Frequency-domain code replica detection for a GNSS receiver

Juan M. Parro-Jiménez[1,2], José A. López-Salcedo[1], Rigas T. Ioannides[2] and Massimo Crisci[2]

[1]Universitat Autònoma de Barcelona (UAB), Spain
[2]European Space Agency, Noordwijk, The Netherlands
Email: {Juan.Parro; Rigas.Ioannides; Massimo.Crisci}@esa.int; Jose.Salcedo@uab.cat

***Abstract*—This paper addresses the problem of detecting the presence of spreading signal replica in GNSS receivers, a problem that is often related to the presence of non-authentic GNSS signals. In order to carry out the detection process, a super-resolution frequency-domain technique is proposed based on the well-known Pisarenko harmonic decomposition, which allows us to circumvent many of the problems encountered by non-parametric spectral methods in the presence of short data records. The proposed technique allows to detect the presence of signal replicas while at the same time, it provides an estimate of its frequencies which can be used for frequency tracking purposes in integrity monitoring applications. The performance of the proposed technique has been tested with real GNSS signals from a hardware simulator, confirming the capability of this technique to detect real-life code replicas, even when they are just a few Hz apart.**

I. Introduction

During the last decade, the interest in using GNSS (Global Navigation Satellite Systems) for navigation and timing purposes has experienced an unprecedented raise. This situation has been, in part, motivated by the need of location during an emergency situation. Local mandates, such as FCC E911 in the US or the E112 recommendation in Europe, demand mobile devices to be able to report the position of the user with a certain accuracy in the case of an emergency. In addition, national governments such as the US use GNSS in security and surveillance operations, for instance, for guiding the border control with fleets of unmanned aerial vehicles (UAV). Timing is another application of GNSS that is widely used, for instance, synchronization between different base stations of mobile cells or power networks is based on GPS time. This means that for the correct interaction between different cells the use of a trustful reference is mandatory.

Despite the generalized idea that GNSS systems are completely trustful, in the recent years it has been demonstrated that the corruption of the navigation signals is possible. Back in 2001, the US Department of Transportation commissioned a report prepared by the John A. Volpe Center [1] regarding the effects of the potential GPS vulnerabilities on the US transportation system. The conclusions of this report clearly showed up that the civilian service of GPS is vulnerable to unintentional and intentional interferences, and so, the services and applications that rely on it. This conclusion is based mainly in three factors. The first is the low received power of the GNSS signals at the earth surface, which make them relatively easy to mask. Secondly, civilian GNSS services have open codes and signal structure what makes feasible that anybody with adequate knowledge can reproduce in a exact manner the legitimate signals. Finally, the emergence of Software Defined Radios (SDR) at reasonably affordable prices, brings the possibility of reproducing GNSS signals by unauthorized users. The works presented in [2] and [3] are clear examples of the possibilities that SDR offer.

Based on the above factors, the deliberate and non-authorized transmission of GNSS signals is becoming more and more feasible and can severely interfere the correct reception of authentic GNSS signals. In spite of this threat, common receivers are not prepared to alert the user under these circumstances, and therefore, it is important to seek ways to increase the robustness of GNSS receivers in front of this problem.

Many recent research works have been focused on the development of detection and mitigation techniques to this singular type of interference. Two sets of methods can be distinguished depending on whether they can be implemented in existing systems or not. In the former case, the defence consists in the evaluation of signal level and navigation parameters to detect the interference signal, for example power [4]–[6], time [7], [8], frequency [9], angle of arrival [10]–[12], relative movement [7], integrity measurements [13], [14]. On the other hand, we can find techniques that require changing the structure of the signal transmitted by the current systems. Often, the objective of this methods is to authenticate, by means of cryptography, the navigation data [15]–[17]. Despite this latter methods can ensure the integrity of the navigation signals, they do not offer a short-term solution for the problem. Instead, the solution for protecting existing systems must involve the analysis of different signal parameters and, since the signal-level information is readily available and its consistency can easily be checked at the receiver side.

Our proposal is based on the idea that GNSS signal replicas are a very specific type of interference. Unlike common RF interferences, spoofing may not be evident until the receiver has corrected its carrier and code at the correlation process. Therefore, by analysing the output correlation values of the

This work was supported by the Spanish Government projects TEC2011-28219 and EIC-ESA-2011-0079

978-1-4799-0486-0/13/$31.00 ©2013 IEEE

receiver one could find the traces of the interferences. At this point, the resulting signal in an interference-free environment is a constant value affected by noise while in the presence of multiple signals with the same spreading code, it is a sum of complex sinusoids at the residual frequencies. The remaining frequency errors in the second case are occasioned by the presence of the interference that affects the correct demodulation of the authentic signal. It is possible to detect the presence of the interference formulating a decision problem with the two states of the output correlation using the Generalized Likelihood Ratio Test (GLRT) which allows to decide the most likely event. However, it requires the estimation of the residual frequencies which are difficult to estimate using classical non-parametric techniques like the periodogram when the data record is short. For this reason we propose the use of a super-resolution frequency estimation method based on the Pisarenko Harmonic Decomposition (PHD) due to its simplicity compared to other algorithms. Thanks to the estimates obtained with PHD it is possible to carry out the GLRT and detect the presence of the interference.

This paper is structured as follows: Section II presents the model of the signal to analyse. Later in Section III the super-resolution detection technique is presented. Later, Section IV presents a couple of experiment results carried out with real signal simulated with advanced hardware.

II. Signal Model

Under normal circumstances the incoming GNSS signal for a given satellite is modulated by a carrier wave at the nominal frequency f_0 which is also affected by the relative movement between the satellite and the receiver causing a Doppler shift f_d. In addition, the propagation delay of the signal affects both the carrier and the code of the received signal by inducing a carrier phase error ϕ and a code-delay τ, respectively. In order to correctly receive the data bits of the message and carry out the time-delay estimation of the received signal (from where to obtain the pseudorange information for each satellite), the receiver performs a demodulation process. In this step the frequency and time errors are precisely estimated by generating a local replica of the carrier and a delayed version of the code signal that are multiplied by the incoming signals. As a consequence of the transformations made to the incoming signal the resulting process at the time instant n can be expressed as follows assuming the receiver is tracking:

$$y(p) = \alpha_1 e^{j\phi_1^e} sinc(f_1^e N_{scode}) R_c(\tau_1^e) + \eta'(p) \quad (1)$$

where ϕ_1^e, f_1^e and τ_1^e are the residual phase, frequency and code delay errors of the signal, $R_c(\tau)$ is the autocorrelation function of the code $c(p)$, N_{scode} is the number of samples per code and $\eta'(p)$ is the correlated noise component at time instant $t = pT_s$ with T_s the sampling time. Note that the value of the data bits has not been included in the correlation output. This assumption is only valid if the bits of the signal can be wiped off, for instance, by using a pilot signal whose secondary code is known. If no pilot signal is available the receiver can also predict the value of the navigation data bits by acquiring a complete copy of the full navigation message as described in [14, p. 166]. The subindex $_1$ in each parameter of (1) means that it is a value of the legitimate signal. Later, this subindex will be used to distinguish between authentic and non-authentic signal parameters. If the receiver is correctly tracking the signal, the errors f_1^e and τ_1^e are sufficiently small to be considered negligible. The same happens with the residual phase error if the relative dynamics of the signal is corrected. Figure 1 shows an expansion in the time domain of the real part of the correlation output $y(p)$ on the left plot. The right part of the figure represents the decimated version of the correlation process which can be defined as $z(n) \doteq y(nN_{scode})$ where N_{scode} is the number of samples per code.

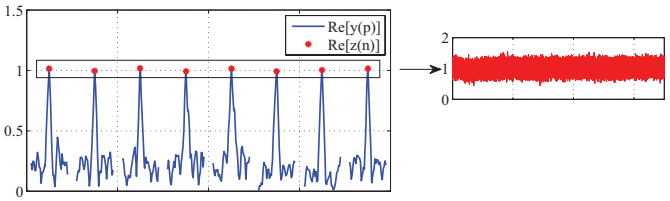

Fig. 1. Correlation process $z(n)$ obtained from the main correlator

Up to this point, the reception of only one signal with the same code has been considered, now, the problem of receiving K signals will be studied. As the transmitter of the false signals is placed in another position relative to the receiver and they are not synchronized, it is a valid assumption to expect different phases, code delays and frequencies in each signal. Under this situation, the correlator outputs will contain residuals of each signal parameter. In this scenario, the receiver tends to follow the signal that has more contribution to the main correlation as it tries to maximize the correlation between the incoming signal and its replica. However, the interaction between different signals can imply lock problems for the receiver, forcing the re-acquisition of the signal as shown in the results of [18]. Thus, the main correlation output can be expressed as:

$$z(n) = \sum_{k=1}^{K} a_k e^{j(2\pi f_k^e n + \phi_k^e)} + \eta(n) \quad (2)$$

where a_k is the amplitude of the k-th signal that includes the time and frequency dependent attenuation factors and $\eta(n)$ is typically modelled as a complex zero mean AWGN whose variance is given by [19, p. 23]: $\sigma_\eta^2 = \frac{N_0}{N_{scode} Ts}$ where N_0 is the noise spectral density. Frequently, the receiver performs an accumulation-and-dump process over N_{acc} consecutive samples of $z(n)$ in order to obtain an averaged version of it.

Based on (2) the detection of the presence of signal replicas is possible by detecting the presence of more than one sinusoid $K > 1$. One could formulate a binary spoofing detection problem where the null hypothesis $\mathcal{H}_0$ represents the case in which $K = 1$ and the spoofing hypothesis $\mathcal{H}_1$ all those cases

in which $K > 1$. In other words, the receiver can raise a spoofing alert if the frequency trace of more than one signal is found. In order to detect that the number of signals is $K > 1$ we will look for the presence of more than one frequency component f_k^e. A starting point to estimate these frequencies is the analysis of the autocorrelation of the data which gathers statistical information of the variations of the data with time.

III. Super-resolution spoofing detection

A. Second order statistical model

As seen in the previous section, and for a given spreading code, the presence of several code replicas in the GNSS received signal causes the code correlator output to be modeled by a superposition of several sinusoids. Each of these sinusoids corresponds to each of the code replicas being present in the received signal. In that sense, the problem of detecting the simultaneous presence of several code replicas can be transformed into the problem of detecting the simultaneous presence of several sinusoids. However, detecting the presence of these sinusoids is not a straightforward task since $z(n)$ is a random process due to the noise and the random phases of the signals. In these circumstances, we must resort to the exploitation of the second-order statistics of the received signal, which provide us information on the spectral content of the received random samples. To do so, we will consider the autocorrelation of the received samples denoted by $r_z(m)$, which is found to be given by:

$$\begin{aligned} r_z(m) &\doteq \mathrm{E}[z(n+m)z^*(n)] \\ &= \mathrm{E}[\sum_{k=1}^{K}\sum_{q=1}^{Q} a_k a_q^* e^{j(\omega_k^e(n+m)-\omega_q^e n+\phi_k^e-\phi_q^e)}] + \\ &+ \mathrm{E}[\eta(n+m)\eta^*(n)] \\ &= \sum_{k=1}^{K}\sum_{q=1}^{Q} \mathrm{E}[a_k a_q^*] e^{j\omega_k^e m} \mathrm{E}[e^{j(\omega_k^e-\omega_q^e)n} e^{j(\phi_k^e-\phi_q^e)}] + \\ &+ \sigma_\eta^2 \delta(m) \end{aligned} \tag{3}$$

where $\omega_k^e \doteq 2\pi f_k^e$, the residual frequencies f_k^e are considered as unknown deterministic values and that the factor $\mathrm{E}[e^{j(\omega_k^e-\omega_q^e)n} e^{j(\phi_k^e-\phi_q^e)}]$ is equal to 0. Note also that $\delta(m)$ represents the Dirac delta function. As a result, we have:

$$r_z(m) = \sum_{k=1}^{K} P_k e^{j2\pi f_k^e m} + \sigma_\eta^2 \delta(m) \tag{4}$$

where $P_k \doteq \mathrm{E}\left[|a_k|^2\right]$ is the power of the k-th signal being present.

Based on (4) it is possible to define the autocorrelation matrix $\mathbf{R_z} \doteq \mathrm{E}\left[\mathbf{z}_l \mathbf{z}_l^H\right]$ which results in a matrix of dimension $M \times M$ with the following structure:

$$\mathbf{R_z} = \begin{bmatrix} \sum_{k=1}^{K} P_k + \sigma_\eta^2 & \dots & \sum_{k=1}^{K} P_k e^{-Mj\omega_k^e} \\ \sum_{k=1}^{K} P_k e^{j\omega_k^e} & \dots & \sum_{k=1}^{K} P_k e^{-(M-1)j\omega_k^e} \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^{K} P_k e^{Mj\omega_k^e} & \dots & \sum_{k=1}^{K} P_k + \sigma_\eta^2 \end{bmatrix} \tag{5}$$

where $\mathbf{z}_l \doteq [z(lM), z(lM+1), \dots, z((l+1)M-1)]^T$ is the vector that contains M consecutive samples of the output of the main correlator corresponding to the instant l.

The structure of the matrix $\mathbf{R_z}$ presented in (5) contains the residual frequencies that have to be estimated in order to detect the presence of the sinusoids. In the following section we will show how this information is extracted in order to obtain the estimations $\hat{f}_k^e$.

B. Super-resolution frequency-domain technique for spoofing detection

As seen in the previous section the autocorrelation $r_z(m)$ in (4) contains the frequencies f_k^e that are present in the received signal. A way to extract this information is by estimating the spectrum of $z(n)$, whose shape will exhibit pronounced peaks at each of the frequency locations corresponding to each of code signal replicas f_k^e. That is,

$$S_z(f) = \sum_{k=1}^{K} P_k \delta(f - f_k) + \sigma_\eta^2 \tag{6}$$

where $S_z(f)$ stands for the power spectral density of the code correlator output samples $z(n)$ in (2). A widely used estimation method of (6) is the computation of the periodogram defined as $\hat{S}_{\mathrm{per}}(f) \doteq \mathrm{FFT}\{\hat{r}_z(m)\}$ where $\hat{r}_z(m)$ is the estimation of $r_z(m)$ based on a finite observation interval of $z(n)$. This method has been proved to be computationally efficient thanks to the implementation of the Fast Fourier Transform (FFT) [20] and it asymptotically provides unbiased estimates of the true spectrum. However, the periodogram presents serious limitations in terms of resolution, i.e. the ability of discriminating between closely spaced frequency components for short observation intervals. Also, it presents power leakage due to the presence of significant sidelobes, which may hinder the determination of the actual number of frequency components being present in the received samples. These drawbacks can be somehow circumvented by using different types of windows over the data at the expense of resolution as shown in [21, table 8.7]. Unfortunately, the application of the well-known periodogram does not fully suit the requirements of spoofing detection. The reasons are twofold. First, that the code replica detection should be performed very quickly, thus leading to the analysis of very short data records. Second, that the frequencies of the present code replicas may be very close one to each other, well below the resolution provided by the traditional periodogram (i.e. otherwise, they would be filtered out by the PLL loop filter). In these circumstances, a more precise spectral estimator is required.

For the problem at hand, spectral estimation techniques based on the eigenanalysis of the autocorrelation matrix $\mathbf{R_z}$ [21, p. 451] do offer a much better performance. These techniques are also known as super-resolution methods. The core idea of these methods is to separate the signal subspace (SS) and noise subspace (NS) present in $\mathbf{R_z}$ and find those frequencies that are orthogonal to the NS. From the set of super-

resolution methods the most used techniques are the MUSIC algorithm [22], the Johnsons approach [23] and the Pisarenko Harmonic Decomposition (PHD) [24]. These techniques have been widely adopted in the fields of radar and sonar, but their application to GNSS has remained unexplored, with the exception of very few contributions such as the one in [25]. In all these eigendecomposition or super-resolution methods, the extraction of the frequencies implies a decomposition of $\mathbf{R_z}$ that may incur in a high computational cost. In particular, according to [26] it implies from M^2 to M^3 operations. Is for this reason that super-resolution methods have had a poor integration in low complexity GNSS receivers. However, the current status of technology makes its implementation every time more feasible. Besides, for the specific case of PHD the whole set of eigenvalues and eigenvector is not needed but just the eigenvector associated to the minimum eigenvalue λ_{min}, and denoted herein by $\mathbf{v}_{\text{min}}$. The computation of $\mathbf{v}_{\text{min}}$ can be achieved iteratively [27]–[29] thus reducing the computational cost of the PHD. Since $\mathbf{v}_{\text{min}}$ is orthogonal to all the frequencies present in the signal, they can be estimated either by extracting its roots [21, p.459] or by computing the so-called pseudo-spectrum defined as:

$$\hat{S}_{\text{PHD}}(f) = \frac{1}{|\mathbf{e}^H(f)\mathbf{v}_{\text{min}}|^2} \tag{7}$$

where $\mathbf{e}(f) \doteq [1, e^{j2\pi f}, \ldots, e^{j(M-1)2\pi f}]^T$. Note that, the denominator of (7) can be computed as squared magnitude of the FFT of $\mathbf{v}_{\text{min}}$ at $f = \frac{2\pi h}{M}$ with $h = 1, 2, \ldots, N-1$, which also reduces its computational cost. In the case that a frequency f is present in the signal, the pseudo-spectrum $\hat{S}_{\text{PHD}}$ will show a peak in its shape.

At this point we propose the use of PHD as a super-resolution spoofing detection method with the aim of monitoring the presence of any residual frequency in the GNSS received signal samples. As long as the receiver is tracking correctly one signal, the estimated residual frequency will be located close to 0 Hz. In the absence of any other anomaly the rest of the estimated frequencies $\hat{f}_k^e$ will be due to the presence of noise, generating random spureous peak but with a much lower height than the one corresponding to the actual true signal. However, when an additional signal replica appears, an additional high peak will clearly appear in the eigenspectrum, thus highlighting the presence of an additional signal in the received samples. Note that, under the assumption that one signal replica is present beside the authentic one, the dimension of the matrix $\mathbf{R_z}$ has to be $M \geqslant 3$ in order to correctly estimate their frequencies. This solution also provides a way to mitigate the effects of the spoofing signal by notch filtering the specific frequency where the replica is located.

Figure 2 shows a comparison between the PHD pseudo-spectrum and the periodogram. Two complex sinusoids at frequencies 0.05 and 0.1 are summed together with complex AWGN noise with a SNR = 20 dB in both cases. For the two spectral estimators, the same correlation lags $r_z(m)$ are used that allow to build a matrix $\mathbf{R_z}$ with dimension $M = 3$ as defined in (5). The periodogram is unable to show the two spectral lines due to the lower resolution. On the other hand the super-resolution method is able to estimate the frequency location of the two signals.

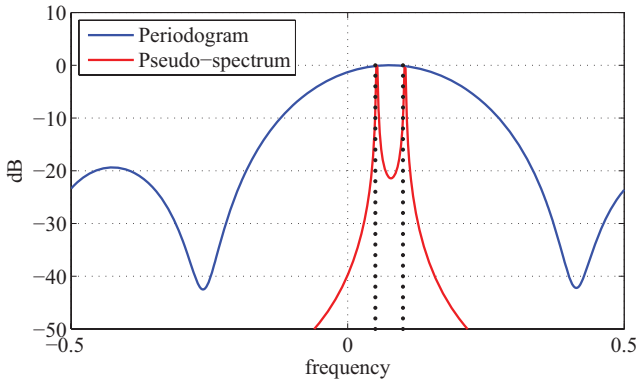

Fig. 2. Estimation of the signal spectrum based on the PHD and the computation of the periodogram when two different signals are present.

Once the frequencies of each signal have been estimated the next step is to detect whether the sinusoids are present or not. For the case of a sinusoidal signal with unknown amplitude, phase, frequency and time of arrival n_0, the Generalized Likelihood Ratio Test (GLRT) is presented in [30, p.269] and decides that a sinusoid at frequency f_0 is present after n_0 if:

$$\max_{n_0, f_0} \frac{1}{L} \left| \sum_{n=n_0}^{n_0+L-1} z(n) e^{-j2\pi f_0 n} \right|^2 > \gamma \tag{8}$$

where L is the observation window of the signal and γ is the decision threshold.

The statistic in (8) is the squared magnitude of the incoming signal multiplied by a complex sinusoid at frequency f_0. Without the knowledge of which frequencies are present in the signal one would have to seek in the whole range of frequencies. In our case, the estimations extracted from the PHD $\hat{f}_k^e$ are used to compute the statistic in (8); if it exceeds γ the detection mechanism declares that the signal is present.

For the selection of the threshold γ it is possible to compute the Receiver Operating Characteristic (ROC) Curve [31] to evaluate the performance of the test presented in (8). With it, a threshold that guarantees a given specification in terms of probability of false alarm P_{fa} or detection P_d can be chosen.

The block diagram in Figure 3 summarizes the different steps that compound the proposed signal replica detection technique. Note that the hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ represent the two states of the decision problem. The former case represents the absence of interference while the second reflects the presence of more than one signal at the correlation output.

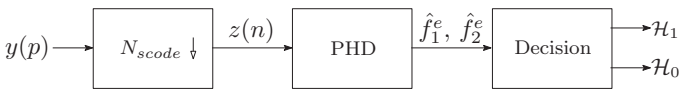

Fig. 3. Block diagram of the proposed super-resolution detection algorithm.

IV. Experiment Results

In order to evaluate the performance of the proposed super-resolution spoofing detection technique real GNSS signals generated by a Spirent hardware simulator have been used. This device allows complete flexibility in the definition of the scenario to simulate and provides full control on the generated signals. The signal simulator is connected to the same external reference than the recording hardware, a USRP N210 equipped with a DBSRX2 daughterboard. This front-end permits the USRP to work in the L1 band and downconvert the received signal to baseband. At this point the digitized signal can be processed in Matlab using a GNSS software receiver.

For this practical experiment the C/A GPS signal has been used. The tracking stage of the software receiver is performed by a pair of closed loops for both phase and code delay. The PLL noise bandwidth (B_{PLL}) is set to 10 Hz while the DLL bandwidth (B_{DLL}) is 1 Hz. For tracking the signal an accumulation of $N_{acc} = 10$ samples is used. Under these circumstances we apply the PHD to the accumulated output of the main correlator of the receiver. For the estimation of the matrix $\mathbf{R}_z$ of dimension $M = 3$ we use an exponential filter in the following way: $\hat{\mathbf{R}}_z^l = \alpha \hat{\mathbf{R}}_z^{l-1} + (1-\alpha)\mathbf{z}_l \mathbf{z}_l^H$ where the factor α is set to 0.98.

A. Experiment #1: Spoofing-free scenario

In this scenario only the authentic signal is present with a C/N_0 level of 46 dBHz. Applying the proposed technique a pair of frequency estimates $\hat{f}_k^e$ are obtained together with a realization of $\hat{S}_{\mathrm{PHD}}(f)$ for each snapshot l. The upper plot of Figure 4 represents the shape of the $\hat{S}_{\mathrm{PHD}}$ and its evolution with time. As can be seen, there is clearly a peak around frequency 0 Hz during all the observation period. In addition, another peak appears at each snapshot as a consequence of the noise. The second plot shows more clearly the two estimated frequencies. The residual frequency of the tracked signal is shown in green while the remaining estimation is plotted in blue. The second estimation has clearly a random behaviour with time as it occasioned by noise.

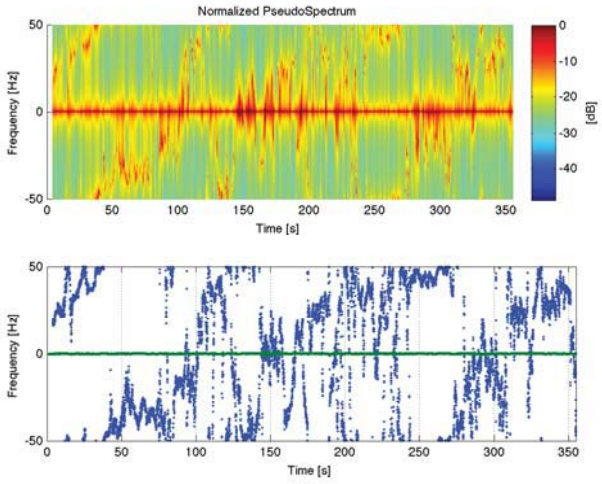

Fig. 4. Results of the PHD of the Experiment #1. The upper plot represents the normalized pseudo spectrum and bottom plot the two estimated frequencies.

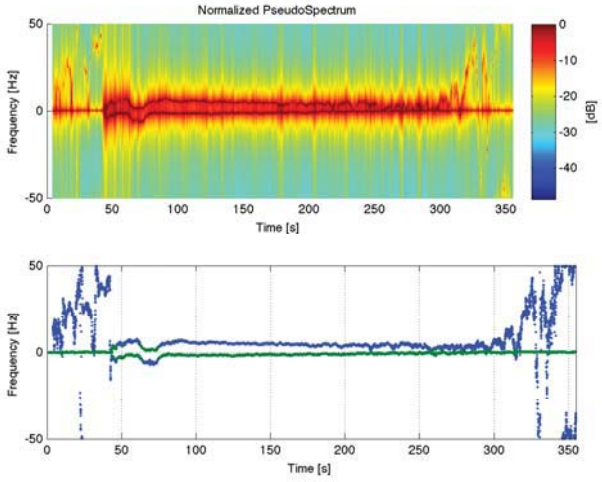

Fig. 5. Results of the PHD of the Experiment #2. The upper plot represents the normalized pseudo spectrum and bottom plot the two estimated frequencies.

B. Experiment #2: Spoofing-present scenario

In this case a signal replica appears after 22 seconds with 3 dB more in power which has, initially, the same frequency as the authentic but, after 45 seconds of simulation, its relative frequency changes to -5 Hz. In Figure 5 one can see clearly how the rise of the signal replica affects the estimation of the frequencies: after 45 seconds the two estimations $\hat{f}_1^e$ and $\hat{f}_2^e$ correspond to the frequencies of both the authentic and the replica signal. From the two plots of Figure 5 it is possible to observe the transition between one signal and the other. As can be seen, the two estimations $\hat{f}_k^e$ get worse as time goes by due to the fact that the relative delay between the two signals is growing. Both signals are distanced in frequency what causes a different relative code delay rate. As a consequence, one of the two signal has less and less contribution to the main correlator, what makes more difficult to estimate its frequency. Analysing in detail the results we can confirm that after the presence of the signal replica the receiver centres its main correlator in it. The measurements of the receiver in Figure 6 indicate that, by the end of the simulation, the power of the tracked signal is 3 dB higher corresponding to the signal replica and that the estimated Doppler shift is 5 Hz lower than at the beginning of the analysis.

Once the receiver detects the presence of the two components it has the possibility to mitigate the effects of the interference by avoiding the shift caused in frequency. The remaining problem to solve is to find which frequency estimation belongs to the signal replica and which not. In order to discriminate between both, the receiver may need to apply additional information such as relative dynamics or the use of integrity techniques to discard a signal.

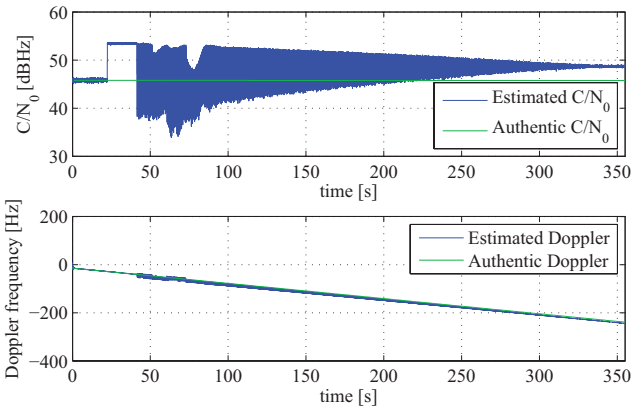

Fig. 6. The authentic and estimated C/N_0 are shown in the upper plot for Experiment #2. The bottom plot shows the authentic and estimated Doppler frequency of the signal.

V. Conclusions

A method for super-resolution detection of multiple GNSS signals under the same spreading code has been presented. The use of the PHD for super-resolution estimation of the main frequency components has been proved to work under the presence of spreading code replicas. Signals affected by this interference present a clear anomaly at the frequency-domain that is estimated by the method. With the outcome of the proposed technique (i.e. the frequency estimates of the signal replicas) the GNSS receiver is able to detect the counterfeit and mitigate its effects notching the frequency of the interference. Future work will include the development of the automatic detection mechanism based on the estimated frequency of the interference signal.

References

[1] "Vulnerabilty assessment of the transportation infrastructure relying on the global positioning system," John A. Volpe National Transportation Systems Center. Office of the Assistant Secretary for Transportation Policy. U.S. Department of Transportation, Tech. Rep., 2011.

[2] A. Brown, R. Tredway, and R. Taylor, "GPS signal simulation using open source gps receiver platform," in *Proceedings of the 21st Virginia Tech Symposium on Wireless Personal Communications, Blacksburg, Virginia*, 2011.

[3] R. Di, S. Peng, S. Taylor, and Y. Morton, "A USRP-based GNSS and interference signal generator and playback system," in *Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION*, april 2012, pp. 470 –478.

[4] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proceedings of the 18th International Technical Meeting of the Satellite Division of the ION*, 2005.

[5] H. Borowski, O. Isoz, F. M. Eklf, S. Lo, and D. Akos, "Detecting false signals with Automatic Gain Control," *GPS World*, vol. April, pp. 38–43, 2012.

[6] J. S. Warner, Ph.D., and P. Roger G. Johnston, "GPS spoofing countermeasures," in ., 2003.

[7] P. Papadimitratos and A. Jovanovic, "GNSS-based positioning: Attacks and countermeasures," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, nov. 2008, pp. 1 –7.

[8] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," in *International Journal of Navigation and Observation*, 2012.

[9] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," in *Proceedings of the 2010 International Technical Meeting of the ION*, 2010.

[10] J. Nielsen, A. Broumandan, , and G. Lachapelle, "GNSS spoofing detection for single antenna handheld receivers," in *Journal of The ION Vol. 58, No. 4,*, 2011.

[11] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," in *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, dec. 2010, pp. 1 –6.

[12] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the 2009 International Technical Meeting of The ION*, 2009.

[13] J. Juang, "GNSS spoofing analysis by VIAS," *Coordinates Magazine*, vol. February to November, 2011.

[14] E. Kaplan, *Understanding GPS - Principles and applications*, 2nd ed. Artech House, December 2005.

[15] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *ION GPS/GNSS 2003, 9-12 September 2003, Portland, OR*, 2003.

[16] M. Kuhn, "An asymmetric security mechanism for navigation signals," in *In Proceedings of the Information Hiding Workshop*. Springer, 2004, pp. 239–252.

[17] O. Pozzobon, "Keeping the spoofs out: Signal authentication for future GNSS," *InsideGNSS*, vol. 59, pp. 48–55, 2011.

[18] J. M. Parro-Jimenez, R. Ioannides, M. Crisci, and J. A. Lopez-Salcedo, "Detection and mitigation of non-authentic GNSS signals: preliminary sensitivity analysis of receiver tracking loops," in *Proc. 6th ESA Workshop on Satellite Navigation User Equipment Technologies (NAVITEC)*, 2012.

[19] J. T. Curran, "Weak signal digital GNSS tracking," Ph.D. dissertation, Department of Electrical and Electronic Engineering, National University of Ireland, Cork., 2010.

[20] H. So, Y. Chan, Q. Ma, and P. Ching, "Comparison of various periodograms for sinusoid detection and frequency estimation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 35, no. 3, pp. 945–952, 1999.

[21] M. H. Hayes, *Statistical Digital Signal Processing and Modeling*. Wiley, Mar. 1996.

[22] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation,*, vol. 34, no. 3, pp. 276–280, 1986.

[23] D. Johnson and S. DeGraaf, "Improving the resolution of bearing in passive sonar arrays by eigenvalue analysis," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 30, no. 4, pp. 638–647, 1982.

[24] V. F. Pisarenko, "The retrieval of harmonics from a covariance function," *Geophysical Journal of the Royal Astronomical Society*, vol. 33, no. 3, pp. 347–366, 1973.

[25] F. Benedetto, G. Giunta, A. Neri, and L. Vandendorpe, "Enhanced code acquisition in global positioning radio systems," in *Proc. of the 3rd Workshop on Positioning, Navigation and Communication (WPNC'06)*, 2006, pp. 1–8.

[26] S. Kay and J. Marple, S.L., "Spectrum analysis;a modern perspective," *Proceedings of the IEEE*, vol. 69, no. 11, pp. 1380–1419, 1981.

[27] Y. H. Hu, "Adaptive methods for real time Pisarenko spectrum estimate," in *IEEE International Conference on ICASSP '85 Acoustics, Speech, and Signal Processing*, vol. 10, 1985, pp. 105–108.

[28] V. Reddy, B. Egardt, and T. Kailath, "Least squares type algorithm for adaptive implementation of Pisarenko's harmonic retrieval method," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 30, no. 3, pp. 399–405, 1982.

[29] H. So and K. W. Chan, "Reformulation of Pisarenko harmonic decomposition method for single-tone frequency estimation," *IEEE Transactions on Signal Processing*, vol. 52, no. 4, pp. 1128–1135, 2004.

[30] S. Kay, *Fundamentals Of Statistical Processing, Volume 2: Detection Theory*, A. Oppenheim, Ed. Pearson Education, 2009.

[31] T. Fawcett, "An introduction to ROC analysis," *Pattern Recogn. Lett.*, vol. 27, no. 8, pp. 861–874, Jun. 2006.