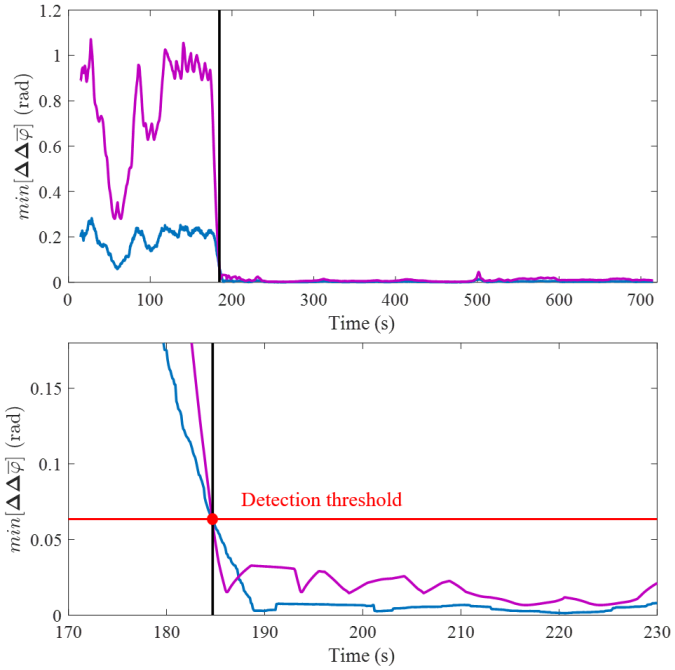

Fig. 8. Moving spoofing detection result obtained by the Smallest of CFAR (SO-CFAR) technique. The bottom sub-figure is zoomed from the top sub-figure. Different from the previous results, the sampled dataset is reversed to show how spoofing can be detected when it suddenly happens, indicated by the vertical black line.

and phase. Besides, the phase estimation obtained by the LS based method is equivalent to the result obtained by the classical method, as we can expect from Eqs. (8) and (32). As indicated by the top sub-figure, the estimated amplitude of the LS based method is slightly different from the classical method and the proposed method, which, however, will not affect the proposed method, as no amplitude reference is needed. Besides, the LS based method method is introduced here not only because it can be a phase reference, also because it will be considered for jamming cancellation, in which the continuous wave structure of the squared signal is no longer available.

As the pseudo-inversion calculation in the LS based method is time-consuming, we have proposed the SGD method to reduce the computational burden of matrix inversion to solve this problem. In figure 10, the weight coefficient calculated by the SGD method is shown with different iterations, where the learning rate is set to be 0.2. It can be seen that the SGD method converges to the pseudo-inverse solution in less than 10^4 iterations for a cold start with a weight coefficient arbitrarily set to 1. Considering the sampling rate of 1 MS/s, such convergence requires about 10 ms. Besides, in real applications, starting with the initial weight obtained by the previous measurement can significantly improve convergence rate as the difference between two antennas will changes continuously.

In Fig. 11, the weight coefficients obtained by different methods in the case of a spoofing power of -60 dBm are shown. In such a case, only the proposed method can get accurate weight coefficient estimation, which is the advantage of the proposed method over the classical method. The amplitude

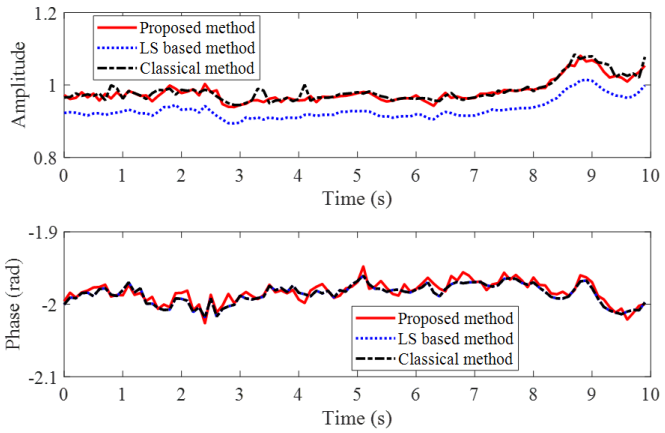

Fig. 9. Amplitude (top) and phase (bottom) of the weight coefficients calculated by different methods with the spoofing power of -40 dBm. All methods yield similar results in amplitude ratio (about 1) and phase difference (about -2 rad) between two antennas.

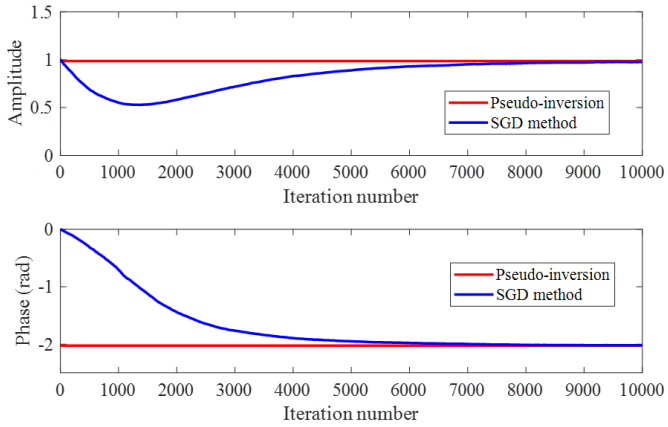

Fig. 10. The amplitude (top) and phase (bottom) convergence of Stochastic Gradient Descent method. The red lines denote the weight obtained by the pseudo-inversion process, acting as the expected value.

(about 1) and phase (about -2 rad) obtained by the proposed method are consistent with the results in the higher spoofing power case (*i.e.*, -40 dBm). On the other hand, the LS based method gives a poor estimate of amplitude and phase, and the classical method does not give phase but gives a reasonable amplitude estimate.

To further demonstrate the superiority of the proposed spoofing suppression method, Fig. 12 shows the beam patterns for different satellite signals. The responses of different satellite signals are calculated by changing the steering vector $\mathbf{v}_m = [1, |\alpha_m^A(2)/\alpha_m^A(1)|e^{j\Delta\varphi_m^A}]^{\mathrm{T}}$: the amplitude term $|\alpha_m^A(2)/\alpha_m^A(1)|$ is assumed to be the same as that obtained by each method and the phase term $e^{j\Delta\varphi_m^A}$ is changing from $-\pi$ to π. It can be seen that, when the spoofing power is -40 dBm, the three methods can all get a deep null at the spoofing direction, i.e., when the phase is about -116 degrees. However, when the spoofing power is changed to -60 dBm, only the proposed method can get a deep null close the spoofing direction (about -107 degrees). Since the classical and LS based methods do not accurately estimate the phase,

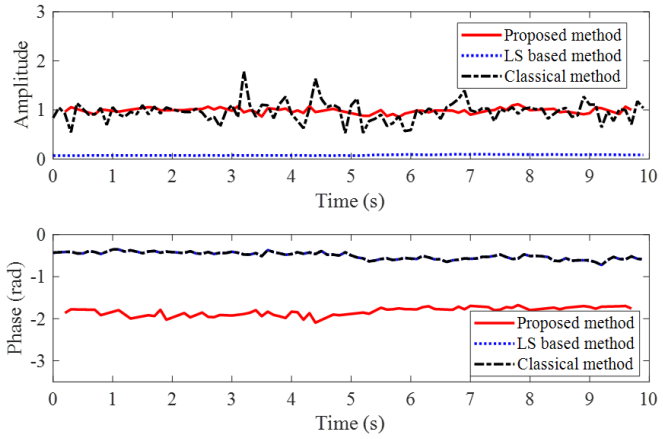

Fig. 11. Amplitude (top) and phase (bottom) of the weight coefficients calculated by different methods with a spoofing power of −60 dBm. Only the proposed method can get the consistent amplitude ratio (about 1) and phase difference (about −2 rad) between two antennas with the case of a −40 dBm spoofing power.

they form a null at about −24 degrees. Therefore, the spoofing signals cannot be effectively suppressed, and the authentic signals cannot be recovered. Besides, as shown by the purple curves, if phase ambiguity occurs and no ambiguity resolving process were conducted in the proposed method, no deep null at the desired direction can be generated, which validates the necessity for ambiguity resolving.

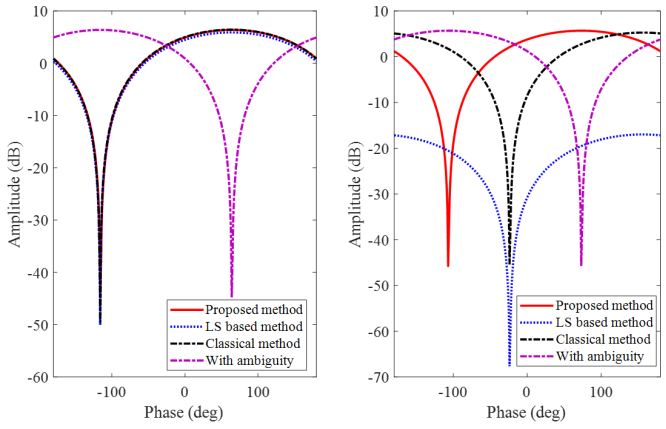

Fig. 12. Beam patterns generated by different methods with the spoofing power of−40 dBm (left) and −60 dBm (right), where the results are shown in dB scale.

Fig. 13 shows the time-frequency and PRN-frequency results after spoofing suppression by the proposed method. On the top right sub-figure, the spoofing contributions of the received signal, shown as varying Doppler frequencies on the top left sub-figure, have been cleaned and only the authentic constellation is visible, as also verified on the frequency-PRN maps in the bottom sub-figures. It can be seen that, when the spoofing signal has not been suppressed, the satellites (PRNs 2, 6, and 9) exhibit different Doppler frequencies from the actual values, resulting in misleading information, Besides, only after spoofing suppression, some authentic satellites (PRNs 26 and 29) can be detected.

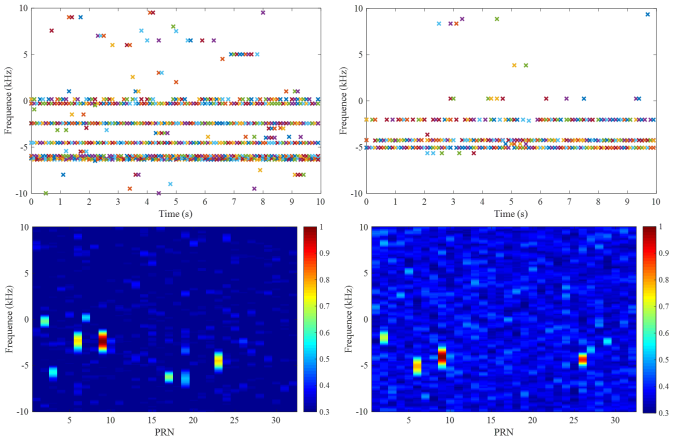

Fig. 13. Time-frequency results (top) and PRN-frequency results (bottom) before (left) and after (right) spoofing suppression by the proposed method.

While suppression of the spoofing signal has been demonstrated on the PRN-frequency maps, recovering a useful authentic signal requires being able to decode the actual position from the cleaned signal. This demonstration is achieved by running the SDR implementation of GNSS decoders based on the GNU Radio framework `gnss-sdr` [29]. We emphasize the computational efficiency of the proposed algorithm: real time spoofing detection and cancellation has been implemented in the single board computer Raspberry Pi4 as a front-end processing of the Signal Source of `gnss-sdr`, and while the results presented here are obtained by post-processing, similar data have been collected following real time processing using the modified source code available at https://github.com/oscimp/gnss-sdr. Compiling `gnss-sdr` to Linux-based embedded platforms using the Buildroot framework is described at https://github.com/oscimp/PlutoSDR/tree/for_next.

Since variable initialization in `gnss-sdr` is random, the capacity to recover the authentic constellation information is a statistical result: in all following experiments, a given dataset is decoded 100 times with the same configuration script tuning gnss-sdr parameters, so that successful identification of the authentic signal is a statistical information given in percentage. Decoding the navigation messages needed for positioning requires longer records than the 10 s authentic or spoofing signals shown previously: all signals collected for demonstrating spoofing suppression by recovering the authentic position in the following analysis are 3-minute long records.

A successful decoding results in the following messages:

```
New GPS NAV message received in channel 15: subframe 5 from satellite GPS PRN 04
New GPS NAV message received in channel 13: subframe 5 from satellite GPS PRN 02
New GPS NAV message received in channel 3: subframe 5 from satellite GPS PRN 23
New GPS NAV message received in channel 6: subframe 5 from satellite GPS PRN 26
Position at 2019-Nov-30 10:59:42.000000 UTC using 4 observations is
Lat = 47.251759020 [deg], Long = 5.993861290 [deg], Height = 687.019 [m]
Velocity: East: -0.092 [m/s], North: -0.091 [m/s], Up = -0.207 [m/s]
```

in which positioning sub-frame navigation messages have been successfully tracked and the true receiver position decoded. Failing to cancel the spoofing signal results in an erroneous latitude/longitude field, while failure to decode any information is identified with the lack of Lat/Long fields after processing the 3-minute long records.

TABLE III
SPOOFING CANCELLATION CAPABILITY AS A FUNCTION OF SPOOFING SIGNAL POWER. EACH ENTRY IS DISPLAYED AS PERCENTAGE OF SOLUTION "BEFORE CORRECTION"/"AFTER CANCELLATION USING THE LS METHOD"/"AFTER CANCELLATION USING THE PROPOSED METHOD"/"AFTER CANCELLATION USING THE METHOD DESCRIBED IN [17]".

Power (dBm)	Constellation	Correct pos. (%)	Wrong pos. (%)	No solution (%)
none	current	100/100/100/96	not relevant	0/0/0/4
−35	current	0/90/100/99	57/0/0/0	43/10/0/1
−40	current	0/93/100/99	96/0/0/0	4/7/0/1
−45	current	0/2/100/100	61/1/0/0	39/97/0/0
−50	current	0/3/100/99	31/7/0/0	69/90/0/1
−55	current	52/23/100/0	0/0/0/0	48/77/0/100
−60	current	88/64/100/13	0/0/0/0	12/36/0/87
−40	-6 h	7/100/100/100	44/0/0/0	49/0/0/0
−50	-6 h	6/4/100/32	90/96/0/0	4/0/0/68

Table III summarizes the result of running `gnss-sdr` on various datasets in which a pair of antennas is exposed to a clear-sky view of the genuine constellation and spoofed over the air by a signal transmitted by the PlutoSDR with a power indicated in the first column, with "none" referring to the absence of spoofing (reference measurement). In each processing case we indicate how many times the correct position is decoded, the erroneous spoofed position, or no solution is found after processing the 3 minute long record. The four fields in each column refer to the raw collected data (one of the two antenna dataset processed by `gnss-sdr`), cleaning the dataset to cancel spoofing using the LS method described in Eq. (33), cleaning the dataset to cancel spoofing using proposed method as described in Eq. (20), or cleaning the dataset to cancel spoofing using the reference published method described in [17] and summarized in Eq. (8) and Eq. (25).

By analyzing the results exhibited in Tab. III, we can conclude that: (a) suppressing the spoofing signal by the proposed method always leads to signal recovery in this set of experiments, both strong and weak spoofing signals can be effectively suppressed; (b) at strong spoofing power (-35 and -40 dBm), the LS based method allows for identifying the spoofing signal weight and hence the spoofing signal can be suppressed, corresponding to the results demonstrated in Figs. 9 and 12 ; (c) at weaker signal (-45, -50, and -55 dBm), authentic and spoofing signals compete so that erroneous positions are detected prior to spoofing suppression. Although the LS based method can still act as the reference for the proposed method, it is unable to properly recover the authentic signal and failure to locate the receiver is the most common result; (d) at low power (-60 dBm), spoofing cannot work well, the correct position can be reached without spoofing suppression in some cases, while, by using the proposed method, the actual position can be reached with a 100% percentage; (e) selecting the current constellation geometry or a significantly different constellation geometry (i.e., a geometry 6 h prior to the current measurement time) does not significantly alter the spoofing suppression capability although it does hinder the ability to spoof the receiver to the erroneous position; (f) finally, the comparison with the reference method described in [17] confirms the statement that the proposed method behaves better at low spoofing power (-50, -55 and -60 dBm), with this conclusion emphasized when the spoofing constellation is not the current constellation and both authentic and spoofing satellites contribute to the phase estimation of Eq. 8.

Intuitively, the better performance of the proposed method is associated with the selection of the spoofing signal to calculate the weight coefficient for null-steering while the classical method and the LS based method uses all available signals, both authentic and spoofing. While all methods can identify accurately the weight coefficient at strong spoofing power well above the authentic signal, the classical method and the LS based method will be disadvantaged when the spoofing power becomes closer to the authentic signal power, both contribute to form the steering null.

C. Jamming rejection

As mentioned previously, the LS based method can be used for both strong spoofing and jamming rejection. Having demonstrated spoofing signal suppression, we investigated jamming rejection in this sub-Section.

Jamming is becoming a common plague from users wishing not to be tracked by GNSS receiver transmitting their coordinate, e.g. to their employer. Low cost "GPS blockers" are found for a few euros: such a jammer was acquired and was reverse engineered to identify the jamming signal as a 300 kHz saw tooth voltage driving a microwave Voltage Controlled Oscillator (VCO) sweeping the 1575 ± 25 MHz range, well within the operating range of GPS. The output power was measured at $+10$ dBm: such a power is so strong that the receiver active antenna low-noise amplifier (LNA) is saturated at ranges of tens of meters unless the emitter antenna is removed. Throughout the following experiments, the commercial jammer antenna was disconnected and the radiofrequency signal radiated by the SMA connector soldered to the VCO output was sufficient to jam the receiver at ranges of several meters. Despite such emission being illegal in France, the jamming signal was assessed to be weak enough to not disturb reception beyond the 80-m radius of the university building. In all experiments representative of practical conditions, the receiving antennas were outdoor exposed to the authentic constellation signal, while the jammer was located indoor next to the receiving antennas at a range from 4.5 m (below which the receiver LNA was saturated) to 9 m (above which the jamming was no longer effective as the radiating antenna had been removed).

The spectra of the received jamming signal are shown in Fig. 14, with the comparison to the spoofing signal. As opposed to the broadband spoofing signal resulting from spectrum spreading by the modulation, the jamming signal exhibits some structures due to the periodic sweep of the VCO, as expected from the simplicity of the low-cost board.

Results from jamming signal rejection are summarized in Tab. IV, from which we can get the following conclusions: (a) strong signal at short range (from 4.5 to 6.0 m) might saturate the radiofrequency frontend, making jamming suppression by the LS based method unsuccessful; (b) at intermediate range

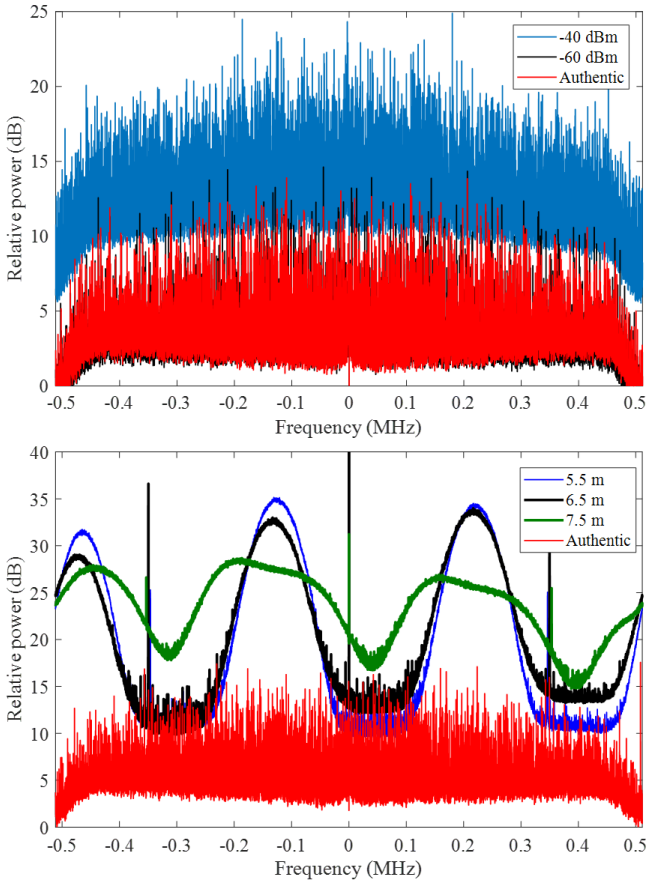

Fig. 14. Spectra of spoofing signal as a function of emitted power (top) and spectra of jamming signal as a function of the jammer to receiver range (bottom).

TABLE IV
JAMMING CANCELLATION CAPABILITY AS A FUNCTION OF JAMMING SIGNAL POWER. EACH ENTRY IS DISPLAYED AS PERCENTAGE OF SOLUTION "BEFORE CORRECTION"/"AFTER CANCELLATION".

Distance	Correct pos.(%)	No sol.(%)
no jamming	100	0
10m00	100/100	0/0
9m00	100/100	0/0
8m00	100/100	0/0
7m50	0/94	100/6
6m50	0/49	100/51
6m00	0/79	100/21
5m50	0/0	100/100
5m00	0/0	100/100
4m50	0/0	100/100

(from 6.0 to 7.5 m), while jamming is effective on the raw receiver, jamming signal rejection by the LS based method is effective and allows for recovering the actual solution with a ratio rising with the range; (c) at long range (from 8.0 to 10 m), jamming is ineffective and jamming rejection is not needed to recover the authentic constellation.

VI. CONCLUSION

This paper demonstrates the ability to spoof GPS signals using widely available hardware by only taking care of feeding the radiofrequency frontend with a stable enough local oscillator to generate a low phase noise signal, the ability to detect spoofing through the phase difference measurement between the signals collected by two antennas, and the ability to tune the antenna array null towards the spoofing emitter in order to destructively interfere the spoofing signal and cancel its contribution in order to recover the authentic constellation signal. All demonstrations have focused on computational efficiency by working on the raw radiofrequency samples rather than tuning SDR GNSS receiver acquisition and tracking procedure: spoofing detection is achieved by applying a computationnally efficient codeless decoding technique and phase difference estimation, while spoofing suppression involves a orthogonal projection method. Since we consider a single spoofing emitter, an array with only two antennas is sufficient to detect and suppress spoofing signals. If more spoofing emitters are located at different positions, an array with more antennas is needed according to the classical beamforming theory. The efficiency of the algorithms is demonstrated by running real time spoofing detection and cancellation on the single board computer Raspberry Pi4 with the modified `gnss-sdr` signal source processing available at https://github.com/oscimp/gnss-sdr.

REFERENCES

[1] JF Zumberge and G Gendt, "The demise of selective availability and implications for the international GPS service," *Physics and Chemistry of the Earth, Part A: Solid Earth and Geodesy*, vol. 26, no. 6-8, pp. 637–644, 2001.

[2] Rigas Themistoklis Ioannides, Thomas Pany, and Glen Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1174–1194, 2016.

[3] Mark L Psiaki and Todd E Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[4] Ling Huang and Qing Yang, "Low-cost GPS simulator GPS spoofing by SDR," in *Proc. DEFCON*, 2015.

[5] Kexiong Curtis Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, and Yaling Yang, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems," in *27th USENIX Security Symposium*, 2018, pp. 1527–1544.

[6] Erick Schmidt, Zachary Ruble, David Akopian, and Daniel J Pack, "Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 8, pp. 2768–2784, 2018.

[7] Chris Bonebrake and Lori Ross O'Neil, "Attacks on GPS time reliability," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 82–84, 2014.

[8] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[9] Ali Jafarnia Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181–191, 2012.

[10] V Dehghanian, J Nielsen, and G Lachapelle, "GNSS spoofing detection based on signal power measurements: statistical analysis," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[11] Mark L Psiaki, Brady W O'hanlon, Steven P Powell, Jahshan A Bhatti, Kyle D Wesson, and Todd E Humphreys, "GNSS spoofing detection using two-antenna differential carrier phase," in *Radionavigation Laboratory Conference Proceedings*, 2014.

[12] Todd E Humphreys, Brent M Ledvina, Mark L Psiaki, Brady W O'Hanlon, and Paul M Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Radionavigation laboratory conference proceedings*, 2008.

[13] M Pini, M Fantino, A Cavaleri, S Ugazio, and L Lo Presti, "Signal quality monitoring applied to spoofing detection," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 2001, pp. 1888–1896.
[14] Jung-Hoon Lee, Keum-Cheol Kwon, Dae-Sung An, and Duk-Sun Shim, "GPS spoofing detection using accelerometers and performance analysis with probability of detection," *International Journal of Control, Automation and Systems*, vol. 13, no. 4, pp. 951–959, 2015.
[15] Sherman Lo, David De Lorenzo, Per Enge, Dennis Akos, and Paul Bradley, "Signal authentication: A secure civil GNSS for today," *inside GNSS*, vol. 4, no. 5, pp. 30–39, 2009.
[16] Carles Fernández-Prades, Javier Arribas, and Pau Closas, "Robust GNSS receivers by array signal processing: Theory and implementation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1207–1220, 2016.
[17] Saeed Daneshmand, Ali Jafarnia-Jahromi, Ali Broumandan, and Gérard Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," in *Proc. 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, 2012, pp. 1233–1243.
[18] Charles E McDowell, "GPS spoofer and repeater mitigation system using digital spatial nulling," July 31 2007, US Patent 7,250,903.
[19] Manuel Cuntz, Andriy Konovaltsev, and Michael Meurer, "Concepts, development, and validation of multiantenna GNSS receivers for resilient navigation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1288–1301, 2016.
[20] Ali Broumandan, Ali Jafarnia-Jahromi, Saeed Daneshmand, and Gérard Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1246–1257, 2016.
[21] Clarence W Fowler, "Codeless GPS sonde," jun 28 1988, US Patent 4,754,283.
[22] Jean-Michel Friedt, Weike Feng, Stéphane Chrétien, Gwenhael Goavec-Merou, and Motoyuki Sato, "Passive radar for measuring passive sensors: direct signal interference suppression on FPGA using orthogonal matching pursuit and stochastic gradient descent," in *Multimodal Sensing: Technologies and Applications*. International Society for Optics and Photonics, 2019, vol. 11059, p. 1105906.
[23] David H Auston, *State of the Art of PTTI Physics and Devices*, National Research Council of the National Academies, 2002.
[24] Andreas Thiel and Michael Ammann, "Anti-jamming techniques in u-blox GPS receivers," Tech. Rep., u-blox, 2009.
[25] J Sanz Subirana, JM Juan Zornoza, and M Hernández-Pajares, "GNSS data processing, volume i: Fundamentals and algorithms," *ESA Communications, ESTEC, Noordwijk, Netherlands*, pp. 145–161, 2013.
[26] Bassem R Mahafza and Atef Elsherbeni, *MATLAB simulations for radar systems design*, CRC press, 2003.
[27] Richard T Behrens and Louis L Scharf, "Signal processing applications of oblique projection operators," *IEEE Transactions on Signal Processing*, vol. 42, no. 6, pp. 1413–1424, 1994.
[28] Gerard V Trunk, "Range resolution of targets using automatic detectors," *IEEE Transactions on Aerospace and Electronic Systems*, , no. 5, pp. 750–755, 1978.
[29] https://gnss-sdr.org/, "GNSS-SDR," *Access online*, 2020.