Detection and mitigation of non-authentic GNSS signals: preliminary sensitivity analysis of receiver tracking loops

Juan M. Parro-Jiménez, Rigas T. Ioannides and Massimo Crisci
TEC-ETN ESA/ESTEC
European Space Agency
Noordwijk, The Netherlands
{juan.parro;rigas.ioannides;massimo.crisci}@esa.int

José A. López-Salcedo
SPCOMNAV Engineering School
Universitat Autònoma de Barcelona
Bellaterra, Spain
jose.salcedo@uab.es

***Abstract*—A myriad of applications are based on the positioning and timing information provided by GNSS systems. Protecting the system against any kind of interference has been always on the focus of researchers and manufacturers. Unintentional and intentional interferences are two well known ways to mislead the results of GNSS receivers. However, it has been recently, with the mass-market production of Software Defined Radio (SDR) equipment and cheap hardware signal generators,when retransmission of delayed signal replicas or the generation of a modified version becomes even more feasible. For this reason, this paper attempts to perform an initial sensitivity assessment of the receiver tracking stage against this singular kind of disturbance. This analysis is critical for the development of appropriate techniques to detect and mitigate the effects of non-authentic signals reception.**

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 this scenario, GNSS can offer a precise information of positioning and timing.

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:

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

- *Low Received Power:* Due to the enormous propagation loss that the GNSS signals suffer, they are received with very low power on the ground, indeed, they are buried in thermal noise. One example of this is [2, subsection 2.2.1] where the nominal received signal of GPS on the Earth surface is specified to be -158.5 dBW. This fact implies that the original signal can be masked by others that, even with relative low power, are more powerful. For this reason, the mitigation of interference signals (intentional or unintentional) is always a hot research topic. Some recent works on this field are [3] and [4].
- *Codes and Structure:* Some GNSS services, such as civilian GPS, are completely open to users. This means that their navigation codes, as well as the message structure, are public. The idea behind this openness is to promote the investigation and development on the field of satellite navigation. The massive use of GNSS in recent years mainly started after the creation of the civilian GPS service, afterwards, other GNSS systems with open services, including GLONASS from Russia or Galileo from Europe, have contributed to it.
- *Low Cost Signal Simulators:* Replicating GNSS signals has always been a requirement of receiver manufacturers that want to test their devices. Advanced signal generators have been used during the last decades to test the performance of GNSS receivers. Nevertheless, the high cost of these simulators has made that only companies or big research centers were able to afford one. However, the rapid advances in semiconductor technologies have allowed the production of Software Defined Radios (SDR) at very low prices, thus making them available to the mass market. In addition, the possibility of easily configuring these devices via software, instead of hardware, attracts the attention of Open Source users interested in developing new and low cost applications. The works presented in [5] and [6] are clear examples of the possibilities that SDR offer for the simulation of GNSS signals.

Based on the above factors, the possibility of receiving GNSS replica signals that can interfere the correct measurement of the authentic signals, is becoming more and more feasible. In addition, common receivers are not prepared to alert the user under these circumstances. Therefore, it is important to seek ways to increase the robustness of the receiver in front of this problem.

There are plenty of activities and applications that rely on GNSS open services that do not include authentication or guarantee. If GNSS navigation can be corrupted it could affect critical activities such as manned/unmanned aviation or maritime guidance. Recently, the researchers of the University of Texas have carried out a replica signal attack to an Unmanned Aerial Vehicle (UAV) [7]. As a consequence of this experiment, the researchers were able to change the directions of the vehicle and force it to land.

Timing is another application of GNSS that is widely used, for instance, synchronization between different base stations of mobile cell networks is based on GPS time. This means that for the correct interaction between different cells the use of a trustful reference is mandatory. Timing corruption can cause that multiple base stations interfere with each other since they assume that all are using the same reference. Power networks also rely on GPS time to correctly measure the status of the system. The corruption of this timing reference can cause the blackout of this service. In this sense, the authors in [8] briefly describe a novel synchronization scheme for a power system network. It is based on the GPS time to synchronize the different devices that control the power status. This synchronization is fundamental for the correct performance of the power system since the measurements of the control units are used to analyse it. As the authors highlight in their work, the use of replica signals is a serious problem to critical infrastructure applications that rely in open GNSS services. Finally, they demonstrate their statement by misleading the timing solution of one of the measurement units, injecting cloned GPS signals. Banking and financial activities also employ GPS as a reference to time stamp the instants of each trade. It is not necessary to say that the lack of synchronization in these kind of operations can compromise the savings and investments of many people. These are just some applications in which the use of a reliable GNSS civilian service is mandatory. Therefore, it is essential to deeply analyse the GNSS-like interferences in order to detect the sensibility of the system and develop techniques to increase the robustness of the receivers.

Many recent research works have been focused on the development of detection and mitigation techniques to this singular type of interference. Two big sets of methods can be distinguished depending on whether they are oriented to existing or to future systems. In the former case, the defence consists in the evaluation of signal level and navigation parameters to detect the interference signal, for example power [9], [10], [11], time [12], [13], frequency [14], angle of arrival [15], [16], [17], relative movement [12], integrity measurements [18], [19]. On the other hand, we can find techniques that require changing the structure of the signal transmitted by the system. Often, the objective of this methods is to authenticate, by means of cryptography, the navigation data [20], [21],[22], [23]. Despite this latter methods can ensure the integrity of the navigation signals, they do not offer a short-term solution for the problem. Therefore, the solution for protecting existing systems must involve the analysis of different signal parameters and checking their consistency. Another difficulty in the development of detection and mitigation methods is the wide range of GNSS applications, each one with its own requirements and limitations.

This paper is an initial evaluation of the effects that a cloned signal can have on the receiver. Specifically, the tracking stage of a common receiver will be the center of our analysis, since this is the key stage where code and phase observables are obtained. We will study how the replica signals interfere the measurements of the receiver for different given configurations. The results of this initial study will be proved by means of practical experimentation. The work presented here will be used as a reference to analyse the sensitivity of a common GNSS receiver, thus allowing us to develop more robust detection and mitigation techniques.

After this introduction, Section II analyses the impact of the reception of GNSS-like signals at the receiver tracking level looking for promising parameters that allow the user to detect the presence of this interference. Once these indicators have been selected, Section III tries to isolate each feature of the signal and describe its potential impact on the receiver. In Section IV, and according to the table developed in Section III, a specific cloned signal scenario will be selected to test experimentally with the appropriate equipment. The results extracted from these simulation environment will be presented and discussed in detail.

Finally, it is important to remark that the results we will present here are based on the GPS L1 signal as it is the former satellite navigation system and thus the majority of the work involving the reception of cloned signals are centred on it.

II. Impact of replica signals at the receiver level

In order to identify which are the key parameters involved in the GNSS receiver processing (i.e. the ones that could be affected by intentional interfering signals) we will start describing the analytical formulation of the received signal affected by a cloned signal and, later, the signal at the output of the correlation process will be presented and studied.

A. Received signal model in the presence of a cloned signal

The baseband equivalent of the transmitted signal from the m-th GNSS satellite can be written in its discrete form as:

$$s_m(n) = \sum_{i=-\infty}^{\infty} b_m(i) \sum_{q=0}^{N_c N sc N_r - 1} c_m((q)_{N_c}) p(n - iN_{sb} - qN_{sc}) \quad (1)$$

where N_{sc} is the number of samples per chip, N_r is the number of code repetitions per bit, N_{sb} is the number of samples per bit, N_c is the number of chips per code, $()_N$ is the

modulo-N operation, $b_m(i)$ is the value of the i-th bit, $c_m(k)$ is the amplitude of the k-th chip. For both cases, the possible values are $\{-1, 1\}$. Finally, $p(n)$ represents the shaping pulse of the signal.

Considering the reception of the signal from M satellites, the distortionless received signal can be expressed as follows:

$$r'(n) = \sum_{m=0}^{M-1} \alpha_m e^{j\phi_m} e^{j2\pi f_m n} s_m(n - \tau_m) + \eta(n) \qquad (2)$$

where $\alpha e^{j\phi_m}$ is the complex amplitude of the m-th incoming signal, f_m is the residual frequency error, τ_m is the delay of the signal and $\eta(n)$ is the n-th sample of the complex Additive White Gaussian Noise (AWGN).

At this point, we consider the injection of cloned GNSS signals which, actually, have the same structure as in (1). Consequently, the received signal is:

$$\begin{aligned} r(n) &= \sum_{m\in\mathcal{A}} \alpha_m^a e^{j\phi_m^a} e^{j2\pi f_m^a n} s_m^a(n - \tau_m^a) + \\ &+ \sum_{l\in\mathcal{S}} \alpha_l^s e^{j\phi_l^s} e^{j2\pi f_l^s n} s_l^s(n - \tau_l^s) + \eta(n) \end{aligned} \qquad (3)$$

where $\mathcal{A}$ is the set of authentic received signals and $\mathcal{S}$ is the set of cloned signals, the superindex a represents the parameters of the authentic signals and s those from the replica signals.

From the set of received satellite signals $\mathcal{A} \cup \mathcal{S}$ we can distinguish three cases: i)only an authentic signal is present; ii) only a non-authentic signal is present and iii) both authentic and non-authentic signals are present. The set of signals with only cloned component can be easily detected by analysing the almanac data of the navigation message. On the other hand, the set of signals that have both an authentic component and an interfering one are the focus of this study since its detection involves a more difficult challenge. From now on, we will distinguish the authentic signal and the replica signal with the superindexes a and s respectively. The following notation represents the received free of noise signal in which $m = l$, being this the PRN index of the satellite:

$$\begin{aligned} r_m(n) &= \alpha^a e^{j\phi^a} e^{j2\pi f^a n} s^a(n - \tau^a) + \\ &+ \alpha^s e^{j\phi^s} e^{j2\pi f^s n} s^s(n - \tau^s) + \eta(n) \end{aligned} \qquad (4)$$

B. Correlator output signal in the presence of signal replicas

The correlation process involves the carrier and code wipe-off in order to correct the delay and residual frequency of the signal. For the signal in (4), the k-th output of the correlator after the integration interval T_i can be expressed, according to [24, pag 364], as follows:

$$\begin{aligned} z_k(\tau_e, f_e) &= \alpha^a e^{j(\phi_k^a - \phi_e)} sinc(\Delta f^a T_i) R(\Delta\tau^a) \\ &+ \alpha^s e^{j(\phi_k^s - \phi_e))} sinc(\Delta f^s T_i) R(\Delta\tau^s) + w_k \end{aligned} \qquad (5)$$

where $R(\tau)$ is the autocorrelation function of the CA code, ϕ_k is the phase of the received signal at integration instant k, w_k is the k-th component of the correlated AWGN noise, $\Delta f = f - f_e$ and $\Delta\tau = \tau - \tau_e$ are the differences between the residual frequency and code delay of the cloned or authentic signal, with respect to the estimated f_e and code delay τ_e at the receiver. Note that, in the absence of replica signal, the estimations f_e and τ_e are close to the values of the authentic signal. Common receivers are equipped with tracking loops for the carrier phase (PLL) and code delay (DLL). The former one aligns the carrier phase (and frequency) of the local oscillator to that of the received signal, whereas the second one aligns the code delay of the local code generator, to that of the received signal. Each loop filters the incoming signals with a very narrow filter (depending on the application it can typically vary from 10 to 20Hz for B_{PLL} and from 0.25 to 5Hz for B_{DLL}). From the amplitude of each signal, the ratio between the two powers when they reach the receiver can be defined as SSR$= \frac{(\alpha^a)^2}{(\alpha^s)^2}$.

The process of correlation slightly attenuates individually each signal present in (5) according to its delay and frequency with respect to the tracking point of the receiver (τ_e, f_e). Regarding the delay of the signal, the attenuation is due to the shape of $R(\tau)$, which is ideally a triangle centred at $\tau = 0$ and extended from -1 to 1 chip. On the other hand, the correlation process implies a filtering effect on the signal reflected by the factor $sinc(\Delta f T_i)$. This means that the receiver itself is able to reject signal components that appear in the incoming signal but are distanced in time and frequency from the tracked signal. Specifically, three are the parameters that define the level of this rejection: the differences in frequency and delay of the signal Δf and $\Delta\tau$, respectively, and the integration time used by the receiver T_i. Figure 1 shows the correlation output affected by a cloned signal for two different cases. In both situations the SSR is the same but the parameters of the cloned signal modify its contribution to the total correlation.

In a normal situation, the receiver tracks the authentic signal. However, if a cloned signal appears in the main correlator, it can modify this behaviour. Specifically, the effects on the

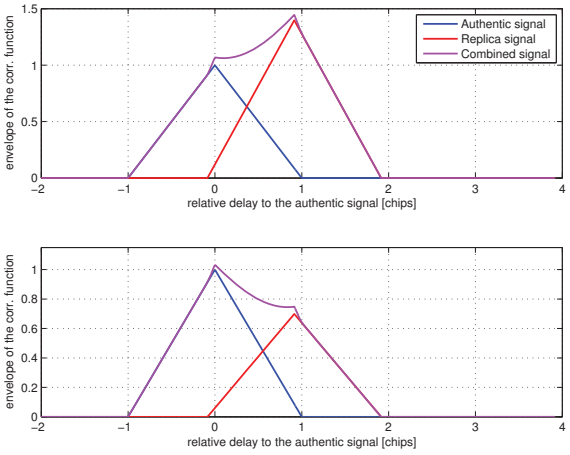

Fig. 1. Envelopes of the authentic, cloned and combined signals for two different pairs of (f^s, τ^s)

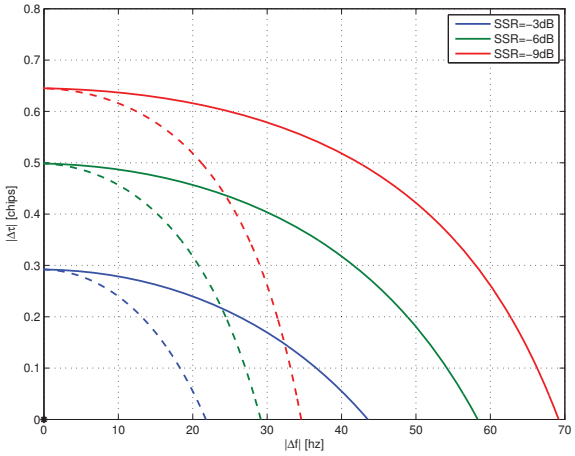

Fig. 2. Limiting border between regions A and B for SSR=-3,-6 and -9. An integration time of 10ms is used in continuous lines and 20ms in discontinuous lines.

tracking loops will depend on the contribution of the new signal in terms of power. As extracted from (5), the replica signal will suffer an attenuation of its power as it is displaced from the tracking point of the receiver. As a consequence of this attenuation, two possibilities involve the contribution of each signal to the main correlator: A) in which the cloned signal is more powerful than the authentic and B) the case in which the authentic signal remains more powerful than the cloned one. Regarding the effects of each situation, a case B replica signal will cause misleading estimations on the receiver, similar to a multipath signal that arrives to the receiver with lower power than the Line Of Sight (LOS). On the other hand, a case A cloned signal can force the receiver loops to follow its dynamics as it is more powerful than the authentic. Nevertheless, the resulting jump in frequency and delay, from the initially tracked signal to the cloned one, may overpass the loop bandwidths resulting in a loss of lock. In the worst case, the transition of the PLL tracking status, will remain stable, since the PLL jump will be buried below the bandwidth. Figure 2 represents the limiting border between the set of cases A, inside the ellipses around the point $\tau_e = 0, f_e = 0$, and cases B, outside the ellipse, for different values of SSR and T_i. As expected, the area of cases A grows with the SSR and narrows with T_i.

Note that the ellipses of Figure 2 are centred on the authentic signal that is placed at $\Delta\tau = 0$ and $\Delta f = 0$ before the replica signal arrives. After that, the estimated values τ_e and f_e will be erroneous as the receiver will track a combination of the two signals as presented in (5). Depending on which of the cases defined previously is happening, the receiver will finally follow one signal or the other. Therefore, the values of SSR and the difference in frequency and code delay of the cloned signal with respect to the tracked signal, will be the key parameters that decide whether the replica signal is finally tracked or not.

III. Impact Assessment Matrix

As seen in the previous section, analysing the consequences of the reception of a GNSS satellite-like signal involves the study of different parameters. Depending on the behaviour of each of them, the impact of their interference will be completely different and so, the way to face the problem. Moreover, depending on the user application, the receiver will have different configuration, different equipment and different requirements, which will change its level of vulnerability in the presence of a specific cloned signal. For instance, the configuration of a user mobile receiver and its hardware will not be comparable to the ones of a ground station. In addition, the defending capabilities of each receiver against the presence of a cloned signal are totally different. In order to develop strong detection and mitigation techniques, it is important for the designers to know exactly what the sensibility level of the receiver for different parameters of a replicated signal.

From the signal model in the presence of a cloned signal presented in Section II-B, it is possible to see that the parameters that will play a more active role are the power, the delay and the frequency of the cloned signal. These parameters will be evaluated relative to the receiver estimates of delay τ_e and frequency f_e and the SSR. We can assume that the interferer will not have the possibility to adapt the carrier phase of its signal, because this would require a perfect knowledge of the user position in the centimetre level. Moreover, the addition of the two signals with different frequencies will cause a continuous change in the carrier phase of the composite signal.

For each of the highlighted parameters different configurations are discussed, thus creating a matrix gathering several number of replay signal cases. The aim of this matrix is to provide an overall picture on the comparison between different configurations of the cloned signal and the corresponding test that needs to be applied in order to identify correctly the replica signal. Note that we analyse the parameters of the cloned signal individually, however, multiple cloned signals may be present in the incoming signal. Consequently, the navigation results obtained from these measurements will change, therefore, the effect of cloning one or more signals should be take into account.

The resulting impact assessment matrix is represented in Figure 3. An additional column includes some possible actions that the receiver could carry out in order to identify the presence of the replica signal.

A. Cloned Signal Power

The power of the cloned signal, represented in (5) as $P^s = (\alpha^s)^2$, is the power received in the antenna of the receiver. The behaviour of P^s with time is essential to identify the impact of the replica signal because, depending on the SSR, it can mislead the receiver results. A power jump of the replica signal, is the most simple case that will be considered in the analysis of the impact on the receiver. A more sophisticated case includes a replica signal that has a linear power ramp which would result in a smoother, and so more difficult to detect, transition of the GNSS receiver tracking loops. As last

Cloned signal Parameter	Configuration	Possible Receiver Defense Action
Power	Constant	Sudden and unexpected jumps in the estimated values of CN0
	Ramp	Unexpected changes in the estimated values of CN0
	Random	Sudden and unexpected jumps in the estimated values of CN0
Delay	Constant	Anomalous code delays estimations
	Ramp (doppler consistent)	Incoherence between user movement and estimated code delay
	Ramp (NO-doppler consistent)	Incoherence between time and frequency
	Random	Unexpected jumps in code delay estimation
Frequency	Constant	Unexpected loss of lock if the frequency exceeds the loop bandwidth
	Ramp	Incoherence between user movement and estimated pseudorange

Fig. 3. Matrix gathering all the configurations of the key parameters involving a replica signal interference.

configuration we assume a value of P^s that will vary in a random way with time.

B. Cloned Signal Code Delay

The code delay of the replica signal is a critical parameter because this is indeed the key observable that is used by most receivers in order to compute the user's position. A replica signal placed in a time delay near the authentic one can cause dramatic errors in the estimation of τ_e, but it can also take control of loops of the receiver depending on its dynamics. For this code delay parameter we will consider several configurations due to its importance. The most simple case is a cloned signal with a constant delay with respect to the authentic signal. Alternatively, the delay τ^s can vary with time, for instance, in a linear way. The concept of changing the amount of delay of the signal is directly related with the relative movement between the receiver and the satellite. As a consequence, an additional doppler shift should affect the frequency f^s if the delay of the signal is consistent with its physical interpretation. Nevertheless, the cases of a ramp delay consistent and non-consistent with the signal frequency will be taken into account. The last configuration assumed for the delay is a value of τ_e that changes randomly, as the cloned signal jumps from one delay to other.

C. Cloned Signal Frequency

As said before, when the receiver is tracking the authentic signal, the corresponding frequency estimate is fully contained within the (very narrow) bandwidth of the PLL loop filter. Consequently, the impact of having present an additional cloned signal frequency on the receiver will depend on the bandwidth of the PLL (B_{PLL}) and the distance of the cloned signal frequency with respect to the frequency currently being tracked. The basic configuration considered for the analysis of this case is a frequency jump lower or higher than B_{PLL}. A more sophisticated configuration involves using a linear ramp in frequency that sweeps through a range of frequencies where the authentic signal is placed. Note that, unlike the case of a frequency jump, this configuration is not related to the value f^a.

IV. Experimental Results

From the parameters matrix presented in Figure 3, it is possible to define a scenario by choosing one specific configuration for each parameter of the matrix. As a result, different cloned signal scenarios can be tested looking for the worst case impact on the receiver. Through this procedure, we can evaluate what the effects suffered by the receiver are in this worst case scenario. Under these circumstances, the development of reliable detection and mitigation methods will be our main objective, since its success against the most dangerous cases will ensure that less dangerous attacks can be also detected.

A. Evaluation Tools

In order to test the effects of different replica signals, a realistic approach would be using a commercial hardware receiver and analyse its results. However, some effects caused by the replica signal can be masked by the processing algorithms of the receiver. For instance, the interaction between the two signals can cause a loss of lock and, for this situation, the receivers are equipped with re-lock algorithms that allow them to reacquire the signal. In order to isolate these practical issues from the actual purpose of this study, we have developed in Matlab a software receiver simulator based only on the tracking stage. This will allow us to simulate a specific replica signal scenario from the matrix in Figure 3 and evaluate the behaviour of conventional tracking loops in the presence of cloned signals.

In order to validate our results with a real hardware receiver, we will use the control tool SCSV developed by Qascom [25] in the GAUPSS project which is already integrated in the Radio-Navigation Laboratoy of ESTEC. With this tool allow us to control a signal simulator under different architectures in order to test different commercial receivers.

B. Experimental Test Results

From the matrix in Figure 3, we have selected a scenario that will be evaluated during the next sections. This scenario is described in Table I. In this case, the cloned signal appears with a certain SSR once the receiver is tracking the authentic signal. Both the code delay and the frequency of the cloned signal (τ^s, f^s) can initially be different from the tracked ones, in our case, we consider a cloned signal at the same delay than the tracked signal but with an additional doppler. While the frequency remains constant in time with respect to the authentic one, the code delay of the signal has a linear ramp dynamics, moving away from the authentic one. This

scenario is clearly sensible to the tracking loops bandwidths of the receiver, for this reason, its effect with respect to this parameter will be evaluated. Our software receiver simulator will be used to set the basis of preliminary conclusions that will be confirmed later on with the hardware equipment in the laboratory presented before.

Power	Constant
Code Delay	Ramp (Doppler Consistent)
Frequency	Constant

TABLE I
SCENARIO WITH REPLICA SIGNAL PARAMETERS CONFIGURATION

1) Experiment I: The first experiment presented here is a set of simulations carried out with the software simulator receiver to individually study how the estimates of power, code delay and frequency of the receiver change with time. To do so, we configure our software receiver with a PLL bandwidth of $B_{PLL} = 10$Hz and the DLL bandwidth to $B_{DLL} = 0,25$Hz. For both cases a third order loop is selected. The E-L spacing used is 0,1 chips and the integration period is set to 10ms. In the case of the DLL discriminator, the envelope Early minus Late is chosen while the PLL discriminator is set to be the $atan$ function Costas discriminator. The interested reader can find more information about these discriminators on [19, Ch.5].

Regarding the cloned simulated signal, a set of three different f^s are selected (5Hz, 15Hz and 25Hz) that, in turn, will define the dynamics of the code delay τ^s. Recall that the rate of change of the code delay is related with the doppler frequency of the signal through $f_d = -f_o r_\tau$ where f_d is the doppler frequency, f_o is the carrier frequency (L1) and r_τ is the rate of change of the code delay. Therefore, if the cloned signal has a constant frequency difference with respect to the authentic signal, the code delay τ^s will change its delay in a linear way with respect to the authentic signal delay τ^a. Initially, we specify that both signals are aligned in time, $\tau^a = \tau^s$, which means that, once the replica signal appears after 10 seconds of simulation, it is also aligned with the receiver estimation τ_e. The value of SSR has a constant behaviour with time and equal to -3dB, meaning that the power of the replica signal is twice the power of the authentic signal. The value of C/N_0 of the authentic signal is set to 44dBHz in order to simulate a good signal condition. The relative phase between the two signals is a random value between π and $-\pi$ radians.

Figure 4 shows the amount of error in the receiver frequency estimation with respect to the authentic frequency as defined in equation (5) as $\Delta f^a = f^a - f_e$, for the three different cases simulated. As we can see for the simulations of 5Hz and 15Hz the receiver is tracking the replica signal frequency instead of the authentic one after the cloned signal appears. Despite the case of 15Hz is above B_{PLL} the receiver is able to track the replica carrier phase. This can be explained as the transition from the initial frequency estimation to 15Hz is not a sudden jump but there is a period where the receiver is tracking the composite signal compound by the authentic and the replica signal. The third subplot is the case of the 25Hz cloned signal which the receiver is not able to track correctly. Note that, in all the cases, there is an interval in which the variability of the estimations is greater, which is caused by interaction of the two signals on the main correlator. Once the cloned signal is away from the delay of the authentic signal by more than 1 chip, it does not have any contribution to the correlator, and the variability of the estimates decreases. In Figure 5 the code delay error in the receiver estimation $\Delta\tau^a = \tau^a - \tau_e$ is represented for the three cases. It is possible to see that the DLL is tracking the replica signal all the time, instead of the authentic signal. The different rates of the code delay are caused by the relation of this parameter with the doppler frequency of the signal. In the case of $f^s = 25$Hz despite the receiver was not able to catch up the carrier phase of cloned signal the DLL is able to track the replica code delay because the envelope of the correlator output is used to track the signal. Finally, Figure 6 represents the difference between the power of the authentic signal and the power estimated by the receiver. Due to the interaction between the two signals, their relative carrier phases are changing with time and so, the power of the combined signal can drop by more than 5dB. In addition, when the two signals are in-phase the resulting power is much greater than the power of the authentic signal. Note that, for Figure 4, 5 and 6 the dashed lines represent the difference between the values of the replica signal and the authentic signal (blue) and the expected value of estimation error if the authentic signal is tracked (green) which is 0.

The results shown here can vary and since because they are simulated as a random process both because of the effect of the noise and the phase difference between the two signals, which is also simulated as a random value. In addition, it is of interest to identify what is the effect that the PLL bandwidth

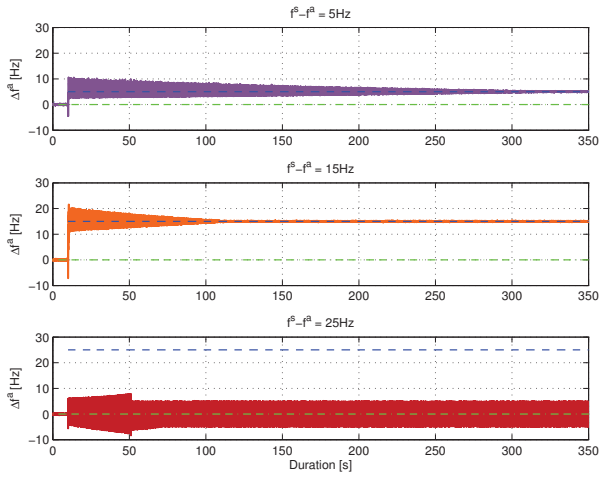

Fig. 4. Evolution of the error in the estimation of the authentic signal frequency.

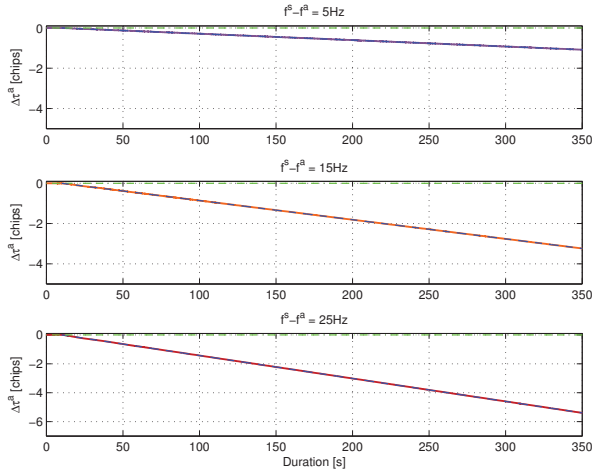

Fig. 5. Evolution of the error in the estimation of the authentic signal code delay.

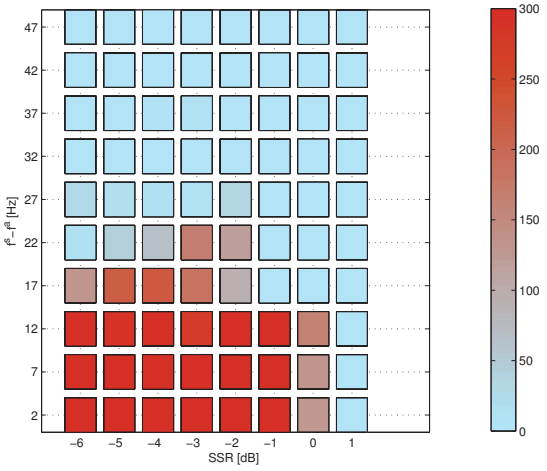

Fig. 7. Results of 300 simulations for different pairs of SSR and $f^s - f^a$ regarding the final tracking of the cloned signal.

has on the signal when a cloned signal is present on the main correlator. Therefore, the scenario of Table I can be studied for different values of cloned signal frequency and for different values of SSR, looking for those pairs that will cause that the replica signal takes the loops of the receiver without losing its lock. Figure 7 shows the number of cases in which the receiver follows the cloned signal, over 300 simulations, for each pair of $f^s - f^a$ and SSR. Note that the same configuration on the receiver has been taken into account. As can be seen, for cloned signal powers lower than the authentic signal the tracking of the authentic remains without change. Regarding the frequency, the receiver has difficulties to track the signals that overpass the authentic one more than 20Hz. However, there is a range of SSR values for which the receiver is able to track the cloned signal for larger values of $f^s - f^a$, specifically between -2 and -4 dB. The explanation of these results is that, as the cloned signal has a power comparable to the authentic signal, the estimate f_e does not suffer a sudden jump but a gradual transition from the authentic signal to the cloned signal. For larger values of SSR, this jump is more abrupt, forcing the loop to lose the lock of the signal. Note that the blue points in Figure 7 represent all the cases in which the receiver is not tracking the replica signal. This includes loss of lock cases, situations in which the authentic signal is tracked, etc. When the phase lock is lost, the re-acquisition process will decide which signal is tracked again.

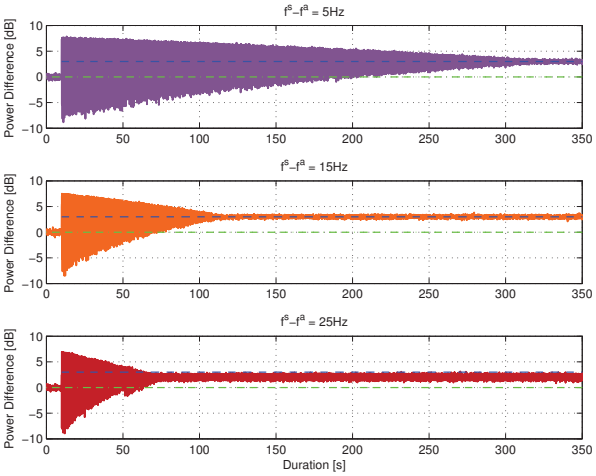

Fig. 6. Difference in power caused by the cloned signal with respect to the authentic signal power.

2) Experiment II: The objective of this experiment is to validate the results of the first experiment on a real hardware receiver. With the use of the laboratory tool presented in Section IV-A we will carry out different simulations with the same conditions of the first experiment. To do so, a configurable commercial receiver is set with the same configuration used previously. We do not expect to have exactly the same results as the behaviour of the receiver against the cloned signal is impossible to predict, however, some similarities are expected. To generate the signal, an advanced signal generator is chosen. The SCSV tool includes the possibility of monitoring the parameters estimated by the receiver and compare them with the values generated by the signal generator.

The same three cases simulated in the previous experiment are tested and the extracted results are presented in Figure 8. For the three cases, the cloned signal appears in the initial instant with the same initial code delay as τ^a but with a different frequency in each case. The top subplot of Figure 8, represents the code delay error estimation $\Delta\tau^a$ against the difference between the code delays of the authentic and the cloned signal $\tau^s - \tau^a$. As can be seen, the errors in the estimates of τ_e are caused by the distance between the authentic and the replica signals since, from the beginning, the receiver is tracking the cloned signal. As happened in the

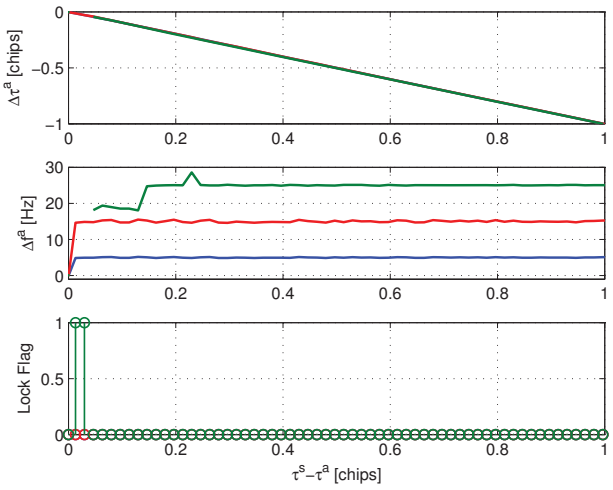

Fig. 8. Influence on the code delay and frequency estimations in the presence of a cloned signal.

previous experiment, the replica signal with 25Hz more, forces the receiver to lose the lock of the signal. The lock flag of the receiver, represented in the bottom subplot of Figure 8, alerts about this problem. After this issue, the receiver can lock the replica signal after some time. The fact that the receiver locks on the cloned signal and not on the authentic signal is related with the conclusions extracted in Section II-B. As the power of the cloned signal in the prompt correlator is greater than the power of the authentic signal, the receiver tends to follow its dynamics even if this implies that it has to re-lock the signal.

V. Mitigation reference techniques

Once we have analysed the impact of replica signals onto the receiver performance, the next step is to develop reliable mitigation techniques. In order to compare the effectiveness of these methods, it is useful to select a pair of simple reference techniques to be used as a benchmark. Since our objective is to use both signal level and navigation parameters, a reference technique from each level has been chosen. These procedures were not explicitly designed for detecting or mitigating cloned signal interferences but to check the health of the receiver measurements which, at the end, is the objective of a so-called integrity receiver. The handicap inherent in these techniques is that they will alert the receiver not only under cloned signal attacks but also under other circumstances such as multipath or system failures.

A. Signal level based technique

The signal level reference technique is the use of Signal Quality Monitoring (SQM) metrics such as the one used in [26]. This monitoring metrics have been proved to be useful in the detection of failures in the signal transmitted by the satellites. These errors directly affect the shape of the correlation peaks of the received signal. Thanks to the computation of the metric, any deformation in the correlation will be reflected in its value. In the case of a cloned signal, the interference between the legitimate and the cloned signal directly cause a deformation of the expected correlation function, resulting in a asymmetric correlation peak. This fact is better understood by analysing Figure 1 where the shape of the combined correlation peak is depicted. Therefore, the anomalies created by cloned signals will be detected by SQM. The first part of the method is to study the statistical behaviour of the selected metric. As a result, the variability of the parameter is obtained. Then, a detection problem can be formulated using the expected behaviour of the metric. The hypothesis $\mathcal{H}_0$ will represent the absence of replica signal that will occur under a threshold m_{th} that ensures a certain probability p_0. Above this threshold, we can consider the hypothesis $\mathcal{H}_1$ representing the case in which the metric m is affected by an anomaly like cloned signals. This procedure was followed by the authors of [16] and [27] with successful results. However, both works highlight the difficulty in the discrimination of the results affected by multipath than those in the presence of cloned signals since the anomalies on the correlation peaks are similar.

B. Navigation level based technique

The navigation reference technique proposed to detect non-authentic signals consists on the assessment of the integrity of the signal measurements. Specifically, the use of Receiver Autonomous Integrity Monitoring (RAIM) [19] is currently being studied for that purpose. RAIM was designed in order to provide information about the integrity of the measurements that are used for the computation of the navigation solution. This is a important requirement in avionics receivers where, due to the high speed of the aircraft, it is extremely important to know whether the pseudorange estimations are correct or not and detect anomalies in the shortest interval possible. In addition, RAIM alerts the user in the case that one of the signals is corrupted and informs him about which is the satellite that is causing the errors. Consequently, by using RAIM it is possible to isolate the erroneous satellite from the navigation computation process. In order to check the consistency of the navigation measurements, RAIM uses a redundant navigation solution, which means that it requires the reception of 5 or more satellites. The output of the algorithm are the parameters of Horizontal Protection Level (HPL) and Vertical Protection Level (VPL) that specify the horizontal and vertical margins around the true position that ensure to contain the position of the user for a given cloned alarm probability. In the presence of a replica signal, the estimated pseudoranges can be corrupted and so the navigation solution. Therefore, we will use RAIM with the aim of detect erroneous measurements caused by the cloned signal. This algorithm has a probed reputation detecting punctual failures on specific measurements. However, the results may be not be completely successful if multiple signals fail at the same time, for instance, because of the reception of cloned signals over different navigation signals.

VI. Conclusions

A preliminary evaluation of the effects of replica signal reception on GNSS receivers has been presented. The interaction between both the authentic and the replica signal have been studied focusing on how it affects the tracking stage of the receiver. From this study, we have tried to identify which are the replica signal parameters that have a more significant impact on the receiver measurements. As a way to assess the level of sensitivity of the receiver in cloned signal scenario, we have considered different configurations of each of these highlighted parameters. Specifically, one arbitrary case has been selected and its consequences on the receiver have been analysed. To do so, multiple software simulations have been carried out while real hardware equipment has been used to confirm the results.

For the future work, the procedure carried out in this paper will be use to elaborate a complete study of the GNSS receiver sensitivity against replica signals. Afterwards, the resulting study will allow us to develop highly reliable techniques to detect and mitigate the presence of these intentional interferences.

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] "Global positioning system standard positioning service performance standard," Department of Defense of the United States of America, Tech. Rep., 2008.

[3] M. Wildemeersch and J. Fortuny-Guasch, "Radio frequency interference impact assessment on global navigation satellite systems," JRC, Tech. Rep., 2010.

[4] A. Szumszki, "Finding the interference: Karunhen-loeve transform as an instrument to detect weak rf signals," *InsideGNSS*, vol. May/June, pp. 56–64, 2011.

[5] 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.

[6] 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.

[7] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks," in *ION GNSS Conference Nashville, TN, September 1921*, 2012.

[8] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Going up against time: The power grids vulnerability to gps spoofing attacks," *Timing*, vol. August, pp. 34–38, 2012.

[9] 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 Institute of Navigation*, 2005.

[10] 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.

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

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

[13] 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.

[14] 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 Institute of Navigation*, 2010.

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

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

[17] 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 Institute of Navigation*, 2009.

[18] J. Juang, "Gnss spoofing analysis by vias," *Coordinates Magazine*, vol. February to November, 2011.

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

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

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

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

[23] K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil gps signal authentication," *Journal of Navigation*, vol. 59, pp. 177–193, 2012.

[24] J. J. Spilker, *Global Positioning System: Theory and Applications, Volume 1*. American Institute of Aeronautics, 1996.

[25] O. Pozzobon, C. Sarto, A. D. Chiara, A. Pozzobon, and G. Gamba, "Status of signal authentication activities within the gnss authentication and user protection system simulator (gaupss) project," in *ION GNSS*, 2012.

[26] D. M. Akos, R. E. Phelts, S. Pullen, and P. Enge, "Signal quality monitoring: Test results," in *ION NTM 2000, 26-28 January 2000, Anaheim, CA*, 2000.

[27] K. D. Wesson, D. P. Shepard, J. A. Bhati, and T. E. Humphreys;, "An evaluation of the vestigial signal defense for civil gps anti-spoofing," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation*, 2011.