Post-correlation Signal Analysis to Detect Spoofing Attacks in GNSS Receivers

Emanuela Falletti and Beatrice Motella and Micaela Troglia Gamba
Navigation Technologies Area, Istituto Superiore Mario Boella, Torino, Italy
Email: {falletti, motella, trogliagamba}@ismb.it

Abstract—**Due to the low level of the received power and to the known signal structure, Global Navigation Satellite Systems (GNSS) civil signals might be vulnerable to different sources of interference. Among them, the spoofing attacks are considered ones of the most deceptive, since their scope is controlling the output of the victim receiver.**

This paper presents a set of live experiments that validate the performance of a spoofing detection method, based on the Chi-square Goodness of Fit (GoF) test and applied post-correlation. Results are promising and show the GoF test capability to successfully warn the user in case of a spoofing attack.

I. Introduction

The key element of any Global Navigation Satellite System (GNSS) receiver is the fine estimation of the satellite-to-receiver signal delay, a parameter that is strictly related to pseudorange measurement, and consequently to the position information estimation. The code delay estimation is generally implemented at the tracking stage, by the Delay Lock Loop (DLL), whose main task is aligning the local code replicas to the code sequences received from the satellites [1]. The DLL uses a set of correlators, in order to estimate the code delay error and correct the previous estimate, maintaining the signal tracked. In general the correlator output can be affected and distorted by several factors, some of them due to the surrounding environment, as the presence of multipath or interfering signals.

The general term of *interference* refers to any electromagnetic source able to interact with the GNSS signals [2]. More specifically, *jamming* is the deliberate in-band emission of unstructure signals to disrupt the system operations, while the term *spoofing* refers to the transmission of GNSS-like signals, with the intent to produce false information in the victim receiver. For this reason spoofing may be deceptive and sinister.

Currently, GNSS systems are used in an extremely wide set of different applications and some of them have strong requirements not only in terms of accuracy, but also in those of reliability. For this reason, many common and emerging applications might need GNSS receivers featuring detection capabilities for interference and spoofing attacks.

As detailed in [3], Signal Quality Monitoring (SQM) techniques, previously employed to monitor the correlation peak quality in multipath environment, have been extended to detect spoofing attacks on GNSS receivers [4], [5]. In fact, the presence of spoofing signals can affect the correlators output in a way similar to that of multipath components. Different types of spoofing detection algorithms, based on the monitoring of the signal correlation shape, have been presented in recent literature. This paper deals with a method based on a statistical testing, namely the Chi-square Goodness of Fit (GoF) test, able to take the decision about possible correlation distortions from the nominal conditions.

GoF tests have been already proposed for GNSS SQM in the literature, either directly applied on the receiver signal (i.e., on the signal samples at the output of the Analog-to-Digital Coverter, ADC) [6]–[8], or on the single receiver channel (i.e., on the correlators outputs) [9], [10]. In this latter case, the receiver is able to raise a warning, taking into account the actual effect of the distortion source after the despreading process. In this paper we present the results of a set of live experiments in which the Chi-square GoF test is applied at the correlators output of a real-time software receiver with the purpose of detecting the presence of a spoofing attack.

After this Introduction, section II describes the mathematical model of the signal along the receiving chain up to the correlators outputs. The Chi-square GoF test is introduced in section III and its use as spoofing detector is discussed. Section IV describes the tests cases, while section V presents the results of the signal processing. The conclusions of the work are summarized in section VI.

II. Signal Model

In a GNSS receiver, signal correlation is the fundamental operation to control the alignment of the local signal replicas with the received satellite signals. Such correlation is implemented as the multiplication of the received signal, down-converted to an intermediate frequency (IF), with a local replica of the IF carrier and of the spreading code sequence, both aligned in frequency and phase with the incoming code sequence. The mixed signal is then integrated along fixed time intervals (integration time, T) to produce the observable metrics necessary to iteratively adjust the alignment of the local signals (integrate and dump, I&D). The result of this I&D operation for each receiver channel can be written as

$$\begin{aligned} y_c\left(iT;\Delta\tau\right) = &\sqrt{2P_A}\,D\left(iT-\tau\right)\,R_{\tilde{c}}\left(\Delta\tau\right) \\ &\cdot\cos\left(2\pi\Delta f_d\,iT+\varphi\right)+w_c\left(iT\right) \end{aligned} \tag{1}$$

where $\sqrt{2P_A}$ is an amplitude factor related to the power of the received signal, $D(t)$ is the navigation message, $R_{\tilde{c}}(\tau)$ is the cross-correlation function of the local code sequence with

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

the incoming one. It might be possibly distorted by multiple correlated replicas (multipath, or even induced fake signals) and limited front-end bandwidth. $\Delta\tau$ is the current code delay estimation error, Δf_d is the current carrier estimation error and $w_c(t)$ is the additive noise component, which also includes the residual code cross-correlation from other GNSS signals. Noise samples $w_c(iT)$ are uncorrelated in time and Gaussian.

The DLL typically works by comparing the value of two I&D samples, taken at the same time instant iT but misaligned of a fraction of chip duration, $d_s/2$, with respect to the current code delay estimate: a so-called 'Early replica' $y_c^{(E)}(iT) = y_c(iT; \Delta\tau + d_s/2)$ and a 'Late replica' $y_c^{(L)}(iT) = y_c(iT; \Delta\tau - d_s/2)$. For $d_s > 0.2$ chips, the rounding-off effect of the front-end filter is typically negligible on $R_{\tilde{c}}(\Delta\tau \pm d_s/2)$, while for $d_s > 1$ the noise samples $w_c(iT; +d_s/2)$ and $w_c(iT; -d_s/2)$ are uncorrelated. Thus, in case of perfect alignment of the local signal and $d_s > 1$,

$$y_c^{(E)}(iT) = \sqrt{2P_A}\, D_i\, R_{\tilde{c}}(+d_s/2) + w_c(iT; d_s/2) \tag{2}$$

$$y_c^{(L)}(iT) = \sqrt{2P_A}\, D_i\, R_{\tilde{c}}(-d_s/2) + w_c(iT; -d_s/2) \tag{3}$$

where $D_i = D(iT)$ and the noise components are independent zero-mean Gaussian samples with variance σ_w^2. In the absence of signal distortions, $R_{\tilde{c}}(\tau) = R_c(\tau) = R_c(-\tau)$ is the theoretical code auto-correlation function symmetric with respet to $\tau = 0$. As a consequence, the difference $Y_i = y_c^{(E)}(iT) - y_c^{(L)}(iT)$ is a zero-mean random variable Gaussianly distributed with variance $\sigma_Y^2 = 2\sigma_w^2$. More in general, if a slightly delayed replica of the true satellite signal impinges the receiver antenna because of a signal reflection or a counterfeit signal, then

$$R_{\tilde{c}}(\tau) = R_c(\tau) + aR_c(\tau - \theta) \tag{4}$$

where a is the amplitude coefficient of the signal replica with respect to the true one and θ is the relative delay.

Although the case $d_s < 1$ is typically preferred for code delay tracking for its anti-multipath performance [1], the case $d_s > 1$ produces the independent observables where an hypothesis test can be built, to assess the possible presence of a signal distortion on the autocorrelation function.

In our implementation, two pairs of Early and Late code replicas have been employed. The former $(E - L)$, spaced of $d_s < 1$ has been used for the signal tracking loop, and the latter $(E\prime - L\prime)$, spaced of $d_s\prime > d_s$, for the hypothesis testing, as detailed in the following section.

III. Hypothesis test

Since we expect that, in the absence of signal distortion, the metric Y_i defined above is Gaussian with zero mean and variance σ_Y^2, the collection of a certain number n of observables Y_i, $\forall\, i = s, s+1, \ldots, s+n-1$ can be used to test the nature of the distribution of Y_i using a Chi-square GoF test. It is well known that such test allows verifying whether the distribution of the observations $\mathbf{Y} = \{Y_i\}_{i=s}^{s+n-1}$ is consistent with an hypothesized distribution or not [11], [12]. The method consists in identifying a finite number k of *categories*, or bins, in which the nominal distribution of the random variable Y_i can be sampled, then counting the number of observed occurrences in $\mathbf{Y}$ for each category. Denoting with O_r the observed number of samples in $\mathbf{Y}$ belonging to the r-th category (for each $r = 1, 2, \ldots k$), and with E_r the expected number of cases given n and the nominal distribution, the Chi-square test statistic is computed as

$$t_\chi = \sum_{r=1}^{k} \frac{(O_r - E_r)^2}{E_r} \tag{5}$$

where the random variable t_χ has asymptotically a χ^2 distribution with $(k-1)$ degrees of freedom. If the code correlation function in (2)-(3) has actually the non-distorted form $R_{\tilde{c}}(\tau) = R_c(\tau)$ (i.e., $a = 0$ in (4)), then the distribution of the metrics $\mathbf{Y}$ well matches with the expected one, the distribution of the test statistic is central and t_χ assumes a small value. On the other case, i.e., if an unexpected signal waveform distorts the code auto-correlation function so that $R_{\tilde{c}}(d_s\prime/2) \neq R_{\tilde{c}}(-d_s\prime/2)$, then the sample distribution results different than the expected one, the distribution of the test statistic is non-central and the value of t_χ increases. Notice that the expected number of cases for each category can be either computed from the theoretical nominal distribution or measured from a representative set of observables taken in a nominal undistorted situation ('calibration' of the method), in order to relax the hypothesis of the knowledge of the theoretical distribution. An example of nominal and distorted distributions, obtained with the live data sets described in section IV, is shown in Fig. 1.

In this way, a binary hypothesis testing is built on top this test statistic. The null and alternative hypotheses for t_χ can be stated as [11]

H_0 : the actual and expected distributions match
H_1 : the actual and expected distributions do not match

and the test statistic indicates which one of the two hypotheses can be accepted, i.e,

$$t_\chi \geq t_\alpha \Rightarrow\ H_0 \text{ not accepted} \tag{6}$$

$$t_\chi < t_\alpha \Rightarrow\ H_0 \text{ accepted} \tag{7}$$

where t_α is called *critical value* and represents the value of the test statistic corresponding to a probability α that the actual and expected distribution differ when the null hypothesis is true. α is known as the *significance level* of the test, and represents the area of the right tail of a nominal central Chi-square distribution with $(k-1)$ degrees of freedom, i.e., the probability that $t_\chi > t_\alpha$ under the hypothesis H_0. Then α also represents the 'false alarm' probability for the detection method.

Given the value of t_χ computed for the current observables $\mathbf{Y}$, the so-called *p-value* p is defined as the probability that the true test statistic for the actual distribution is greater than the computed value t_χ under the hypothesis H_0. Being p monotonically decreasing with t_χ increasing, the hypothesis

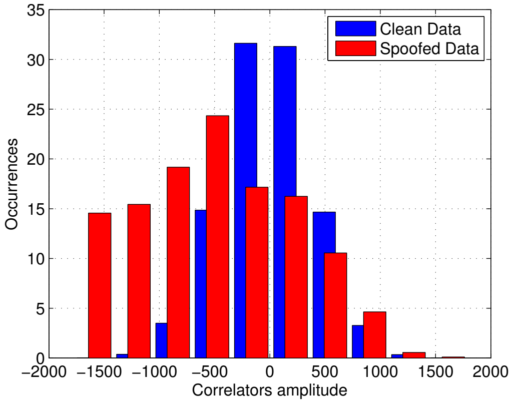


Fig. 1. Histogram of clean and spoofed data.

TABLE I
CHARACTERISTICS OF THE TESTS AND FRONT-END CONFIGURATION.

Test setup		
	Experiment A	Experiment B
User	static	dynamic
True constellation	GPS + Galileo	GPS + Galileo
False constellation	GPS + Galileo	GPS (partial)
GNSS bands	L1/E1	L1/E1
Spoofing-genuine signals power ratio (dB)	0.5	0.5
Front-end configuration		
Sampling frequency	8.192 MHz	
Down-conversion	Baseband	

test (6)-(7) can be rewritten as

$$p \leq \alpha \Rightarrow \; H_0 \text{ not accepted} \tag{8}$$

$$p > \alpha \Rightarrow \; H_0 \text{ accepted} \tag{9}$$

In what follows we show the application of this test to detect the appearance of a spoofing signal at the receiver. The nominal distribution of the observables across $k = 10$ categories is obtained from a calibration phase executed on a portion of clean signal, while the significance level of the test is set as $\alpha = 0.05$. The calibration phase allows the definition of the expected distribution E_r, from which the test statistic (5) can be measured during normal operations, as well as the corresponding p-value [13].

IV. Description of the Tests Cases

The detection method described in section III has been already validated by the authors against both recorded and simulated datasets of jamming and spoofing scenarios [8]–[10]. However, the importance of testing the method also through live experiments is unquestionable. In fact, in this way, it is possible to directly verify the behavior of the GNSS receiver equipped with anti-spoofing capabilities.

For this purpose, a test campaign was hosted by the Joint Research Centre (JRC) of the European Commission, that made available the anechoic room of the laboratories in Ispra, Italy. A real-time dual-constellation GPS/Galileo Software Defined Radio (SDR) receiver, namely the NGene receiver [14], has been equipped with a GoF-based distortion detection module, used to test the capability of recognizing certain types of spoofing attacks. NGene is a mixed assembly/C-language, PC-based receiver which elaborates samples from both Universal Serial Bus (USB) front-ends and files [15]. The choice of using an SDR receiver guarantees the high level of flexibility needed to test the proposed technique, that works with the output of two additional correlators per channel, spaced of $d_{s'}$ fractions of chip apart.

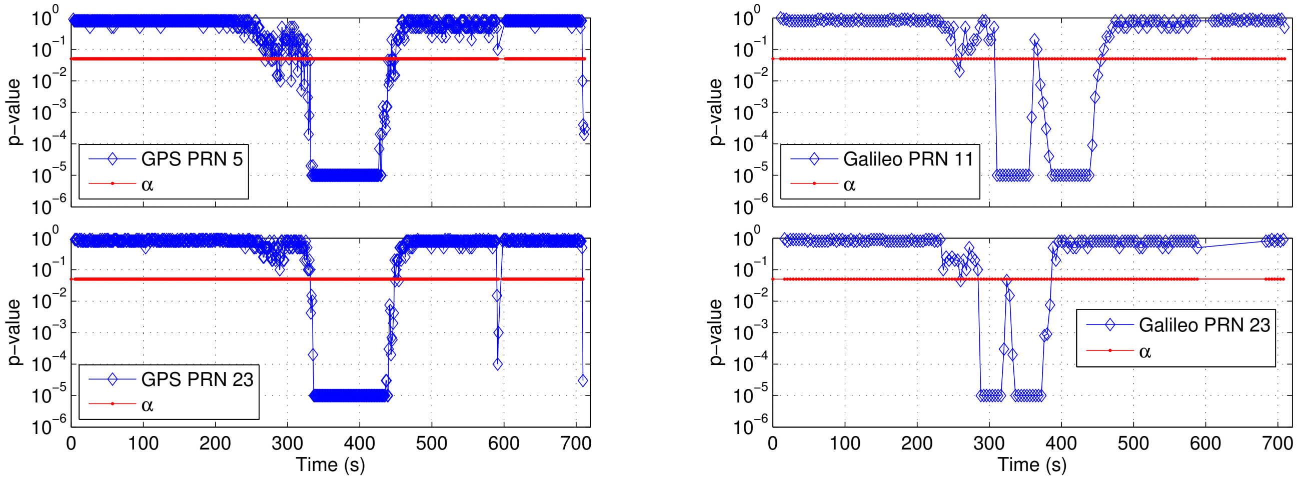
During the experiments, the constellation of GNSS signals is generated by a signal generator, able to add to the genuine signal its counterfeit replica. Thanks to the fact that the experiments are performed in the anechoic room, the signals can be transmitted at Radio Frequency (RF) and received with a standard GNSS antenna connected to the front-end and the NGene software receiver.

Two tests were performed. Both of them last 12 minutes and the attack starts after 240 seconds; in addition, in both cases simulated signals from GPS and Galileo satellites are transmitted on the L1/E1 frequency band. Test A simulates a static user under a spoofing attack that tries to force his position on a trajectory toward North East, by adding signals replicas of all the satellites in view. In the case of Test B, a dynamic user that moves toward North with a constant velocity is simulated and the spoofer aims at reproducing a North-East trajectory operating on a sub-set of GPS signals. In both cases, by using the terminology of [16], the attack can be classified as *matched-power*, since the false-to-genuine signal power ratio is equal to 0.5 dB. The main test characteristics and the front-end configuration are summarized in Table I, while the results of the two experiments are described in section V.

V. Tests Results

On the basis of the theoretical description of section III, the Chi-Square GoF test has been applied at the correlators output. In the implementation at hand, the $E' - L'$ correlators spacing $d_{s'}$ and the integration time T specific for the test were set respectively to 1.5 chips and 1 ms for the GPS signal, and 0.75 chips and 4 ms for the Galileo signal. In the presented results, the tests have been performed using $n = 1000$ correlation values, i.e. once per second for GPS and once per 4 seconds for Galileo.

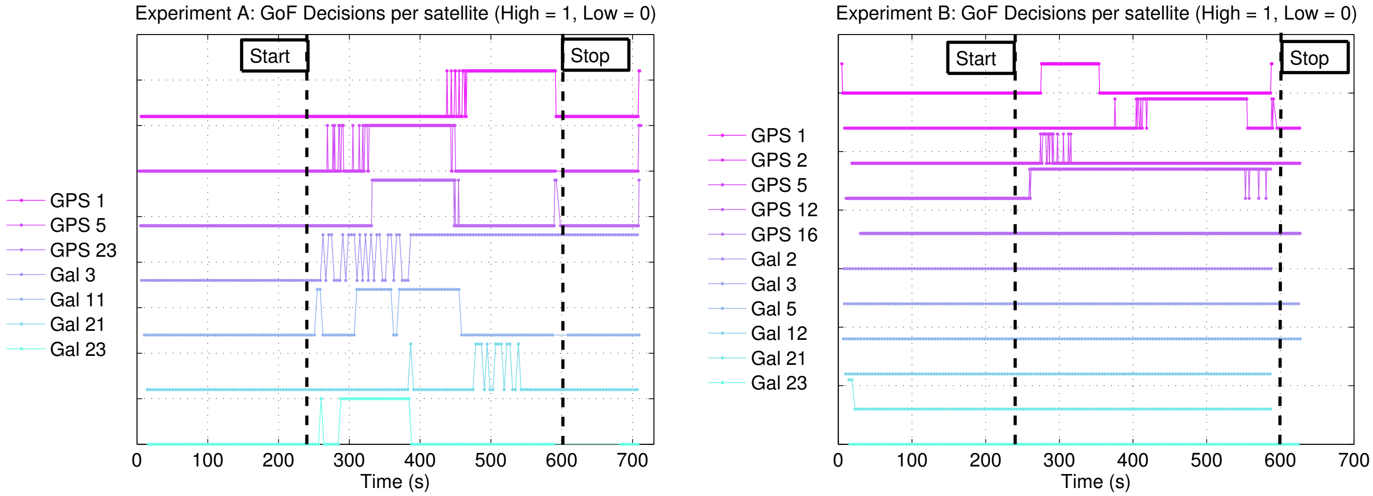
Fig. 2 shows the time sequence of the p-values for the GoF test in the experiment A, applied to four of the tracked satellites, two GPS and two Galileo, taken as an example. The GoF test shows to be able to perform a sharp spoofing detection: when the attack starts, after 240 seconds from the beginning of the data recording, the p-value slowly starts to decrease and then, when the distortions of the correlation function become more evident, abruptly drops well below the *significance level*. The GoF detection capability stops, i.e. the p-value gets back above α, when the receiver channels lock



(a)

(b)

Fig. 2. Experiment A: time sequences of the p-values for the GoF test obtained for GPS PRNs 5 and 23 (a) and Galileo PRNs 11 and 23 (b).


Experiment A: GoF Decisions per satellite (High = 1, Low = 0)

Experiment B: GoF Decisions per satellite (High = 1, Low = 0)

(a)

(b)

Fig. 3. Time sequences of the hypothesis test decisions for all the tracked satellites in both the experiments A (a) and B (b).

the spoofed signals, likely because the low power advantage of the attack.

The time series of the decisions D_χ for all the tracked satellites are reported in Fig. 3 for both the experiments. In particular, $D_\chi = 1$ indicates that the attack has been detected, as in (8), while $D_\chi = 0$ means no attack, as in (9). The black flags point out the start and stop instant of the spoofing attack. In both experiments, the first 240 seconds are clean and the hypothesis on the absence of distortion H_0 is always accepted, while between 240 and 600 seconds the GoF test is able to detect anomalies in the correlation functions of all the spoofed satellites, i.e. all satellites in experiment A and four GPS in experiment B. These results, particularly those shown in Fig. 3(b), proves the GoF test capability to detect an abnormal distortion of the output of the correlators, corresponding to the appearance of the counterfeit signal, and to clearly discriminate between spoofed and clean signal.

Such capability can be exploited to make the receiver aware of possible spoofing attacks, for instance implementing a selection strategy for the satellites to be used for the Position-Velocity and Time (PVT) computation. Those satellites which are declared to be under attack can be excluded from the PVT. In this regard, Fig. 4 and Fig. 5 illustrate the time sequence of the position in East-North-Up (ENU) coordinates produced by the receiver during both experiments. In particular, in the experiment A, no exclusion strategy can be adopted, since all satellites are simultaneosly under attack, thus all satellites are employed to compute the position, in Fig. 4, and the effect of the attack is evident: the false signal takes control of the static receiver, making its estimated position to drift towards NE. The receiver output is colored in red when at least one satellite is declared spoofed and in green when no detection is performed. In the experiment B, instead, only a sub-set of

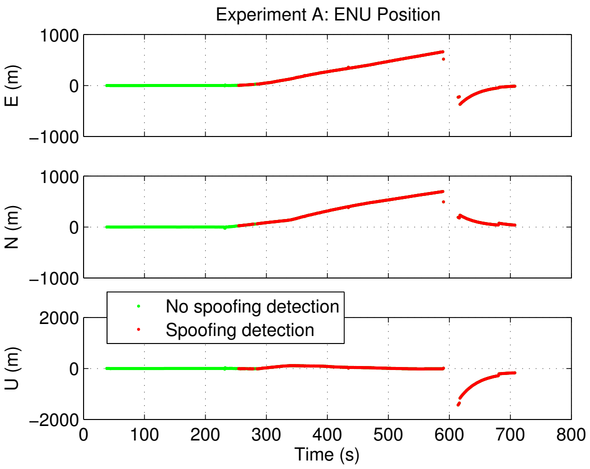


Fig. 4. Experiment A: ENU position obtained with all satellites.

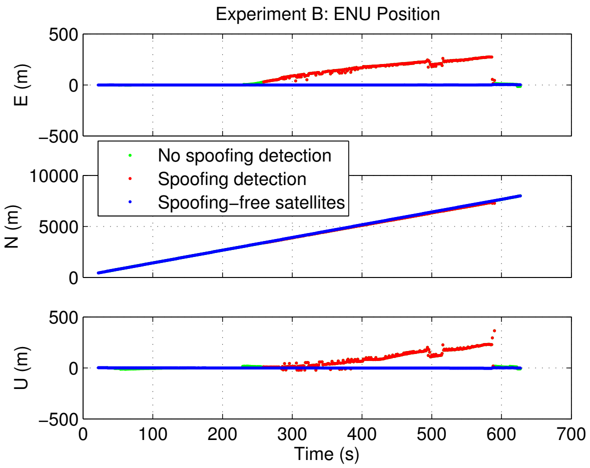


Fig. 5. Experiment B: ENU position obtained both with all satellites and with the spoofing-free only satellites.

in-view satellites are spoofed and can then be excluded. The obtained position is indicated in blue in Fig. 5: the receiver is moving on a straight trajectory towards N and the EU drift induced by the counterfeit signal is completely avoided, mitigating the effect of the attack.

VI. Conclusions

This paper has presented the validation of a spoofing detection method, namely the Chi-square Goodness of Fit test, implemented in a software receiver and applied post-correlation against two live spoofing experiments. The results obtained in two scenarios, static the former and dynamic the latter, prove the GoF capability to successfully detect the fake signal, and further support the need to make the receiver robust against spoofing attacks.

In addition, it is worth mentioning that these kind of techniques, if properly enhanced, can be applied not only as spoofing detectors, but also for distinguishing between spoofing and environmental effects, such as multipath [17].

For the next future, a smart exclusion strategy of the spoofed satellites from the PVT computation has to be implemented. Such strategy should combine the GoF decisions with other signal quality indicators along the receiving chain.

Acknowledgment

The described tests campaign has been hosted by the Institute for the Protection and Security of the Citizen (IPSC) of the Joint Research Centre (JRC), in Ispra, Italy. The authors would like to thank the researchers of JRC, that gave support during the experiments set-up and execution.

References

[1] E. D. Kaplan and C. J. Hegarty, *Understanding GPS - Principles and Applications*, 2nd ed. Artech House, 2006.

[2] F. Dovis, *GNSS Interference Threats and Countermeasures*. Artech House, 2015.

[3] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS vulnerability to spoofing threats and a review of antispoofing techniques,” *International Journal of Navigation and Observation*, vol. 2012, pp. 1–16, 2012.

[4] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, “An in-line anti-spoofing device for legacy civil GPS receivers,” in *Proc. of the 2010 Int. Tech. Meeting of the Sat. Div. of the Institute of Navigation*, San Diego, CA, Jan. 2010, pp. 698–712.

[5] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, “Detection of spoofed GPS signals at code and carrier tracking level,” in *Proc. of the 5th ESA Workshop on Satellite Navigation Technologies (NAVITEC 2010)*, Dec 2010, pp. 1–6.

[6] B. Motella and L. Lo Presti, “Methods of goodness of fit for GNSS interference detection,” *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 50, no. 3, pp. 1690–1700, July 2014.

[7] F. Bastide, D. Akos, C. Macabiau, and B. Roturier, “Automatic Gain Control (AGC) as an Interference Assessment Tool,” in *16th Int. Tech. Meeting of the Sat. Div. of The Institute of Navigation (ION GPS/GNSS 2003)*, Portland, OR, Sep. 2003, pp. 2042–2053.

[8] B. Motella, M. Pini, and L. Lo Presti, “GNSS Interference Detector based on Chi-square Goodness-of-Fit Test,” in *Proc. of the 6th ESA Workshop on Satellite Navigation Technologies, (NAVITEC 2012)*, Noordwijk, The Netherlands, Dec. 5–7, 2012, pp. 1–6.

[9] M. Troglia Gamba, B. Motella, and M. Pini, “Statistical Test applied to Detect Distortions of GNSS Signals,” in *Proc. of the 2013 Int. Conf. on Localization and GNSS (ICL-GNSS 2013)*, Turin, Italy, Jun. 25–27, 2013, pp. 1–6.

[10] M. Pini, B. Motella, and M. Troglia Gamba, “Detection of Correlation Distortions Through Application of Statistical Methods,” in *Proc. of the 26th Int. Tech. Meeting of the Sat. Div. of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, September 2013, pp. pp. 3279–3289.

[11] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses*. New York: Springer-Verlag, 2005.

[12] J. L. Devore, *Probability and Statistics for Engineering and the Sciences*, 8th ed. Brooks/Cole, Cengage Learning, 2012.

[13] M. Troglia Gamba, M. D. Truong, B. Motella, E. Falletti, and T. T. Hai, “Hypothesis testing methods to detect spoofing attacks: a test against the TEXBAT datasets,” *GPS Solutions (to appear)*, 2016.

[14] A. Molino, M. Nicola, M. Pini, and M. Fantino, “N-Gene GNSS software receiver for acquisition and tracking algorithms validation,” in *Proc. of the 17th European Signal Processing Conference (EUSIPCO 2009)*, Glasgow, Scotland, Aug. 2009, pp. 2171–2175.

[15] M. Troglia Gamba, M. Nicola, and E. Falletti, “Performance assessment of an ARM-based dual-constellation GNSS software receiver,” in *Proc. of the 2015 Int. Conf. on Localization and GNSS (ICL-GNSS 2015),*, Gothenburg, Sweden, Jun. 2015, pp. 1–6.

[16] T. Humphreys, J. Bhatti, D. Shepard, and K. Wesson, “The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques,” in *Proc. of the 25th Int. Tech. Meeting of the Sat. Div. of the Institute of Navigation (ION GNSS 2012)*, Nashville, TN, Sep. 2012, pp. 3569–3583.

[17] E. G. Manfredini, B. Motella, and F. Dovis, “Signal Quality Monitoring for Discrimination between Spoofing and Environmental Effects, Based on Multidimensional Ratio Metric Tests,” in *28th Int. Tech. Meeting of the Sat. Div. of the Institute of Navigation (ION GNSS+ 2015)*, Tampa, Florida, Sep. 2015, pp. 3100–3106.