Signal-Level Integrity Monitoring Metric for Robust GNSS receivers

Juan M. Parro-Jimenez*(1,2), Jose A. Lopez-Salcedo†(2), Rigas T. Ioannides‡(1) and Massimo Crisci§(1)

(1) European Space Agency, Noordwijk, 2201AZ, The Netherlands

(2) Universitat Autonoma de Barcelona, Bellaterra, 08193, Spain

This paper deals with the problem of detecting distortions on the received signals of Global Navigation Satellite Systems (GNSS) that may degrade the measurements accuracy and compromise the overall receiver operation. Amongst others, multipath and spoofing are two of the most concerning threats for the robustness of GNSS receivers. These two phenomena have similar effects on the received signal, which can be exploited with the aim of developing a common defence mechanism. The detection process presented herein uses the fact that, in the presence of signal anomalies, the correlation function at the receiver side becomes distorted and loses its symmetry. An assessment on how severe is the effect of this distortion is presented herein. Besides, the proposed scheme is validated with the analysis of real signals simulated with an advanced hardware simulator.

I. Introduction

GNSS receivers are used in several applications as the main tool for positioning, navigation or timing. Many of them have strict requirements since they are involved in critical missions such as airplane landing, maritime or railway and road guidance. In those cases, the required response time in case of an alert must be as short as 2 seconds[1] or even shorter, depending on the criticality of the operation. In this context, the concept of integrity is defined as the level of trust that users can expect from the navigation information provided by the system. The need of this measure is becoming more and more important as the demand of reliable navigation in critical applications is also becoming of paramount importance in different economic sectors. Currently, there are different approaches to calculate the level of integrity such as the use of Ground or Satellite Based Augmentation Systems (GBAS and SBAS) or the implementation of Receiver Autonomous Integrity Monitoring (RAIM) techniques. However, other alternatives are necessary for standalone receivers where the need of low complexity techniques is a usual requirement. In this context, signal-level based techniques are a good solution for extracting the information present at the physical-layer where signal anomalies occur.

One of the phenomena that can degrade the quality of the navigation signals is the well-known multipath effect. It is caused by the reception of multiple reflections of the authentic signal coming from objects surrounding the user receiver. Multipath represents one of the major sources of error in GNSS introducing errors in the pseudorange and carrier phase measurements, which in turn produce errors in the computation of the Position, Velocity and Time (PVT) solution. Many methods to detect and mitigate multipath have been already proposed in the literature, the authors of[2] present a populated table with some off-the-shelf techniques.

The intrinsic characteristics of GNSS can also make them susceptible to interferences that corrupt the integrity of the user measurements. The received power signals are commonly 20 dB below the thermal noise floor[3] which make them easy to be masked by abnormal or unlicensed signals that may be present in the same band. Besides, the lack of authentication mechanisms on the current open GNSS services

*Juan.Parro@esa.int, TEC-ETN.

†Jose.Salcedo@uab.es, SPCOMNAV.

‡Rigas.Ioannides@esa.int, TEC-ETN.

§Massimo.Crisci@esa.int, TEC-ETN.

makes feasible the replication and transmission of GNSS signals by unauthorised users with the objective of misleading standard receivers with false measurements. This sort of attack, popularly known as spoofing, represents a major threat for the integrity of GNSS-based applications, which in turn can have serious security and economical implications. Some examples are aircraft landing operations, Road User Charging (RUC) systems,[4] fishing vessels guidance or GNSS based network synchronization.

In the presence of multipath or spoofing, the effects at the signal level share important similarities. Mainly, the two phenomena produce a distortion of the correlation peak between the received signal and the local replica. In the particular case of the GPS L1 C/A signal, the expected triangular shape at the correlation becomes no longer symmetric. This fact has been used by many techniques with the goal of detecting degradations in the signal such as evil waveforms,[5,6] multipath[7] and, more recently, spoofing.[8,9] These techniques have been shown to be useful for the early detection of faulty signals, although one of their main limitations is the difficulty in inferring what the source of the error is.[9] In[10] the authors proposed the use of a metric called Slope Asymmetry Metric (SAM) with the objective of detecting the presence of multipath in indoor scenarios based on exploiting the geometric properties of the correlation peak. However, since the effects of both multipath and spoofing over the resulting correlation are very similar, the SAM can be also used to detect spoofing. In this way, if a faulty signal is detected because the symmetry principle is not fulfilled, the user has the possibility to discard the satellite and avoid the propagation of errors in the measurements to the PVT solution. In this context, this paper presents the integrity monitoring capabilities of the SAM in the presence of both multipath or spoofing.

The paper is structured as follows: first a brief explanation is presented on how the integrity of the received signals is altered by multipath or spoofing. Later, the metric proposed by the authors in[10] for multipath detection in harsh scenarios is described and its detection capabilities are explored in the presence of multipath or spoofing. Finally, experimental simulations are presented to verify the correct performance of the metric.

II. Signal Model

Satellite navigation systems such as GPS are based on a direct-sequence spread spectrum (DS-SS) scheme. The modulation of the navigation data bits is carried out using orthogonal Pseudo-Random (PN) codes $c[k]$ which are a sequence of N_c chips with amplitudes $\{1, -1\}$. The orthogonality of the codes allows the receiver to discriminate between signals of different satellites by correlating the incoming signal with a local replica. The autocorrelation function of the code $c[k]$ at lag τ can be expressed as $R[\tau] = \sum_{k=0}^{N_{scp}-1} c[k]c^*[k-\tau]$, where N_{sc} represents the number of samples per code. Thus, for a given satellite, the output correlation in the presence of multipath and spoofing can be expressed, for the discrete-time baseband equivalent received signal, as:

$$z_n = \alpha_a R[\hat{\tau}_n - \tau_{a,n}] \exp\{j(\hat{\theta}_n - \theta_{a,n})\} + z_{\mathrm{mp},n} + z_{\mathrm{sp},n} + \eta_n \tag{1}$$

where α_a, $\tau_{a,n}$ and $\theta_{a,n}$ are the amplitude, the code delay and the phase of the received signal, $\hat{\tau}_n$ and $\hat{\theta}_n$ are the code delay and phase estimation of the receiver, $z_{\mathrm{mp},n}$ and $z_{\mathrm{sp},n}$ are the contributions of multipath and spoofing respectively and η_n is the correlated complex Gaussian noise component which has zero mean and variance σ_η^2.

From the model of (1) the multipath contribution can be expressed as a sum of $i = 1, ..., M$ replicas of the authentic signal with random amplitudes α_i caused by the reflection of the signal and delayed $\Delta\tau_i$ with respect to the authentic signal due to the longer path experienced by each replica. Note that the delays of each replica will always be larger than the delay of the authentic signal. The overall multipath component can be expressed as:

$$z_{\mathrm{mp},n} = \sum_{i=1}^{M} \alpha_i R[\hat{\tau}_n - \tau_{a,n} - \Delta\tau_{i,n}] \exp\{j(\hat{\theta}_n - \theta_{a,n} - \Delta\theta_{i,n})\} \tag{2}$$

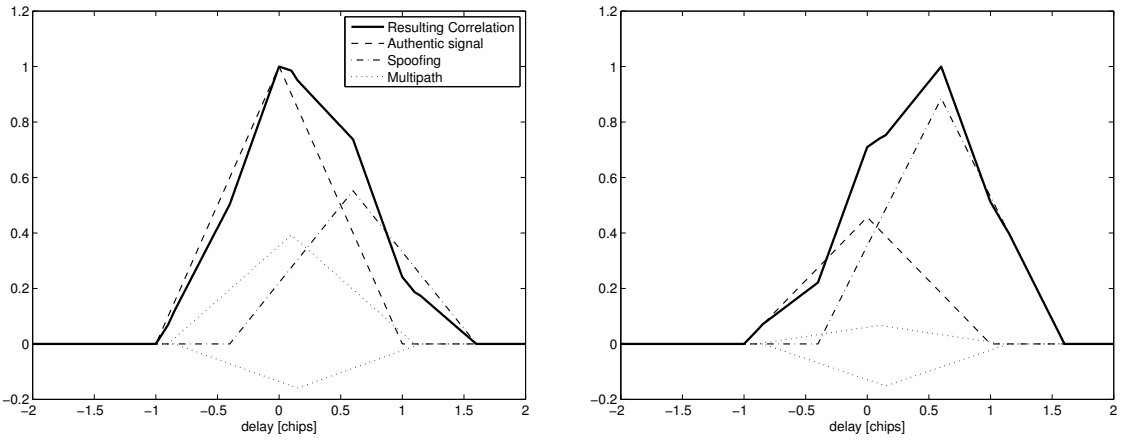
where $\Delta\theta_{i,n}$ denotes the relative phase of the i-th replica.

Regarding the contribution of spoofing to the resulting correlation, it has similar values to the authentic signal in terms of power and coherence with time. However, due to fact that it is likely to have different code delay and frequency than the authentic signal, the correlation of the spoofed signal presents the corresponding

code-delay $\Delta\tau_{\mathrm{sp}}$, phase $\Delta\theta_{\mathrm{sp},n}$ and frequency Δf_{sp} relative values:

$$z_{\mathrm{sp},n} = \alpha_{\mathrm{sp}} R[\hat{\tau}_n - \tau_{a,n} - \Delta\tau_{\mathrm{sp},n}] \exp\{j2\pi\Delta f_{\mathrm{sp}} n + j(\hat{\theta}_n - \theta_{\mathrm{a},n} - \Delta\theta_{\mathrm{sp},n})\} \tag{3}$$

Both the contributions of multipath and spoofing are very similar based on the models of (2) and (3). In the two cases, different replicas of the correlation function $R[\tau]$ are added to the authentic signal with a given Desired-to-Undesired power ratio defined as $D/U = \alpha_a^2/\alpha^2$, where α is the amplitude of the replica occasioned either by multipath or spoofing. As a result, the obtained signal has a different shape from the one obtained in a scenario without anomalies. Figure 1 shows two examples for the specific case with a GPS L1 C/A signal where the resulting correlation function is affected by multipath and spoofing. An infinite bandwidth has been assumed for the representation of the correlation. As can be seen, the authentic signal has the standard triangular shape while the result has been distorted. From this result we can conclude that the lack of symmetry in the resulting correlation function is, by itself, a way to measure the level of degradation present in the received signal. The following section will explore what is the behaviour of the metric SAM in the presence of multipath and spoofing and how it can be used to detect the degradation on the signal.



(a) (b)

Figure 1: Degradation of the resulting correlation peak due the presence of multipath and spoofing.

III. Slope Asymmetry Metric (SAM)

The proposed integrity monitoring metric consists on comparing the left and right slopes of the received signal correlation peak. Ideally, both slopes should be equal but with opposite sign, and thus their sum should be theoretically equal to zero. The first step for calculating this metric consists on the approximation of each side of the correlation peak by a straight line. To do so, three correlator outputs from each side are calculated at delays ± 0.25 chips, ± 0.5 chips and ± 0.75 chips obtaining the vectors $\mathbf{z}_l$ (left slope) and $\mathbf{z}_r$ (right slope) which contain the squared magnitudes of the correlators. For each side, we find the least-squares estimate of the straight line that best fits the set of three correlators next to the prompt correlator, which is not taken into account on this estimation. The slope $\hat{a}$ and the vertical offset $\hat{b}$ estimates of each line are obtained as:

$$[\hat{a}, \hat{b}]^T = \mathbf{M}^{\#}\mathbf{z} \tag{4}$$

where $\mathbf{M}^{\#}$ represents the Moore-Penrose inverse of matrix $\mathbf{M} = \begin{pmatrix} -T_s & 0 & T_s \\ 1 & 1 & 1 \end{pmatrix}^T$ being T_s the time spacing between the correlation values of vector $\mathbf{z}$. As a result, we obtain the estimates of the slopes for the left ($\hat{a}_l$) and right ($\hat{a}_r$) line. With them, it is possible to calculate the SAM as:

$$\mathrm{SAM} \doteq \hat{a}_l + \hat{a}_r \tag{5}$$

Note that, if any misalignment is produced in the peak the metric will present a mean value μ_{SAM} different from zero. This effect will be used to detect any possible degradation that multipath or spoofing can cause to the navigation signals.

A. SAM envelope

As said before, in a perfectly clean scenario the correlation peak preserves its symmetry, and thus the estimates of the slopes have the same magnitude. As a result, the obtained SAM has a mean value μ_{SAM} equal to zero. However, in the presence of any anomaly such as multipath o spoofing, the presence of replicas of the satellite signal create a distortion on the symmetry of the correlation peak which introduces a non-zero mean value of the SAM μ_{SAM}.

In order to simply the evaluation of the effects of both spoofing and multipath on the metric, we can consider that both phenomena can be approximated by the sum of a single correlation peak with a given amplitude, code delay and phase relative to the authentic signal. Thus, resulting in

$$z_{\text{simp},n} = \alpha_a R[\hat{\tau}_n - \tau_{a,n}] \exp\{j(\hat{\theta}_n - \theta_{a,n})\} + \alpha R[\hat{\tau}_n - \tau_{a,n} - \Delta\tau_n] \exp\{j(\hat{\theta}_n - \theta_{a,n} - \Delta\theta_n)\} + \eta_n. \tag{6}$$

Based on this model we can assess how the value μ_{SAM} evolves for different configurations of the signal replica, giving us an insight of the SAM detection capabilities for integrity monitoring. Figure 2 shows the evolution of μ_{SAM} for the cases of $D/U = \{10, 6\}$ dB and $\Delta\theta = \{0, \pi\}$ rad. This analysis is similar to the multipath envelopes which are used to evaluate the impact of a multipath replica on the estimated time delay. For the case of the SAM, also the in-phase and counter-phase represent the extreme error cases for a given relative delay, and thus, they are taken as a reference. In our analysis, the four cases of study have been tested for relative code delays between -2 and 2 chips. Note that time advanced code delays are taken into account for the specific case of spoofing since the replica can be placed anywhere relative to the authentic signal, unlike the case of multipath. From the results of the SAM envelope in Figure 2 some conclusions can be extracted such as the fact that the value of μ_{SAM} increases with the power of the signal replica. As can be seen, the envelopes for the case of $D/U = 6$ dB produce larger values than in the case of $D/U = 10$ dB. It is also interesting that those cases in which the relative phase is equal to π present larger magnitude errors than in the in-phase case. This effect is caused by the fact that a counter-phase signal produces a larger deformation on the correlation than in the in-phase case, hence, the slope estimates have magnitudes that are more distinct. From Figure 2 we can also see that for some relative delays the resulting μ_{SAM} is equal to zero. In this cases, the occasioned bias in the two slopes is the same and thus, the resulting SAM has a mean equal to zero. Note that this effect is occasioned because the simplified model of one signal replica is used. In the case of multipath it is expected to have several replicas which will make unlikely that $\mu_{\text{SAM}} = 0$. In the case of spoofing, since the relative phase between the satellite signal and the replica is changing continuously, the resulting μ_{SAM} will vary between the in-phase and the counter-phase envelope.

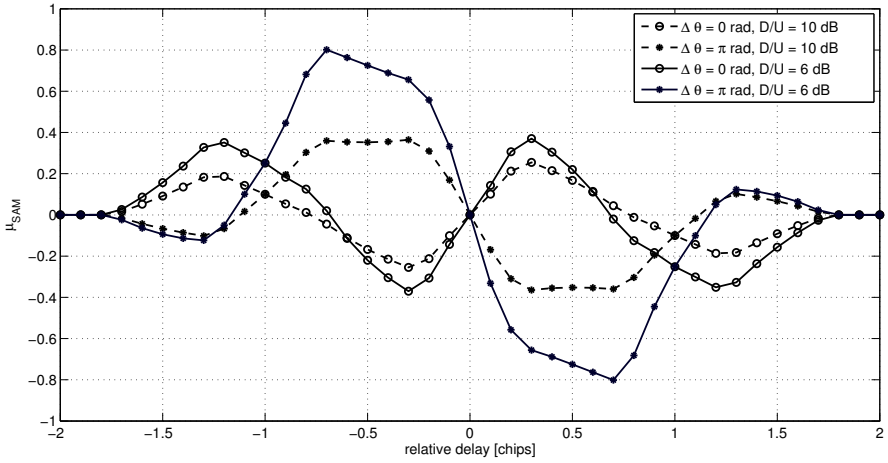


Figure 2: Evolution of the mean value of the metric SAM for different relative delays of the replica.

B. ROC performance

We can define a binary hypothesis test in order to decide whether the symmetry of the correlation peak is preserved or not based on the behaviour of the SAM shown in the previous section. In this way, we can distinguish between two conditions of the SAM: the null hypothesis ($\mathcal{H}_0$) which represents the absence of any distortion on the signal and thus, $\mu_{\text{SAM}} = 0$, and the alternative hypothesis ($\mathcal{H}_1$) reflecting the case in which the mean value of the slopes is different from zero and thus, $\mu\text{SAM} \neq 0$.

In order to assess the performance of the detection scheme two parameters are commonly defined. First the probability of false alarm P_{fa} is defined as the probability that under the absence of anomalies the detector indicates the hypothesis $\mathcal{H}_1$. On the other hand, the probability of detection P_d is the probability that we decide that the anomaly is present, i.e. hypothesis $\mathcal{H}_1$, when it is indeed present.

The Receiver Operating Characteristics (ROC) of a given detector illustrates its behaviour in terms of P_{fa} and P_d. ROC curves can be calculated empirically carrying out Monte Carlo simulations.[11] Figure 3 illustrates the ROC performance of the SAM for the cases of an in-phase (left) and counter-phase (right) replica with a $D/U = 10$ dB at different relative delays when the C/N_0 of the authentic signal is 46 dB-Hz. Again, the in-phase and counter-phase cases are chosen for the analysis since they represent the extreme SAM errors for a given relative delay. As can be seen, the performance of the detector improves in the two cases as the relative delay between the two signals increases. Note that this closely related with the results of Figure 2. The deformation of the SAM is reduced to zero with the relative delay. In other words, the closer the signal replica is to the authentic, the lower the deformation on the shape of the resulting signal. This means that it will be more difficult to detect multipath or spoofing whose replicas are close to the main peak than those that are far from it. Another interesting result comes when the effect of the relative phase between signals is analysed. According to the ROC curves, the performance of the detector is better if the signals are π rad apart. Again, as was shown in Figure 2, it is demonstrated that the distortion entailed by a counter-phase signal is greater than the occasioned by a in-phase replica, which makes more easy to identify the degradation on the integrity of the signal.

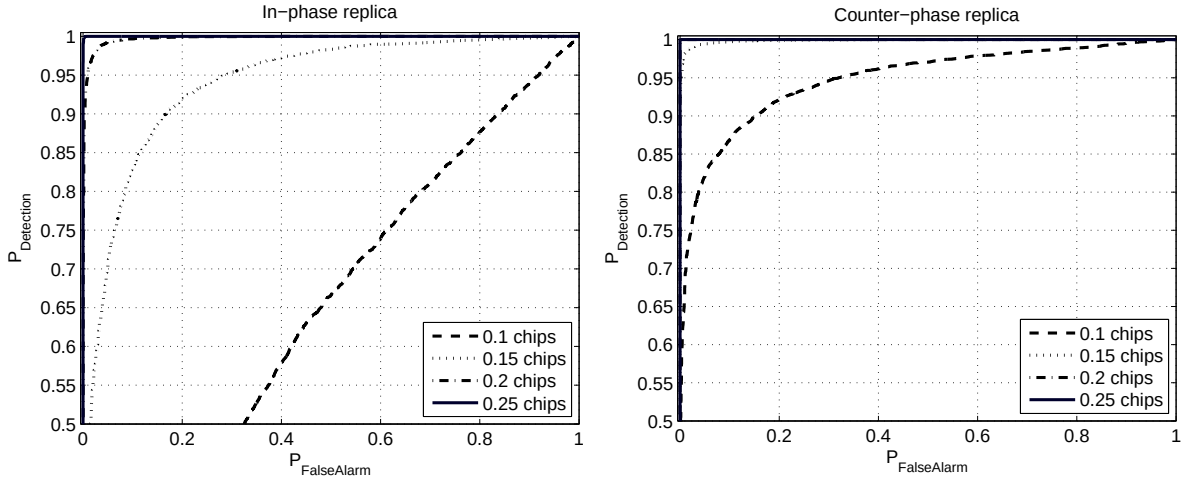


Figure 3: ROC performance of the detector for the specific cases of in-phase signals (a) and counter-phase signals (b) for different relative code delays.

IV. Experimental Results

In order to evaluate the performance of the integrity monitoring metric, real GNSS signals have been generated using an advanced hardware simulator. This device allows complete flexibility in the definition of the scenario to be simulated and provides full control on the generated signals. The simulator is not only used to generate the authentic signals but also to recreate the presence of multipath replicas or to emulate the reception of a spoofing signal. The transmitted signals are digitized using 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.

The metric will be evaluated in three different experiments. In Experiment #1 a multipath environment is tested. Experiments #2 and #3 are scenarios where a spoofing signal is present with different initial code delays in each case. For the detection of the anomaly in all the three experiments a conservative assumption is considered, assuming that a signal replica is present with a $D/U = 10$ dB, $\Delta\tau = 0.2$ chips and a relative phase of $\Delta\theta = 0$ rad, which causes the smaller degradation on the SAM. Two thresholds that provide a P_d of 0.95 and 0.85 in this scenario are chosen. In the three scenarios a level of $C/N_0 = 46$ dB-Hz is selected for the authentic signal and a sampling frequency of 10 MHz is used. The correlator values z_n are accumulated during an interval of $T_{acc} = 10$ ms.

A. Experiment #1

For the simulation of the multipath environment we selected the model presented in[12] that gives the possibility to simulate different types of channel (open, rural, suburban, urban and highway). It distinguishes between two types of reflections, near to the authentic signal or far from it. The number of near replicas present in such channel N_n follows a Poisson distribution:

$$P_{Poisson}(N_n) = \frac{\lambda^M}{N_n!}\exp\{-\lambda\}, \tag{7}$$

while the delay of each replica is exponentially distributed:

$$P_{exp}(\tau) = \frac{1}{b}\exp\{\frac{-\tau}{b}\} \tag{8}$$

and the power profile of these echos has an exponential decrease given by:

$$S(\tau) = S_0\exp\{-d\tau\}. \tag{9}$$

Regarding the far echos, its number $M - N_n$ is also Poisson distributed while the delays are uniformly distributed between τ_e and $\tau_{\max}$. Their mean power values are attenuated between -20 and -30 dB with respect to the authentic signal.

For the scenario of experiment #1 we have selected an urban environment which can be simulated using the parameters presented in Table 1. In our experiment we will consider that the Line-of-Sight (LOS) signal

Parameter	Value
λ	3.5
τ	0.069 μs
S_0	-23 dB
d	6.5 dB
τ_e	0.6 chips

Table 1: Parameters of Experiment #1.

is always present with a $C/N_0 = 46$ dB-Hz, and thus no shadowing effect is experienced.

Figure 4 shows the SAM evolution with time in the simulated scenario together with the selected thresholds of $P_d = 0.95$ and $P_d = 0.85$, which are illustrated as different horizontal lines. The receiver is working during the firsts 50 seconds in a multipath-free scenario. As a result, the initial SAM values are bounded inside the the more relaxed threshold of $P_d = 0.85$. After the initial period the channel is affected by multipath and, as can be seen, the values of the metric indicate that there is a distortion that corrupts the integrity of the signal. The mean value of the SAM measurements is no longer equal to zero due to the presence of the multipath replicas. In addition, the variability of the metrics changes motivated by the randomness of the multipath components. Note that, even though the replicas present in the scenario are highly attenuated, the metric is able to show their effect on the shape of the correlation function.

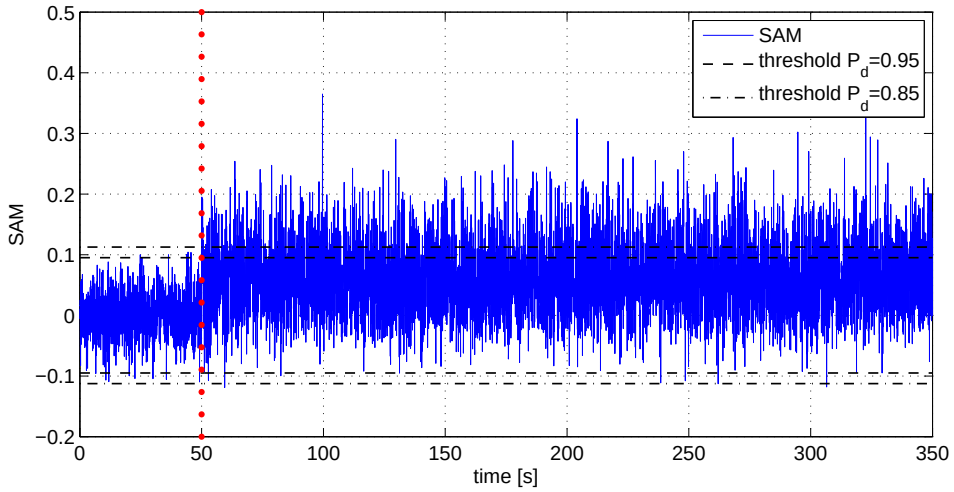


Figure 4: Evolution of the SAM in the scenario of Experiment #1.

B. Experiment #2

The objective of this experiment is to test the performance of the metric in the presence of spoofing. In this scenario, the replica approaches the main peak in a linear way from an initial code delay of $\Delta\tau_{\text{sp},0} = -1$ chip having greater power. The parameters of the scenario are summarized in Table 2.

Parameter	Value
C/N_0	46 dB-Hz
D/U	-3 dB
Δf_{sp}	-5 Hz
$\Delta\tau_{\text{sp},0}$	-1 chip

Table 2: Parameters of Experiment #2.

Figure 5 illustrates the evolution of the SAM during the experiment. As can be observed, the fact that the replica starts far from the main peak induces large errors in the slope estimates, as can be seen in the steep jump experienced at time 50 sec. As the simulation time advances, the SAM values obtained gradually become smaller since the two signals are aligning their code delays, and thus, the aggregate correlation peak becomes less distorted. This effect is clearly shown after 360 seconds where the spoofing signal has the same code delay than the authentic signal, i.e. $\Delta\tau_{\text{sp}} = 0$, and the metric is again beneath the detection threshold.

This experiment represents a realistic spoofing case in which the transmitter of the spoofing signal does not know the code delay of the authentic with accuracy. Then, the solution is to sweep the spoofing signal for a range of delays trying to capture the tracking loops of the receiver. Under this situation, it is easy for the integrity metric to detect the anomaly even before it affects the measurements thanks to the use of multiple correlators combined at each slope. In this sense, the use of multiple correlators to estimate each of the slopes provides an advantage to the SAM since it creates a protection region for the signal. If a spoofing signal approaches to the authentic one, from outside the main peak, monitoring the SAM will alert the user that the integrity of the signal can be corrupted.

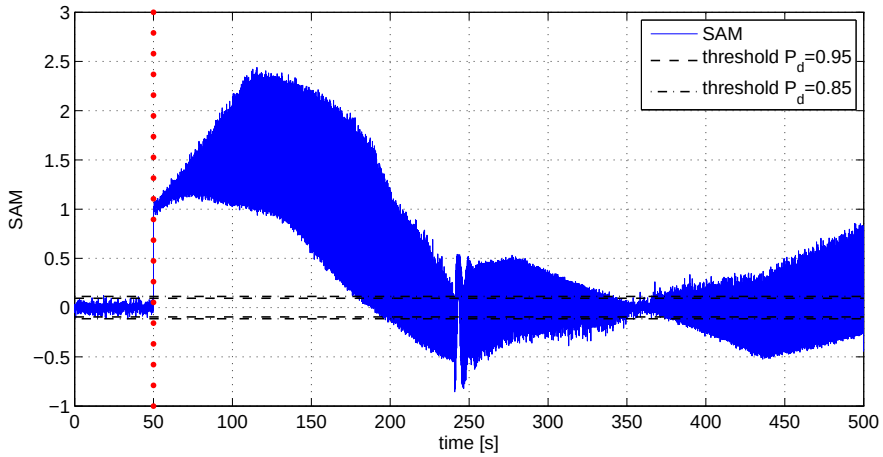


Figure 5: Evolution of the SAM in the scenario of Experiment #2.

C. Experiment #3

In this experiment we are interested in studying the effects of a spoofing signal that is initially aligned with the authentic signal ($\Delta\tau_{\text{sp},0} = 0$) and, after an initial period, it increases its relative code delay. As said before, in order to carry out this spoofing type the transmitter of the replica needs an accurate estimate of the receiver code delay which, amongst other parameters, requires an estimation of the receiver position with centimetre accuracy. The parameters of the scenario are summarized in table 3.

Parameter	Value
C/N_0	46 dB-Hz
D/U	-3 dB
Δf_{sp}	-5 Hz
$\Delta\tau_{\text{sp},0}$	0 chips

Table 3: Parameters of Experiment #3.

Figure 6 shows the evolution of the metric SAM for the first 255 seconds of the simulation. The spoofing signal starts its movement after 50 seconds. As was expected, the SAM values obtained when the spoofing signal is close to the authentic do not reflect the presence of the interference since the symmetry of the resulting peak is only slightly degraded. As soon as the spoofing signal advances, the shape of the peak is distorted more and more which is clearly identified by the metric.

As the authors of[9] pointed, the only way the spoofer has to avoid the degradation of the resulting correlation peak is by transmitting two spoofing signals. The objective of the first replica is to eliminate the presence of the authentic signal. To do so, it is transmitted with the same amplitude than the authentic but in counter-phase, which eliminates the authentic signal. The second spoofing signal is the one that the attacker uses to mislead the receiver measurements without affecting the shape of the correlation function as there is no interaction with any other signal. This scenario can be simulated in the laboratory where both transmitter, spoofer and receiver are synchronized. Figure 7 shows the results of this experiment. Figure 7a monitors the SAM of the signal which does not overpass the detection threshold because the authentic signal is correctly removed after 50 seconds using a counter-phased replica. At that instant, the receiver is tracking the second spoofing signal which has different frequency and code delay as is shown in Figure 7b.

Despite the effectiveness of this attack, the elimination of the real signal requires a high accurate knowledge of the position, movement and velocity of the user, which makes this kind of attack highly unlikely. Even in the case the attacker has access to the receiver, which provides him a perfect knowledge of the receiver conditions, it would need a highly accurate estimate of its processing delay.[9]

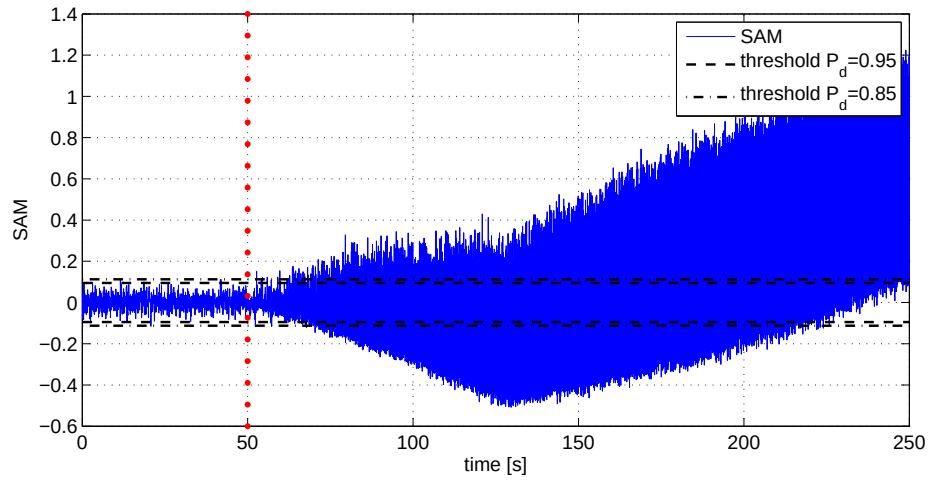
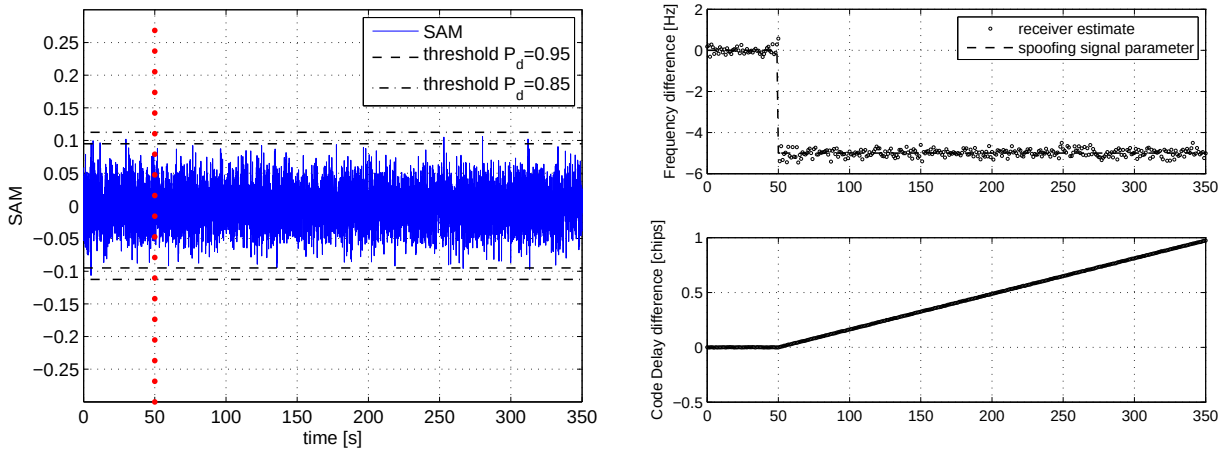


Figure 6: Evolution of the SAM in the scenario of Experiment #3.



(a) SAM

(b) Receiver estimates

Figure 7: Evolution of the SAM and the receiver estimates in a scenario where the authentic signal has been removed by transmitting an aligned counter-phase signal and the same amplitude.

V. Conclusion

A metric for the monitoring of the integrity of GNSS signals at the signal-level is presented. It exploits the fact that a healthy signal maintains the symmetry of the correlation peak, a property that is not fulfilled when an anomaly is present in the received signal, such as multipath or spoofing. In those situations, the value of the metric reflects that there is misalignment between the estimates of the slopes of the correlation peak. This effect has been first studied for different configurations of multipath and spoofing taking into account that both phenomena have a similar effect on the final correlation of the signal. This initial study has been confirmed later on with experimental simulations carried out in a controlled laboratory environment with an advanced hardware simulator and SDR equipment to analyse the results. The proposed metric has been proved to successfully alert the user about the degradation of the signal under realistic multipath and spoofing scenarios.

Acknowledgements

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

References

[1]Gleason, S. and Gebre-Egziabher, D., *GNSS Applications and Methods*, GNSS technology and applications series, Artech House, Incorporated, 2009.

[2]Dragunas, K. and Borre, K., "Multipath Mitigation Based on Deconvolution," *Journal of Global Positioning Systems*, 2011.

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

[4]Feng, S., Ochieng, W., and North, R., "Quantitative Measures for GPS Based Road User Charging," *11th International IEEE Conference on Intelligent Transportation Systems, 2008. ITSC 2008.*, 2008, pp. 495–500.

[5]Akos, D. M., Phelts, R. E., Pullen, S., and Enge, P., "Signal Quality Monitoring: Test Results," *ION NTM 2000, 26-28 January 2000, Anaheim, CA*, 2000.

[6]Phelts, R., Akos, D., and Enge, P., "Robust Signal Quality Monitoring and Detection of Evil Waveforms," *Proceedings of ION GPS-99, the 12th International Technical Meeting of the Satellite Division of The Institute of Navigation*, 1999.

[7]Irsigler, M., *Multipath Propagation, Mitigation and Monitoring in the Light of Galileo and the Modernized GPS*, Ph.D. thesis, Bundeswehr University Munich, 2008.

[8]Pini, M., Fantino, M., Cavaleri, A., Ugazio, S., and Presti, L. L., "Signal Quality Monitoring Applied to Spoofing Detection," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011). September 20 - 23, 2011.Oregon Convention Center, Portland, Oregon. Portland, OR.*, 2011.

[9]Wesson, K. D., Shepard, D. P., Bhati, J. A., and Humphreys;, T. E., "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation*, 2011.

[10]Lopez-Salcedo, J. A., Parro-Jimenez, J. M., and Seco-Granados, G., "Multipath detection metrics and attenuation analysis using a GPS snapshot receiver in harsh environments," *3rd European Conference on Antennas and Propagation, 2009. EuCAP 2009.*, march 2009, pp. 3692 –3696.

[11]Fawcett, T., "An introduction to ROC analysis," *Pattern Recogn. Lett.*, Vol. 27, No. 8, June 2006, pp. 861–874.

[12]Jahn, A., Bischl, H., and Heiss, G., "Channel characterisation for spread spectrum satellite communications," *IEEE 4th International Symposium on Spread Spectrum Techniques and Applications Proceedings, 1996.*, Vol. 3, 1996, pp. 1221–1226 vol.3.