A Sum-of-Squares Approach to GNSS Spoofing Detection

Article *in* IEEE Transactions on Aerospace and Electronic Systems · August 2016

2 authors:

Daniele Borio
European Commission
114 PUBLICATIONS **739** CITATIONS
SEE PROFILE

Ciro Gioia
European Commission
45 PUBLICATIONS **145** CITATIONS
SEE PROFILE

A Sum-of-Squares Approach to GNSS Spoofing Detection

Daniele Borio[1] and Ciro Gioia[2]
1) European Commission, Joint Research Centre (JRC),
Institute for the Protection and Security of the Citizen (IPSC),
Security Technology Assessment (STA) Unit, Ispra (VA), Italy
2) Piksel S.p.a., Milano, Italy
Email: daniele.borio@jrc.ec.europa.eu, ciro.gioia@tin.it

***Abstract*— This paper analyses the Sum-of-Squares (SoS) detector which is designed to reveal the presence of a spoofing attack. The SoS decision statistic is computed using carrier phase measurements from two spatially separated GNSS receivers and assumes a simple form which makes it suitable for real-time applications. The detector is theoretically characterized and its effectiveness is shown using simulations and experiments involving real GPS data.**

***Index Terms*—Carrier phase, Detection, Dual-antenna, GNSS, Sum-of-Squares, Spoofing.**

I. Introduction

In a spoofing attack, counterfeit Global Navigation Satellite System (GNSS) signals are used to mislead a GNSS receiver that will determine an erroneous user Position Velocity and Time (PVT) solution. Over the last decade, spoofing has been perceived as a more and more concrete threat. This perception has been motivated by technological progresses and by the availability of advanced Software Defined Radio (SDR) platforms that are making the development of GNSS spoofers not only feasible but also affordable. Privacy, taxation and payment avoidance are some of the reasons that motivate the development of spoofing platforms.

As a response to this threat, several techniques have been developed to reveal the presence of a spoofing attack [1]–[4]. Spoofing attacks can be defeated by exploiting and possibly introducing specific features difficult to counterfeit. These features can be at the signal, measurements and position level. A high-level view of different anti-spoofing approaches is provided in Fig. 1. Three main categories are identified: cryptographic defences [5]–[7], techniques based on signal features [1] and approaches exploiting external verification sources.

The cryptographic defence is the most effective but requires GNSS signals to be designed to support cryptographic functions. Cryptographic defences can be further divided into encryption-based approaches, which requires fully or partially encrypted GNSS signals, and authentication-based defences where GNSS signals have specific features which allow their authentication. Code and navigation message encryptions are forms of signal encryptions. In the first case, the Pseudo-Random Noise (PRN) code used to modulate the GNSS signal is encrypted and known only to authorized users. This is the case of the GPS P(Y) and Galileo Publicly Regulated Service (PRS) signals. It is noted that encrypted signals can be used for anti-spoofing without knowing the actual signal code. A reference receiver and a communication link are however required [8]. The reference receiver stores the samples of the encrypted signals and compares them with that of the rover receiver. If a high correlation is found, then it is possible to assume that the rover receiver is operating normally. The lack of correlation indicates a spoofing attack [8]. This form of defence is based on a specific signal feature, i.e. the presence of an encrypted signal component, and it is denoted as "P-code and PRS verification" in Fig. 1.

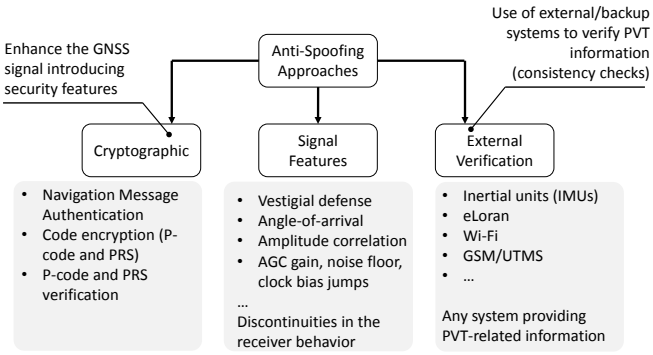


Fig. 1. Summary of different spoofing detection approaches available in the literature.

Navigation message encryption implies that the GNSS signal can be acquired and tracked normally since its PRN code is known. However, the content of the navigation message is available only to authorized users.

Authentication is allowed by specific signal features [5], [9] such as the presence of random-like sequences in the signal code or navigation message. Only using an authentication key, is it possible to establish whether the transmitted sequence is authentic or not.

Several anti-spoofing techniques are based on signal features which are difficult to counterfeit. For example, the vestigial defence [10] is based on the assumption that original GNSS signals are present also during a spoofing attack. Thus, spoofing can be detected by verifying the presence of residual signal components in addition to the signal already tracked

by the receiver. The Angle-Of-Arrival (AOA) defence [3], [11] exploits the fact that genuine GNSS signals come from different directions whereas counterfeit signals are transmitted by a single source. The development of an innovative AOA defence is the main focus of this paper and additional details on this approach are provided in the following.

The assumption that spoofing signals are broadcast by the same antenna and reach the receiver following the same path is also exploited by [12] that developed a spoofing detection approach based on the correlation between the amplitudes of the different received signals. Finally, discontinuities in the clock bias, in the Automatic Gain Control (AGC) time series and in the noise floor estimates may occur during a spoofing attack. These effects can be used for spoofing detection [13]. Finally, spoofing can be detected by comparing the GNSS PVT with alternative sources of location. Examples of technologies which can be coupled with GNSS for spoofing location are: inertial units, Enhanced LOng RAnge Navigation (E-LORAN), Wireless Fidelity (WiFi) and cellular-based location.

An exhaustive review of the different anti-spoofing techniques is out of the scope of this paper and the interested reader is referred to review articles [1], [2].

Among the different spoofing detection approaches, the AOA defence is one of the most effective [3], [11], [14] since it does not require external infrastructures providing complementary PVT information or cryptographic signal features. Genuine GNSS signals are transmitted by different satellites and arrive at the receiver from different directions. On the contrary, counterfeit signals are assumed to be broadcast from a single direction and thus share a common AOA. A dual-antenna system can be used to verify if all the signals received share the same AOA [3], [11], [14].

In this paper, a novel AOA approach for spoofing detection is developed. In particular, the Sum-of-Squares (SoS) detector is derived using the Generalized Likelihood Ratio Test (GLRT) approach. Differently from previous work [3], [11], [14], carrier phase cycle ambiguities are modelled as random variables assuming value on an arbitrary set of integers. Thus, they don't need to be estimated as in [3], [11]. This novel formulation leads to the SoS detectors where decision variables are expressed as the sum of squared carrier phase single differences corrected for a pseudo-mean and for their integer parts. In addition to the innovative design, the approach proposed has several advantages with respect to previous AOA spoofing detection approaches. The orientation of the antennas used for spoofing detection is considered as a nuisance parameter and does not need to be estimated. In this way, antenna array calibration is not needed. The SoS decision statistic derived is expressed in closed form and can be evaluated with a reduced computational load. AOA spoofing detectors from the literature require complex numerical algorithms for the evaluation of their decision statistics [3]. The SoS formulation makes SoS detectors particularly suitable for real-time implementations as demonstrated in [15].

Moreover, a simple criterion for fixing the decision threshold is provided and analyzed. Most AOA spoofing detectors available in the literature [3], [11], [14] have to use empirical criteria, often based on Monte Carlo simulations, to set the decision threshold [3]. The criterion proposed here is general and can be applied to most satellite and signal conditions. Moreover, it does not require extensive Monte Carlo simulations [3] or tabulated threshold values. Thus, the complexity of the method is further reduced with respect to other AOA anti-spoofing techniques [3], [11], [14].

SoS detectors are thoroughly analysed and AOA spoofing detection is demonstrated using Commercial Off-The-Shelf (COTS) components: the algorithm proposed does not need dedicated SDR platforms [3] and can be implemented using commercial GNSS receivers able to provide carrier phase measurements. This is a significant advantage with respect to previous attempts in the literature which require dedicated hardware such as front-ends sharing the same clock [3]. Monte Carlo simulations and experiments using live GPS data support the theoretical findings and confirm the effectiveness of the SoS paradigm for spoofing detection.

This paper focuses on theoretical aspects and on the statistical characterization of the SoS detectors. The results obtained are complemented by conference paper [15] which discusses a possible implementation of the SoS detector on a real-time platform.

The remainder of this paper is organized as follows. In Section II, a model for carrier phase single difference is introduced and used in Section III to derive the SoS detector. A statistical characterization and a criterion for fixing the decision threshold are provided in Section IV. Experiments involving live GPS signals are described in Section V and conclusions are finally drawn in Section VI.

II. System and Measurement Model

Commercial GNSS receivers are able to output carrier phase measurements which can be modelled as [16]:

$$\phi_i = d_i + N_i\lambda + c(dt - dT) - d_{ion,i} + d_{trop,i} + \eta_i \quad (1)$$

where:

- the index i is used to denote measurements from the ith satellite
- ϕ_i is the carrier phase measured by the receiver in units of metres
- d_i is the geometric distance between the receiver and the ith satellite
- c is the speed of light and dt and dT are the satellite and receiver clock errors
- N_i is the cycle ambiguity and is an integer number
- λ is the signal wavelength (approximately 0.19 meters for the GPS L1 frequency)
- $d_{ion,i}$ and $d_{trop,i}$ model the ionospheric and tropospheric effects
- η_i is a noise term accounting for residual unmodelled errors.

When two receivers are available, it is possible to build single carrier phase differences:

$$\Delta\phi_i = \phi_i^1 - \phi_i^2 = (d_i^1 - d_i^2) + \Delta N_i\lambda + c(dT^2 - dT^1) + \Delta\eta_i \quad (2)$$

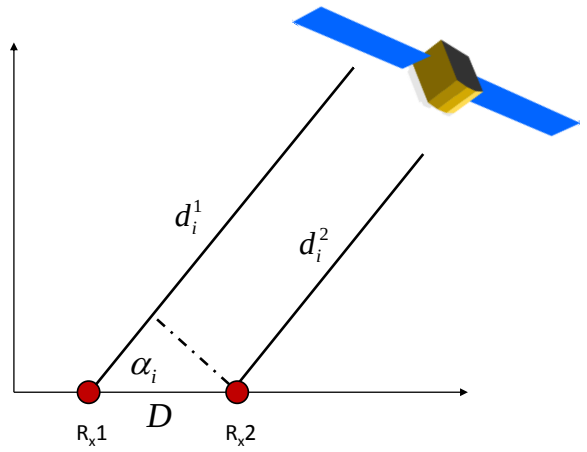


Fig. 2. Signal reception from two closely-spaced GNSS receivers. RF waves impinging on the two receivers can be considered parallel.

where superscripts 1 and 2 denote measurements from the two receivers. Under the assumption that the two receivers are closely spaced, the ionospheric and tropospheric effects cancel out [16]. Moreover, since the distance between satellites and receivers is much greater than the distance between the two receivers, it is possible to assume the geometric configuration shown in Fig. 2: the Radio Frequency (RF) waves are almost parallel when they reach the receivers. Using this approximation, the difference $(d_i^1 - d_i^2)$ can be expressed as:

$$d_i^1 - d_i^2 = D\cos\alpha_i \tag{3}$$

where D is the distance between the two receivers and α_i is the AOA of the ith satellite signal. Thus,

$$\Delta\varphi_i = \frac{\Delta\phi_i}{\lambda} = \frac{D}{\lambda}\cos\alpha_i + \Delta N_i + \frac{c}{\lambda}(dT^2 - dT^1) + \frac{1}{\lambda}\Delta\eta_i \tag{4}$$

models carrier phase single differences expressed in units of cycles.

The AOA defence can be implemented using carrier phase single differences (4) by verifying if the geometric term, (3), is the same for all the signals received. This principle is exploited in the next section to design the SoS detector.

III. Sum-of-Squares Detection

Carrier phase single differences (4) can be used to design a statistical test for spoofing detection. In particular, the clock bias term in (4)

$$b = \frac{c}{\lambda}\left(dT^2 - dT^1\right) \tag{5}$$

is common to all measurements and the term

$$\mu_i\left(\alpha_i, D\right) = \frac{D}{\lambda}\cos\alpha_i \tag{6}$$

only depends on the AOA, α_i, of the ith received signal. When transmitted by a spoofer, all the signals are from the same AOA, α, and geometric term (6) is common to all carrier phase single differences. Thus, the spoofing detection problem can be formulated as a binary test:

$$\begin{aligned} H_0) &\quad \mu_i(\alpha_i, D) = \mu \quad \forall i \\ H_1) &\quad \exists i : \mu_i(\alpha_i, D) \neq \mu. \end{aligned} \tag{7}$$

The null hypothesis H_0 is selected if the geometric term, $\mu_i(\alpha_i, D)$, is the same for all carrier phase single differences. The geometric term, $\mu_i(\alpha_i, D)$ is not directly observable since carrier phase single differences are affected by the clock bias, b, and by the ambiguities, ΔN_i. However, b, is common to all measurements and test (7) can be restated as

$$\begin{aligned} H_0) &\quad \mu_i(\alpha_i, D) + b = k \quad \forall i \\ H_1) &\quad \exists i : \mu_i(\alpha_i, D) + b \neq k. \end{aligned} \tag{8}$$

where k is an arbitrary constant. The ambiguities ΔN_i are described here in a statistical sense and are not considered as parameters to be estimated as in [3]. In particular, it is assumed that ΔN_i are discrete random variables uniformly distributed over the integer numbers between N_{min} and N_{max}. This implies that ΔN_i can assume any integer value between N_{min} and N_{max} with the same probability. Note that N_{min} and N_{max} are arbitrary constants and can, for example, correspond to the minimum and maximum value used to represent the integer part of carrier phase single differences. The probability density function (pdf) of ΔN_i can be expressed as:

$$p_N(n_i) = \frac{1}{N_{max} - N_{min} + 1}\sum_{j_i=N_{min}}^{N_{max}} \delta\left(n_i - j_i\right) \tag{9}$$

where $\delta(\cdot)$ is the Dirac Delta. The noise term $\frac{1}{\lambda}\Delta\eta_i$ is assumed to be a zero mean Gaussian noise with variance σ_i^2 and its pdf is given by:

$$p_\eta(\eta_i) = \frac{1}{\sqrt{2\pi\sigma_i^2}}\exp\left\{-\frac{1}{2\sigma_i^2}\eta_i^2\right\}. \tag{10}$$

Finally, the pdf of the sum of the ambiguity and noise term is given by:

$$\begin{aligned} p_m(m_i) &= p_N(m_i) * p_\eta(m_i) \\ &= \frac{\sum_{j_i=N_{min}}^{N_{max}} \exp\left\{-\frac{1}{2\sigma_i^2}\left(m_i - j_i\right)^2\right\}}{\sqrt{2\pi\sigma_i^2}\left(N_{max} - N_{min} + 1\right)} \end{aligned} \tag{11}$$

where symbol '$*$' denotes the convolution product. The sum of noise and ambiguity is characterized by a mixture of Gaussian density functions with means centered around the integers between N_{min} and N_{max}.

In this paper, the GLRT approach [17] is used to design the test for spoofing detection. In this respect, it is necessary to estimate the likelihoods associated with the carrier phase single differences under both H_0 and H_1.

A. Likelihood under H_0

Under, H_0, all signals arrive from the same direction and all the measurements are characterized by the same geometric term and clock bias. Thus, the pdf associated with a single measurement is given by

$$p_\varphi\left(m_i \middle| H_0\right) = \frac{\sum_{j_i=N_{min}}^{N_{max}} \exp\left\{-\frac{1}{2\sigma_i^2}\left(m_i - j_i - k\right)^2\right\}}{\sqrt{2\pi\sigma_i^2}\left(N_{max} - N_{min} + 1\right)} \tag{12}$$

where k is the arbitrary constant introduced in (8) to denotes the sum of the geometric and clock terms. Pdf (12) has been

obtained by translating (11) by k. Since single carrier phase differences are statistically independent, the joint pdf under H_0 is given by the product of the individual pdfs. Finally, the likelihood under H_0 is obtained by introducing the actual measurements in (12):

$$\begin{aligned} L(k|H_0) &= \prod_{i=0}^{I-1} p_\varphi\left(\Delta\varphi_i|\, H_0\right) \\ &= K_\sigma \prod_{i=0}^{I-1} \sum_{j_i=N_{min}}^{N_{max}} \exp\left\{-\frac{1}{2\sigma_i^2}\left(\Delta\varphi_i - j_i - k\right)^2\right\} \end{aligned} \tag{13}$$

where

$$K_\sigma = \frac{\prod_{i=0}^{I-1} \frac{1}{\sqrt{2\pi\sigma_i^2}}}{\left(N_{max} - N_{min} + 1\right)^I} \tag{14}$$

and I is the number of measurements available. In (13), k is unknown and needs to be estimated. In particular, in the GLRT approach, k is selected in order to maximize likelihood (13). The product of weighted summations in (13) makes the maximization complex and additional simplifications are required. In particular, it is possible to assume that

$$\sigma_i \ll 1 \text{ cycle} \tag{15}$$

i.e. that the standard deviation of the measurements is significantly lower than 1 cycle. This assumption is reasonable since, standard deviations higher then 1 would cause frequent cycle slips and loss-of-lock in the tracking loops used to process the signal carrier. Condition (15) implies that

$$\exp\left\{-\frac{1}{2\sigma_i^2}\left(\Delta\varphi_i - j_i - k\right)^2\right\} \approx 0 \qquad \text{for } |\Delta\varphi_i - j_i - k| > 1. \tag{16}$$

Thus, the summations in (13) can be simplified by considering only the dominant terms for which $|\Delta\varphi_i - j_i - k| < 1$. Only two terms in the summations in (13) respect this condition and are obtained for

$$j_i = \begin{cases} \lfloor \Delta\varphi_i - k \rfloor \\ \lfloor \Delta\varphi_i - k \rfloor + 1 \end{cases} \tag{17}$$

where $\lfloor \cdot \rfloor$ denotes the *floor* operator that evaluates the largest integer not greater than its argument. In this way, $\Delta\varphi - k - \lfloor \Delta\varphi - k \rfloor$ is a positive real number lower than 1. $\Delta\varphi - k - \lfloor \Delta\varphi - k \rfloor - 1$ is a negative real number greater than -1. Using these conditions, (13) becomes:

$$\begin{aligned} &L(k|H_0) \\ &= K_\sigma \prod_{i=0}^{I-1} \left[\exp\left\{-\frac{1}{2\sigma_i^2}\mathrm{f}_r^2\left(\Delta\varphi_i - k\right)\right\} \right. \\ &\quad \left. + \exp\left\{-\frac{1}{2\sigma_i^2}\left(\mathrm{f}_r\left(\Delta\varphi_i - k\right) - 1\right)^2\right\} \right] \\ &= K_\sigma \prod_{i=0}^{I-1} 2\exp\left\{-\frac{1}{2\sigma_i^2}\left[\left(\mathrm{f}_r\left(\Delta\varphi_i - k\right) - \frac{1}{2}\right)^2 + \frac{1}{4}\right]\right\} \\ &\quad \cdot \cosh\left(\frac{\mathrm{f}_r\left(\Delta\varphi_i - k\right) - \frac{1}{2}}{2\sigma_i^2}\right) \end{aligned} \tag{18}$$

where

$$\mathrm{f}_r(x) = x - \lfloor x \rfloor. \tag{19}$$

Likelihood (18) can be now easily maximized with respect to k using, for example, an exhaustive search approach. Note that $\mathrm{f}_r(x)$ and thus $L(k, H_0)$ are periodic in k with period 1. Thus, it is sufficient to limit the search for k in the range (0, 1]. $L(k|H_0)$ can be further simplified under the assumption that

$$\left|\frac{\mathrm{f}_r\left(\Delta\varphi_i - k\right) - \frac{1}{2}}{2\sigma_i^2}\right| \gg 1 \tag{20}$$

In this case, the hyperbolic cosine in (18) can be approximated as

$$\cosh\left(\frac{\mathrm{f}_r\left(\Delta\varphi_i - k\right) - \frac{1}{2}}{2\sigma_i^2}\right) = \frac{1}{2}\exp\left\{\frac{\left|\mathrm{f}_r\left(\Delta\varphi_i - k\right) - \frac{1}{2}\right|}{2\sigma_i^2}\right\} \tag{21}$$

and likelihood $L(k|H_0)$ becomes

$$\begin{aligned} &L(k|H_0) \\ &= K_\sigma \prod_{i=0}^{I-1} \exp\left\{-\frac{1}{2\sigma_i^2}\left[\left(\Delta\varphi_i - k\right) - \mathrm{round}\left(\Delta\varphi_i - k\right)\right]^2\right\} \end{aligned} \tag{22}$$

where

$$\mathrm{round}\left(x\right) = \begin{cases} \lfloor x \rfloor & \text{if } \mathrm{f}_r(x) < 0.5 \\ \lfloor x \rfloor + 1 & \text{if } \mathrm{f}_r(x) > 0.5 \end{cases}. \tag{23}$$

This result is equivalent to consider only one term in the summations in (13). This term is obtained for

$$j_i = \mathrm{round}(\Delta\varphi_i - k). \tag{24}$$

The validity of the approximations considered above is analysed in Fig. 3 where a single factor of likelihood (13) is provided as a function of k. In the figure, $\Delta\varphi_i$ has been selected randomly in the range $[0, 1)$. $\Delta\varphi_i$ introduces a shift in the factor depicted and thus does not impact the validity of the approximations introduced. Two cases are considered in Fig. 3:

- $\sigma_i = 0.26$ cycles: when the GPS L1 centre frequency is considered, it corresponds to carrier phase single differences with a standard deviation equal to 5 cm
- $\sigma_i = 0.05$ cycles: it corresponds to carrier phase single differences with a standard deviation equal to 1 cm.

The two terms approximation derived in (18) is effective for measurements with a relatively high standard deviations (5 cm) and for all values of k. When $\sigma_i = 0.26$ is considered, single term approximation (22) is valid only for values of k close to $\Delta\varphi_i - \mathrm{round}(\Delta\varphi_i)$ (0.9420 cycles in Fig. 3). The single term approximation becomes valid for all values of k for $\sigma_i = 0.05$. This type of accuracy is generally achieved by standard GNSS receivers [18] and approximation (22) is thus adopted in the following.
The maximization of (22) is equivalent to the minimization of

$$L_l(k|H_0) = \sum_{i=0}^{I-1} \frac{1}{\sigma_i^2}\left[\left(\Delta\varphi_i - k\right) - \mathrm{round}\left(\Delta\varphi_i - k\right)\right]^2 \tag{25}$$

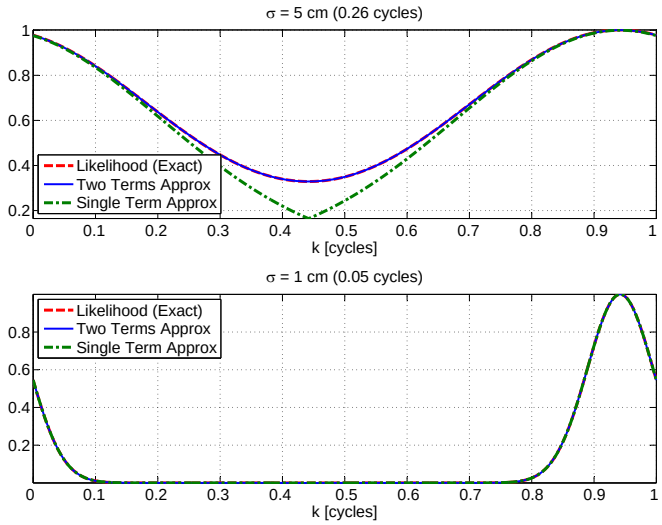


Fig. 3. Different approximations of a single factor present in likelihood function (13). The summation of exponential functions is approximated considering only two and one term, respectively.

which is a scaled log-likelihood function. The solution to the problem

$$\hat{k}|H_0 = \arg\min_k L_l(k|H_0) \tag{26}$$

is discussed in Appendix A where it is shown that $\hat{k}|H_0$ assumes the following form

$$\hat{k}|H_0 = \sum_{i=0}^{I-1} w_i \left[\Delta\varphi_i - \text{round}\left(\Delta\varphi_i\right) + n_i^{opt}\right] \tag{27}$$

where w_i are positive weights defined as

$$w_i = \frac{\frac{1}{\sigma_i^2}}{\sum_{j=0}^{I-1}\frac{1}{\sigma_j^2}} \tag{28}$$

and $\left\{n_i^{opt}\right\}_{i=0}^{I-1}$ are binary constants, i.e. they assume value in $\{0,1\}$. A procedure for determining $\left\{n_i^{opt}\right\}_{i=0}^{I-1}$ is also outlined in Appendix A. $\hat{k}|H_0$ can be interpreted as the mean of the fractional part of $\Delta\varphi_i$ corrected for a term depending on the $\left\{n_i^{opt}\right\}_{i=0}^{I-1}$ and it is thus a pseudo-mean. Finally, $\hat{k}|H_0$ is an M-estimator [19], [20] since it has been obtained as the solution of a Maximum Likelihood (ML) problem.

B. Likelihood under H_1

Under H_1, the measurements are characterized by different geometric terms and the pdf associated to a carrier phase single difference is given by

$$p_\varphi\left(m_i|\,H_1\right) = \frac{\sum_{j_i=N_{min}}^{N_{max}} \exp\left\{-\frac{1}{2\sigma_i^2}\left(m_i - j_i - k_i\right)^2\right\}}{\sqrt{2\pi\sigma_i^2}\left(N_{max} - N_{min} + 1\right)} \tag{29}$$

where

$$k_i = \mu_i(\alpha_i, D) + b. \tag{30}$$

Following the same approach adopted in Section III-A, it is possible to show that the likelihood function under H_1 can be approximated as:

$$\begin{aligned} &L(k_0, k_1, ..., k_{I-1}|H_1) \\ &= K_\sigma \prod_{i=0}^{I-1} \exp\left\{-\frac{1}{2\sigma_i^2}\left[\left(\Delta\varphi_i - k_i\right) - \text{round}\left(\Delta\varphi_i - k_i\right)\right]^2\right\}. \end{aligned} \tag{31}$$

In this case, the maximization of the likelihood has to be performed with respect to the different k_i. The problem is easily solved and a solution is given by:

$$\hat{k}_i|H_1 = \Delta\varphi_i - \lfloor\Delta\varphi_i\rfloor. \tag{32}$$

Solution (32) has been obtained by assuming $0 < k_i \leq 1$. This solution is significantly different from that obtained in [3] which introduces a dependency on the geometrical parameters of the system and tries to estimate the carrier phase ambiguities. Estimates (32) make the arguments of the exponential terms in (32) vanish and the maximum value of $L(k_0, k_1, ..., k_{I-1}|H_1)$ is K_σ.

C. GLRT Decision Statistic

The GLRT decision statistic is obtained as [17]

$$\begin{aligned} \Lambda &= \Lambda(\Delta\varphi_0, \Delta\varphi_1, ..., \Delta\varphi_{I-1}) \\ &= -2\log\left(\frac{\sup_k L(k|H_0)}{\sup_{k_0,k1,...,k_{I-1}} L(k_0, k_1, ..., k_{I-1}|H_1)}\right) \\ &= \sum_{i=0}^{I-1}\frac{1}{\sigma_i^2}\left[\left(\Delta\varphi_i - \hat{k}\right) - \text{round}\left(\Delta\varphi_i - \hat{k}\right)\right]^2 \end{aligned} \tag{33}$$

where $\hat{k}$ is the M-estimator discussed in Section III-A. The specifier, '$|H_0$', has been dropped for ease of notation and since $\hat{k}$ is unambiguously defined by (27).

Decision statistic Λ is a weighted sum of squared differences and thus the detector associated to (33) is named SoS detector. It is noted that (33) is analogous to the Analysis-Of-Variance (ANOVA) [21] decision statistic obtained to test if all the elements of a population have the same mean. In the ANOVA framework, measurements are affected by Gaussian noise only. In the case considered here, the presence of the ambiguities, ΔN_i, increases the complexity of the problem and measurements need to be corrected using the rounding operations indicated in (33). In ANOVA, $\hat{k}$ is replaced by the weighted mean of the measurements and the decision statistic is a measure of the dispersion of the measurements.

The test is performed by comparing Λ with a decision threshold, T_h. If Λ is greater than T_h, then the H_0 hypothesis is rejected and normal operating conditions are declared. A methodology for setting the decision threshold in discussed in Section IV.

In the following, special cases of (33) are at first analysed.

D. Uniform weighting

Each squared term in the summation in (33) is weighted by the inverse of the measurement variance, σ_i^2. A special case of the SoS is obtained when all the variances are equal:

$$\sigma_i^2 = \sigma^2. \tag{34}$$

Condition (34) expresses the fact that carrier phase single differences are assumed to be *homoscedastic*, i.e., they have homogeneous variances [22]. Using this assumption, the dependence from $\sigma_i^2 = \sigma^2$ can be dropped and (33) becomes:

$$\Lambda_u = \sum_{i=0}^{I-1} \left[\left(\Delta\varphi_i - \hat{k} \right) - \text{round} \left(\Delta\varphi_i - \hat{k} \right) \right]^2 \tag{35}$$

where the subscript, u, indicates that uniform weighting is applied. Moreover, the computation of $\hat{k}$ is simplified and (27) becomes

$$\hat{k} = \frac{1}{L} \sum_{i=0}^{I-1} \left[\Delta\varphi_i - \text{round} \left(\Delta\varphi_i \right) \right] + \frac{N^{opt}}{I} \tag{36}$$

where N^{opt} is an integer in the set $\{0, I-1\}$. N^{opt} minimizes (35) and can be found by direct inspection. Although, the assumption of homoscedasticity is, in general, not verified Eqs. (35) and (36) define a spoofing detector which is simpler to implement in practice.

E. Double difference detector

A suboptimal spoofing detector can be obtained by approximating (27) using the following approach. Assume that one of the carrier phase single differences is characterized by a significantly lower variance than that of the other measurements. This implies

$$w_R \gg w_i \qquad \text{for } i = 0, 1, ..., I-1; i \neq R \tag{37}$$

where R is the index associated with the measurement with the lowest variance or equivalently with the highest Carrier-to-Noise power spectral density ratio (C/N_0). Then (27) can be approximated as

$$\hat{k} \approx \Delta\varphi_R - \text{round} \left(\Delta\varphi_R \right) + n_R^{opt}. \tag{38}$$

In (38), w_R is implicitly approximated as 1. This approximation is justified by definition (28) and by assumption (37). Using approximation (38), the double difference SoS detector is obtained:

$$\begin{aligned} \Lambda_d &= \sum_{i=0}^{I-1} \frac{1}{\sigma_i^2} [\left(\Delta\varphi_i - \Delta\varphi_R - \text{round} \left(\Delta\varphi_R \right) + n_R^{opt} \right) \\ &\quad - \text{round} \left(\Delta\varphi_i - \Delta\varphi_R - \text{round} \left(\Delta\varphi_R \right) + n_R^{opt} \right)]^2 \\ &= \sum_{i=0}^{I-1} \frac{1}{\sigma_i^2} \left[\left(\Delta\varphi_i - \Delta\varphi_R \right) - \text{round} \left(\Delta\varphi_i - \Delta\varphi_R \right) \right]^2 . \end{aligned} \tag{39}$$

In (39), $\text{round} \left(\Delta\varphi_R \right) + n_R^{opt}$ are integers and thus commute with the round$(\cdot)$ operator. In this way, decision statistic (39) only depends on the carrier phase double differences:

$$\Delta^2 \varphi_{i,R} = \Delta\varphi_i - \Delta\varphi_R.$$

Decision statistic (39) measures the dispersion of the carrier phase double differences and, although it leads to a suboptimal detector, Λ_d is simpler to compute and does not need any search for the optimal $\hat{k}$. If the variances of the measurements are unknown, (39) can be further simplified and decision statistic

$$\Lambda_{du} = \sum_{i=0}^{I-1} \left[\left(\Delta\varphi_i - \Delta\varphi_R \right) - \text{round} \left(\Delta\varphi_i - \Delta\varphi_R \right) \right]^2 \tag{40}$$

can be adopted.
The general SoS decision statistic is analysed in the next section. The characterization of suboptimal detectors, (35) and (39), are left for future work.

IV. Statistical Characterization and Threshold Setting

In this paper, the decision threshold, T_h is fixed in order to obtain a target probability of type I error [17]. A type I error corresponds to reject the null hypothesis even if it is true. Since H_0 has been defined as the hypothesis of a spoofing attack, a type I error occurs when spoofing is undetected. This criterion allows one to fix the probability of missing a spoofing attack, i.e. the probability of missed detection. Note that in [3], H_0 was defined as the hypothesis of normal operating conditions. This choice however does not allow the derivation of a simple criterion for fixing the decision threshold. In particular, the authors of [3] acknowledged that, in their case, deriving an analytical criterion for fixing the decision threshold is still an open problem and off-line Monte Carlo simulations may be the only solution. Problem formulation (8) allows the derivation of a practical criterion for fixing the decision threshold. This approach is similar to that adopted in [23] where H_0 was defined as the presence of a spoofing attack.
The probability of missed detection is defined as

$$P_{md}(T_h) = P(\Lambda > T_h | H_0) \tag{41}$$

where Λ is decision statistic (33). Using the results reported in Appendix A (see Eq. (53)), decision statistic (33) can be expressed as

$$\Lambda = \sum_{i=0}^{I-1} \frac{1}{\sigma_i^2} \left[\bar{y}_i - \sum_{j=0}^{I-1} w_j \bar{y}_j \right]^2 \tag{42}$$

where

$$\bar{y}_i = \Delta\varphi_i - \text{round}(\Delta\varphi_i) + n_i^{opt}. \tag{43}$$

Λ is thus a weighted sample variance [24] of the carrier phase single differences corrected for an integer number of cycles. If the $\bar{y}_i$ defined in (43) were Gaussian random variables with the same mean, then Λ would be a χ^2 random variable with $I-1$ degrees of freedom [24]. From signal model (4), it follows that $\Delta\varphi_i$ are Gaussian random variables translated by an arbitrary integer number of cycles. Corrected measurements, $\bar{y}_i$ are obtained from $\Delta\varphi_i$ through the function

$$f(x) = x - \text{round}(x) \tag{44}$$

which removes the dependency on the integer number of cycles. Function (44) is analysed in Fig. 4: it is a piecewise linear function which approximately preserves the Gaussian nature of the random variable at its input. This is true if σ_i^2, the variance of the input random variable, is significantly

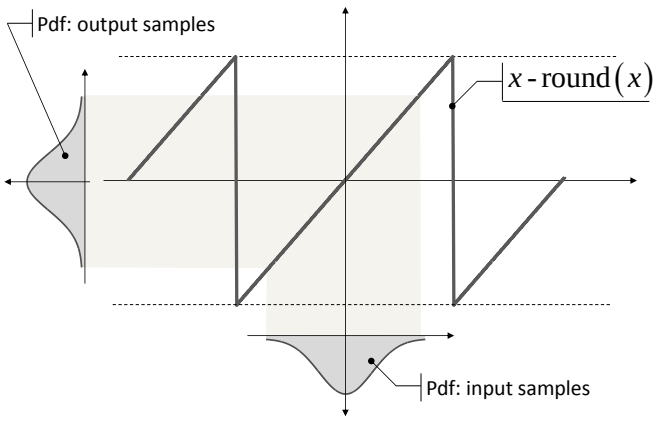


Fig. 4. Impact of "$x - \text{round}(x)$" on the pdf of the corrected carrier phase single differences.

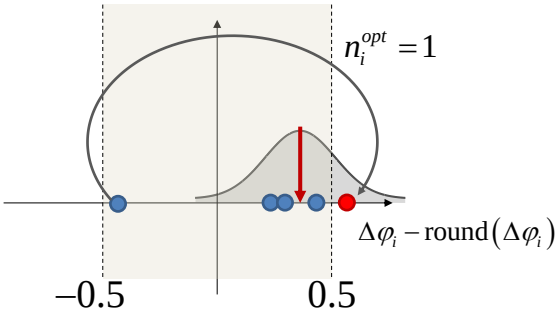


Fig. 5. Impact of n_i^{opt} on the measurements corrected through the "round" operator: n_i^{opt} compact the measurements around a common mean.

lower then 1. In particular, effects on the tails of the pdf of the random variable can be neglected for $\sigma_i^2 \ll 1$. This condition was already adopted in (15) for the design of the SoS detector and is used here for the evaluation of probability (41). Thus, $\Delta\varphi_i - \text{round}(\Delta\varphi)$ can be considered Gaussian. Moreover, the addition of n_i^{opt} does not alter the distribution of the measurements. In particular, n_i^{opt} are obtained minimizing the dispersion of $\Delta\varphi_i - \text{round}(\Delta\varphi)$ around a common mean. This fact is graphically illustrated in Fig. 5. Under H_0, carrier phase single differences have the same mean, their statistical nature is not altered by function (44) and the addition of the n_i^{opt} further compact them around a common mean. These arguments are used to justify the approximation according to which $\bar{y}_i|H_0$ are independent Gaussian variables with the same mean. These approximations and the result proved in [24] imply that $\Lambda|H_0$ is χ^2 distributed with $I-1$ degrees of freedom. Thus, probability (41) becomes:

$$P_{md}(T_h) = 1 - \frac{\gamma\left(\frac{I-1}{2}, \frac{T_h}{2}\right)}{\Gamma\left(\frac{I-1}{2}\right)} \tag{45}$$

where $\Gamma(\cdot)$ and $\gamma(\cdot,\cdot)$ are the Gamma and lower incomplete Gamma functions [25], respectively. Probability (45) is the complementary Cumulative Density Function (CDF) of a χ^2 random variable and can be easily inverted using efficient numerical methods. Finally, threshold, T_h is obtained by fixing a target probability of missed detection, P_{md}^{tar}, and inverting

TABLE I
PARAMETERS ADOPTED FOR THE MONTE CARLO SIMULATIONS AND THE ESTIMATION OF THE PDF OF $\Lambda|H_0$.

Parameter	Value
Number of simulation runs	10^5
Number of satellites	$I = 6$
Measurement mean	randomly selected for each simulation run, common to all measurements
Variance	common to all measurements

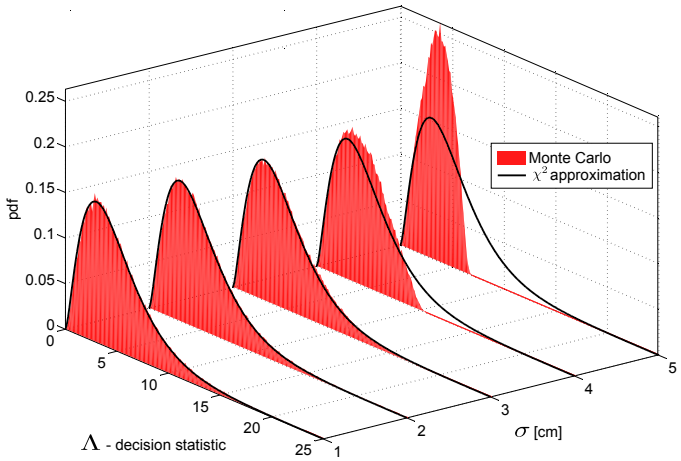


Fig. 6. Comparison between pdfs estimated through Monte Carlo simulations and theoretical χ^2 approximations for different measurement variances, σ^2. $I = 6$ measurements.

(45):

$$T_h = P_{md}^{-1}\left(P_{md}^{tar}\right). \tag{46}$$

The validity of the χ^2 approximation for $\Lambda|H_0$ is analysed in Fig. 6 using Monte Carlo simulations. In particular, signal model (4) has been used to simulate several realizations of carrier phase single differences which, in turn, have been used for the evaluation of the decision statistic, $\Lambda|H_0$. Simulations have been conducted using the parameters reported in Table I: in order to simplify the analysis, the same variance was assumed for all the measurements. Empirical pdfs have been estimated using the histogram method and compared with the theoretical pdf of a χ^2 random variable. The analysis has been conducted as a function of the measurement standard deviation, σ, which has been expressed in cm in Fig. 6. σ can be converted into cycles through division by the wavelength of GPS L1 signals, $\lambda = 19$ cm. The choice of using σ in cm is justified by the fact that it provides a more intuitive representation of the magnitude of the errors affecting carrier phase single differences. The comparison performed in Fig. 6 shows that the χ^2 approximation is valid for carrier phase single differences with standard deviations lower than 4 cm (approximately 0.2 cycles). These accuracies are easily achieved by standard GNSS receivers as shown in Section V where real GPS data are considered. For $\sigma = 4$ and $\sigma = 5$ cm, function (44) introduces aliasing effects on the pdf of the input random variables and the χ^2 approximation is no longer valid.

V. Real Data Analysis and Simulations

In this section, real data and simulations are used to support the theoretical findings described in the previous sections. Real data have been collected using the dual-antenna system described in [15] which is made of two ublox LEA-6T receivers [26] able to provide GPS carrier phase measurements. Carrier phase single differences are then constructed and used to evaluate decision statistic (33). It is noted that the evaluation of (33) requires the knowledge of the measurement variances, σ_i^2, that are in general unknown. The approach adopted here is to estimate σ_i^2 from the input measurements, (4). Although, $\frac{D}{\lambda}\cos\alpha_i + \Delta N_i$ can be considered constant over short time intervals, clock term (5) is time-varying and thus does not allow the direct estimation of the variance of $\frac{1}{\lambda}\Delta\eta_i$. For this reason, an approach based on carrier phase double differences has been developed. In particular, carrier phase double differences

$$\Delta^2\varphi_{i,j} = \Delta\varphi_i - \Delta\varphi_j \qquad i > j \tag{47}$$

are at first computed. The clock term, b, disappears in double differences (47) and

$$\sigma^2_{i,j} = \mathrm{Var}\left\{\Delta^2\varphi_{i,j}\right\} = \mathrm{Var}\left\{\Delta\varphi_i\right\} + \mathrm{Var}\left\{\Delta\varphi_j\right\} = \sigma_i^2 + \sigma_j^2. \tag{48}$$

Carrier phase double differences can be computed from the vector of carrier phase single differences using the combining matrix, H, defined in Appendix B. When I measurements are available, $M = \frac{I(I-1)}{2}$ double differences can be computed and H has size $(M \times I)$. Since the clock term, b, has been removed it is finally possible to estimate the variances of the carrier phase double differences using for example the standard sample variance estimator [21]. At this point, a vector of M estimated variances

$$S_d = \begin{bmatrix} \hat\sigma^2_{0,1} \\ \hat\sigma^2_{0,2} \\ \vdots \\ \hat\sigma^2_{I-2,I-1} \end{bmatrix} \tag{49}$$

is obtained. Symbol "$\hat{}$" is used to indicate that the quantities considered have been estimated. Finally, the variances of the carrier phase single differences are obtained as

$$\begin{bmatrix} \hat\sigma^2_0 \\ \hat\sigma^2_1 \\ \vdots \\ \hat\sigma^2_{I-1} \end{bmatrix} = \left(G^T G\right)^{-1} G^T S_d \tag{50}$$

where G is the matrix defined in Appendix B and accounts for relationship (48). This approach can be implemented using the procedure detailed in Fig. 7 and it is suitable for real-time applications. More specifically, variances (49) can be determined using a sequential estimator or considering only the N most recent carrier phase double differences. In the experiments performed, $N = 60$ was used to estimate the sample variances. In this way, the expectation time is sufficiently short to make the geometric change of the mean value of the double differences negligible. This technique is a "M-cornered hat" approach [27] which is usually adopted to estimate the Allan variance of individual oscillators.

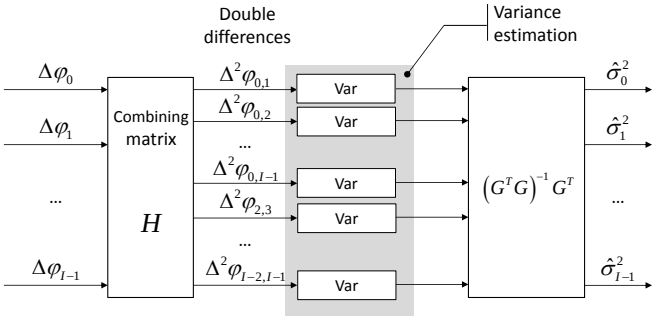


Fig. 7. Schematic representation of the procedure adopted for estimating the variances of the carrier phase single differences.

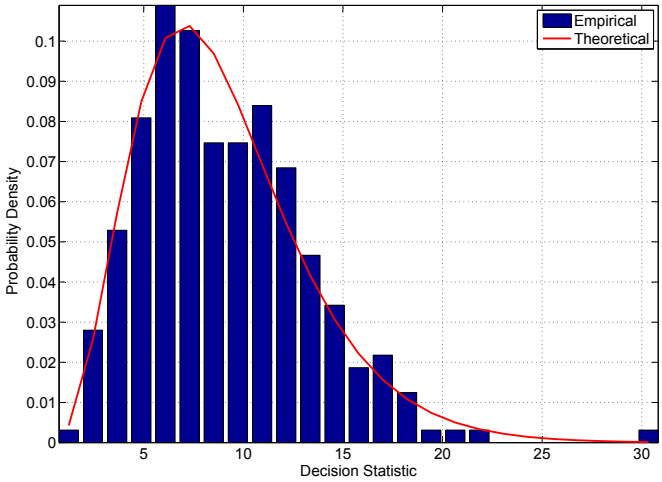


Fig. 8. Histogram of the SoS decision statistic evaluated using real data collected in an anechoic chamber. The experiment reproduces a spoofing attack.

Using the estimated variances, it is finally possible to compute decision statistic (33). Sample results obtained using carrier phase measurements from the dual-antenna system mentioned above are provided in Figs. 8 and 9. In the experiment considered in Fig. 8, data were collected in a large anechoic chamber where GPS signals were broadcast from a single antenna. In this case, all the signals were from the same direction and the experiment reproduced the case of a spoofing attack. The ublox receivers were able to process 10 signals which were characterized by C/N_0 values greater then 40 dB-Hz. The scenario considered reproduced open-sky conditions and thus good satellite visibility and high signal strengths were obtained. Under such favourable conditions, estimated standard deviations were less than 1 mm. Thus, hypothesis (15) was meet. Five minutes of data were collected at 1 Hz rate and carrier phase single differences were used to estimate the histogram of the SoS decision statistic. The histogram in Fig. 8 approximately follows a χ^2 distribution further supporting the theoretical and simulation results provided in the previous sections.

A second experiment which consider data collected under normal operating conditions is analysed in Fig. 9. The histogram

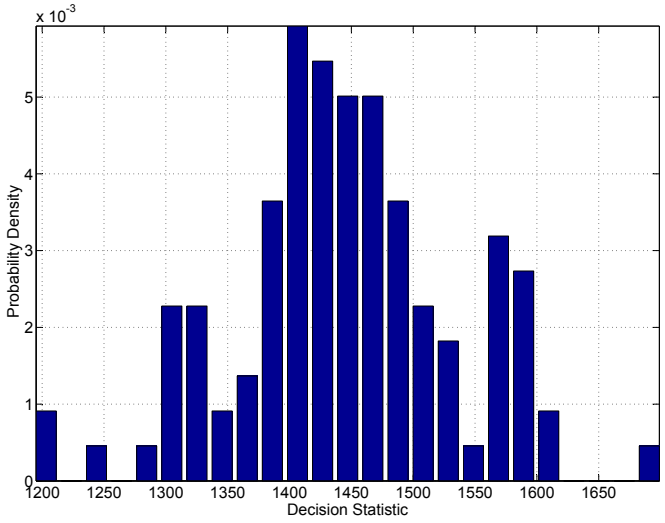


Fig. 9. Histogram of the SoS decision statistic evaluated using real data collected in an open-sky scenario. The experiment reproduces normal operating conditions.

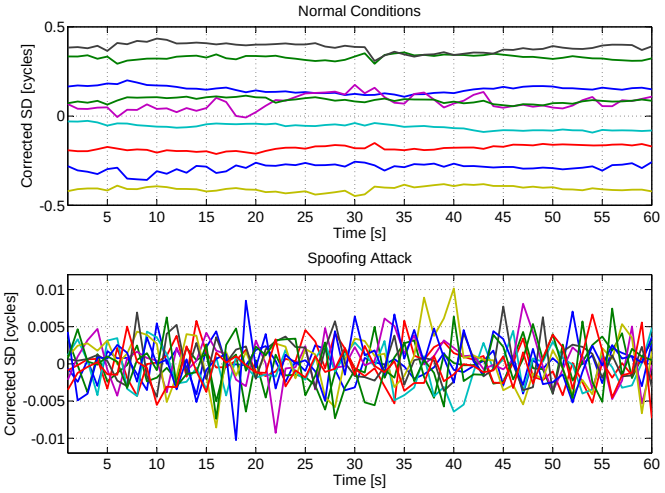


Fig. 10. Comparison between carrier phase single differences under normal and spoofing conditions. Carrier phase single differences have been corrected using $\hat{k}$ and operator (44).

of the SoS decision statistic was evaluated using real data collected in an open-sky scenario. In this case, 9 satellites were tracked and C/N_0 values greater than 41 dB-Hz were obtained. These signal conditions are similar to that of Fig. 8. The scenario considered in Fig. 9 is representative of the H_1 hypothesis: GPS signals are from different directions and the decision statistic does not follows a χ^2 distribution. Moreover, the SoS decision statistic assumes values greater than 1200 that are 40 times higher than those observed in Fig. 8. These results suggest that the SoS detector is able to effectively discriminate between normal operating conditions and a spoofing attack.

Carrier phase single differences under normal and spoofing conditions are further analysed in Fig. 10. In particular, $\Delta\varphi_i - \hat{k} - \text{round}(\Delta\varphi_i - \hat{k})$ are shown for the two cases considered in Figs. 8 and 9. Under normal conditions, corrected carrier phase single differences are scattered in the whole range $(-0.5, 0.5]$

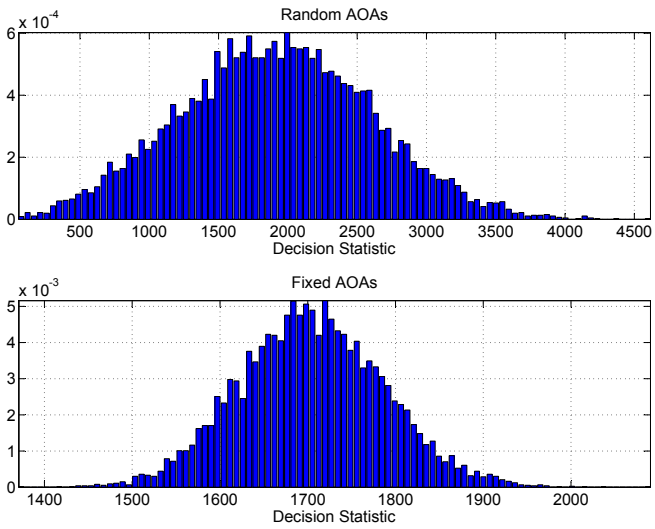


Fig. 11. Empirical pdfs (histograms) of the decision statistic, Λ, under H_1. Two cases are considered: in the upper part, the AOAs of the different signals are randomly selected. In the bottom part, the AOAs are fixed and correspond to the values in the upper plot of Fig. 10. $I = 9$, $\sigma = 0.1$ cm.

whereas they are concentrated around zero under H_0. This fact is an additional indication of the validity of the approach developed.

Real data results have been complemented using simulations. In particular, Monte Carlo simulations have been used to characterize the performance of the SoS detector under H_1 and evaluate its false alarm rate. In this case, different AOAs were selected in order to simulate normal operating conditions. The empirical pdfs (histograms) of the decision static, $\Lambda|H_1$, are shown in Fig. 11. Two cases are considered: in the upper part of the figure, the AOAs of the different signals are randomly selected. This implies that geometry conditions are randomly changed at each simulation run and thus the resulting histogram is an average with respect to different geometry conditions. The pdf of $\Lambda|H_1$ is spread over a large support and is significantly separated from the pdfs considered in Fig. 6. The case where the AOAs are fixed is considered in the bottom part of Fig. 11. In particular, the AOA have been selected to mimic the same geometry conditions considered in Fig. 9 and in the upper part of Fig. 10. This choice was performed in order to be able to compare empirical and simulation results. In both cases in Fig. 11, $I = 9$ and $\sigma = 0.1$ cm were adopted: these values correspond to the ones obtained during the experiment considered in Fig. 9. The histogram in the bottom part of Fig. 11 is consistent with the results reported in Fig. 9 and the residual differences are due to the reduced number of measurements considered in Fig. 9 and by the fact that homoscedastic conditions are assumed for the simulations.

The performance of the SoS detector is further analyzed in Fig. 12 which shows the Receiver Operating Characteristics (ROCs) [17] obtained for $I = 6$ and for different measurement standard deviations. ROCs are the plot of the detection probability as a function of the false alarm rate [17]. The detection probability is the complementary probability of P_{md} which is provided in closed form in (45) and which is fixed by the

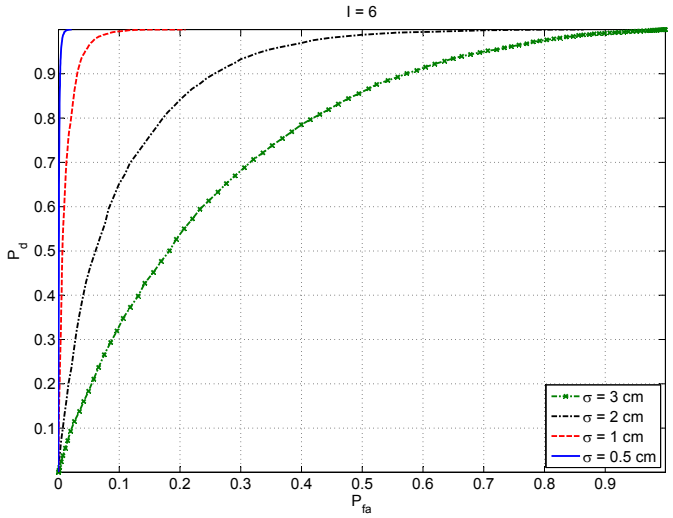


Fig. 12. ROCs of the SoS detector for $I = 6$ and for different measurement deviations. The AOAs of the different signals are randomly selected.

decision threshold, T_h. A false alarm occurs when a spoofing attack is incorrectly declared and the associated probability is obtained by integrating the pdfs considered in Fig. 11. ROCs have been obtained considering random AOAs as for the evaluation of the upper histogram in Fig. 11: thus they represent the average behaviour with respect to the different geometry conditions. In Fig. 12, large measurement variances are considered to analyze the detector performance under challenging conditions. Moreover, for more realistic scenarios, for example for $\sigma = 0.1$ cm, ROC curves saturate on the upper left corner of the plot confirming the good performance of the SoS detector. This effect can be already noted for $\sigma = 0.5$ cm which is considered in Fig. 12: very large probabilities of detection are obtained even for false alarm rates close to zero. As expected, the detector performance increases as the noise variance decreases.

These results support the effectiveness of the approach proposed.

VI. Conclusions

The class of SoS detectors have been derived using the GLRT approach. Differently from previous approaches, the cycle ambiguities affecting carrier phase measurements have been modelled as random variables and not as constants to be estimated. This design choice has led to a new class of detectors, which can be expressed as the sum of squared carrier phase single differences corrected for a pseudo-mean and for their integer parts. The detector derived has a simple form and thus is suitable for real-time applications. The theoretical characterization of the detector has led to a simple criterion for fixing the decision threshold: empirical methods and extensive Monte Carlo simulations are no longer required for setting the threshold further simplifying the algorithm implementation. Monte Carlo simulations and real data analysis support the theoretical findings and show the effectiveness of the SoS approach for discriminating between normal operations and a spoofing attack.

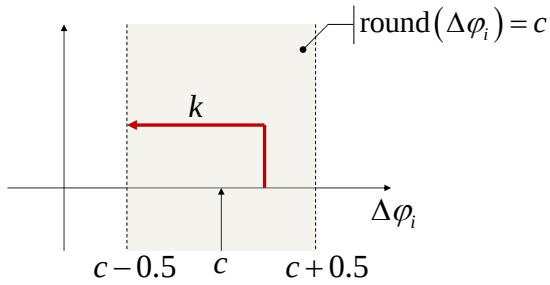


Fig. 13. Graphical justification of properties (51) and (52). The symbol c is used to denote an integer constant.

Appendix A
Evaluation of $\hat{k}|H_0$

In this appendix, a procedure for the evaluation of $\hat{k}|H_0$ is described. As mentioned in Section III-A, cost function (22) is periodic in k with period 1 cycle. This periodicity is due to the presence of the round$(\cdot)$ operator. Thus, it is possible to simplify the optimization problem by constraining k in a specific interval. In this case, the interval $[0, 1)$ is selected. This choice is particularly convenient since for $k \in [0, 1)$

$$\text{round}(\Delta\varphi_i - k) = \text{round}(\Delta\varphi_i) - n_i \tag{51}$$

where

$$n_i = \begin{cases} 0 & \text{if } k < \Delta\varphi_i - \text{round}(\Delta\varphi_i) + 0.5 \\ 1 & \text{if } k > \Delta\varphi_i - \text{round}(\Delta\varphi_i) + 0.5 \end{cases} . \tag{52}$$

Properties (51) and (52) are graphically justified in Fig. 13: k does not change the value of round$(\Delta\varphi_i - k)$ unless $\Delta\varphi_i - k$ is lower than round$(\Delta\varphi_i) - 0.5$. Since k is in the interval $[0, 1)$ the maximum decrement of round$(\Delta\varphi_i - k)$ is 1 with respect to round$(\Delta\varphi_i)$. Eqs. (51) and (52) directly follow from these considerations.

Using (51), cost function (25) becomes:

$$\begin{aligned} L_l(k|H_0) &= \sum_{i=0}^{I-1} \frac{1}{\sigma_i^2} \left[(\Delta\varphi_i - k) - \text{round}\left(\Delta\varphi_i\right) + n_i \right]^2 \\ &= \sum_{i=0}^{I-1} \frac{1}{\sigma_i^2} \left[y_i - k + n_i \right]^2 \end{aligned} \tag{53}$$

where

$$y_i = \Delta\varphi_i - \text{round}\left(\Delta\varphi_i\right). \tag{54}$$

Similarly to the cost function considered by [3], (53) is piecewise quadratic and the intervals where $L_l(k|H_0)$ is purely quadratic are determined by the n_i and condition (52). The intervals considered here are different from those determined in [3] for the adoption of different constraints on the cost function and on the interval selected for k. Using these premises, it is finally possible to determine $\hat{k}|H_0$. In particular, let $y_{(i)}$ be the ith order statistic of the set $\{y_i\}_{i=0}^{I-1}$ where

- $y_{(0)} = \min\{y_0, y_1, ..., y_{I-1}\}$ is the smallest carrier phase single difference corrected for its closest integer
- $y_{(I-1)} = \max\{y_0, y_1, ..., y_{I-1}\}$ is the largest of the y_i
- $y_{(i)}$ is the $(i+1)$th smallest corrected measurement

and define the shifted version of $y_{(i)}$ as

$$m_{(i)} = y_{(i)} + 0.5. \tag{55}$$

From (54), it follows that

$$0 \leq m_{(i)} < 1 \tag{56}$$

and the set $\{m_{(i)}\}_{i=0}^{I-1}$ can be completed by introducing

$$m_{(-1)} = 0, \qquad m_{(I)} = 1. \tag{57}$$

Using these definitions it is possible to determine the intervals

$$I_i = [m_{(i-1)}, m_{(i)}], \text{ for } i = 0, 1, ..., I. \tag{58}$$

The way intervals (58) have been constructed implies that the binary terms, $\{n_i\}_{i=0}^{I-1}$, are constant inside each interval. In particular, changes in the $\{n_i\}_{i=0}^{I-1}$ occur only at the interval boundaries, $m_{(i)}$. Thus, cost function (53) is quadratic on each interval, I_i. For each interval, $\{n_i\}_{i=0}^{I-1}$ can be computed using (51) and replacing k with any value lying inside the interval considered. In particular,

$$n_i^j = \text{round}(\Delta\varphi_i) - \text{round}(\Delta\varphi_i - k_j^c) \tag{59}$$

where the index j has been introduced to denote the fact that n_i, the binary constant associated to the ith carrier phase single difference, has been computed considering the jth interval, I_j. k_j^c in (59) denotes the centre of the jth interval:

$$k_j^c = \frac{m_{(j-1)} + m_{(j)}}{2}. \tag{60}$$

Thus, for each interval it is possible to evaluate a local minimum of $L_l(k|H_0)$:

$$\hat{k}_j = \sum_{i=0}^{I-1} w_i(y_i + n_i^j). \tag{61}$$

where $\{w_i\}_{i=0}^{I-1}$ are the weights defined in (28). Eq. (61) is obtained by setting to zero the first derivative of (53) and fixing $n_i = n_i^j$. The global minimum is one of the local minima determined in (61) and can be found by simple inspection. Note that if the local minimum, $\hat{k}_j$, computed considering the jth interval, does not belong to I_j, then it is possible to show that $\hat{k}_j$ is not an acceptable solution and that the global minimum of $L_l(k|H_0)$ does not belong to I_j. This property derives from considerations on the left and right derivatives of $L_l(k|H_0)$ at the transition points $\{m_{(i)}\}_{i=-1}^{I}$. Thus, it is possible to show that $L_l(k|H_0)$ has at most I local minima in the interval $[0, 1)$.

An example of log-likelihood function, $L_l(k|H_0)$, is provided in Fig. 14. The global minimum, $\hat{k}|H_0$, is one of the local minima determined in (61) and thus can be expressed as in (27) where the binary terms, n_{opt}^j, are equal to the n_i^j of the interval containing the global minimum. In interval I_3 in Fig. 14, $L_l(k|H_0)$ does not have a local minimum of form (61) and assumes its lowest value at the boundary point, m_3. In such conditions, it is possible to show that both left and right derivatives of $L_l(k|H_0)$ are negative and thus m_3 cannot be a minimum of $L_l(k|H_0)$. Similar considerations can be made when $L_l(k|H_0)$ is increasing on the whole interval under consideration.

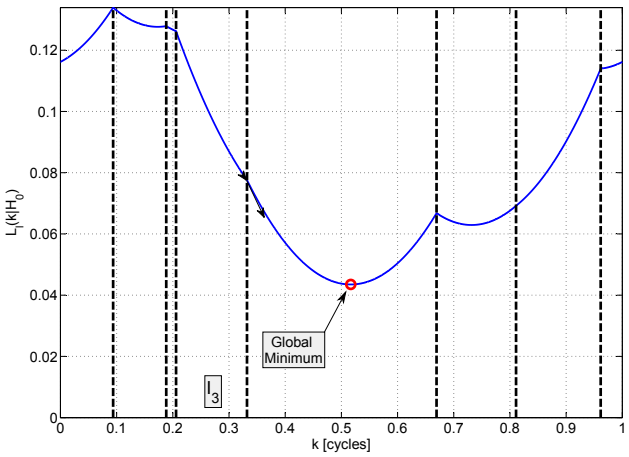


Fig. 14. Minimization of the log-likelihood function $L_l(k|H_0)$.

APPENDIX B
DIFFERENCE MATRIX H

When I measurements are available, $M = \binom{I}{2} = \frac{I(I-1)}{2}$ pairs can be formed. There are thus $M = \frac{I(I-1)}{2}$ unique carrier phase double differences which can be computed using the H matrix defined below. H is an $M \times I$ matrix which can be decomposed in $(I-1)$ sub-matrices:

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \cdots \\ H_{I-1} \end{bmatrix} \tag{62}$$

where H_i has size $(I-i) \times I$ and accounts for the differences between the ith and jth measurement with $j > i$. Each sub-matrix can be written as

$$H_i = \begin{bmatrix} \mathbf{0}_{(I-i,i-1)} & \mathbf{1}_{I-i} & -\mathbb{I}_{(I-i)} \end{bmatrix} \tag{63}$$

where $\mathbf{0}_{(a,b)}$ denotes a $(a \times b)$ matrix with zeros as entries, $\mathbf{1}_c$ is a column vector with c elements all equal to 1 and $\mathbb{I}_d$ is the identity matrix of size d.

H can be used to compute carrier phase double differences from the carrier phase single differences available. Carrier phase double differences can then be used to estimate composite variances that, in turn, can be used to compute the variances of carrier phase single differences. This can be done by using the pseudo-inverse of the G matrix defined similarly to H as

$$G = \begin{bmatrix} G_1 \\ G_2 \\ \cdots \\ G_{I-1} \end{bmatrix} \tag{64}$$

where

$$G_i = \begin{bmatrix} \mathbf{0}_{(I-i,i-1)} & \mathbf{1}_{I-i} & \mathbb{I}_{(I-i)} \end{bmatrix}. \tag{65}$$

With respect to (63), the minus sign in front of the identity matrix has been removed to account for (48).

REFERENCES

[1] Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., and Lachapelle, G., "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, no. Article ID 127072, pp. 1–16, May 2012.

[2] Günther, C., "A survey of spoofing and counter-measures," *NAVIGATION, Journal of The Institute of Navigation*, vol. 61, no. 3, pp. 159–177, Fall 2014.

[3] Psiaki, M. L., O'Hanlon, B. W., Powell, S. P., Bhatti, J. A., Wesson, K. D., Humphreys, T. E., and Schofield, A., "GNSS spoofing detection using two-antenna differential carrier phase," in *Proc. of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*, Tampa, Florida, Sep. 2014, pp. 2776–2800.

[4] Wen, H., Huan, P. Y.-R., Dyer, J., Archinal, A., and Fagan, J., "Countermeasures for GPS signal spoofing," in *Proc. of the ION GNSS'05*, Long Beach, CA, September 2005, pp. 1285–1290.

[5] Wesson, K., Rothlisberger, M., and Humphreys, T., "Practical cryptographic civil gps signal authentication," *NAVIGATION, Journal of The Institute of Navigation*, vol. 59, no. 3, pp. 177–193, Fall 2012.

[6] Humphreys, T. E., "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

[7] Scott, L., "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proc. of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS)*, Portland, OR, Sep. 2003, pp. 1543–1552.

[8] Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., and Humphreys, T. E., "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2250–2267, Oct. 2013.

[9] Wesson, K. D., Rothlisberger, M. P., and Humphreys, T. E., "A proposed navigation message authentication implementation for civil GPS anti-spoofing," in *Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, Portland, OR, Sep. 2011, pp. 3129 – 3140.

[10] Wesson, K. D., Shepard, D. P., Bhatti, J. A., and Humphreys, T. E., "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, Portland, OR, Sep. 2011, pp. 2646 – 2656.

[11] Montgomery, P. Y., Humphreys, T. E., and Ledvina, B. M., "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proc. of the International Technical Meeting of The Institute of Navigation*, Anaheim, CA, Jan. 2009, pp. 124 – 130.

[12] Broumandan, A., Jafarnia-Jahromi, A., V.,, Dehghanian,, Nielsen, J., and Lachapelle, G., "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proc. of the IEEE/ION Position Location and Navigation Symposium (PLANS)*, Apr. 2012, pp. 479–487.

[13] Akos, D. M., "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *NAVIGATION, Journal of the Institute of Navigation*, vol. 59, no. 4, pp. 281 – 290, Winter 281-290.

[14] Hartman, R., "Spoofing detection system for a satellite positioning system," Patent, Sep., 1996.

[15] Borio, D. and Gioia, C., "A dual-antenna spoofing detection system using GNSS commercial receivers," in *Proc. of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*, Tampa, Florida, *sep* 2015, pp. 1–6.

[16] Kaplan, E. D. and Hegarty, C., Eds., *Understanding GPS: Principles and Applications, Second Edition*, 2nd ed. Artech House, November 2005.

[17] Kay, S., *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*. Prentice Hall, Feb. 1998, vol. 2.

[18] Hoffmann-Wellenhof, B., Lichtenegger, H., and Collins, J., *Global Positioning System: Theory and Practice*, 2nd ed. Springer, Apr. 1992.

[19] Arce, G. R., *Nonlinear Signal Processing: A Statistical Approach*. Wiley-Interscience, Nov. 2004.

[20] Huber, P. J. and Ronchetti, E. M., *Robust Statistics*, 2nd ed. John Wiley & Sons, Feb. 2009.

[21] Casella, G. and Berger, R. L., *Statistical Inference*, 2nd ed. Duxbury Press, june 2001.

[22] Mason, R. L., Gunst, R. F., and Hess, J. L., *Statistical Design and Analysis of Experiments, with Applications to Engineering and Science*, 2nd ed. Wiley-Interscience, Feb. 2003.

[23] Borio, D., "PANOVA tests and their application to GNSS spoofing detection," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 1, pp. 381–394, Jan. 2013.

[24] Irwin, J. O., "On the distribution of a weighted estimate of variance and on analysis of variance in certain cases of unequal weighting," *Journal of the Royal Statistical Society*, vol. 105, no. 2, pp. 115–118, 1942. [Online]. Available: http://www.jstor.org/stable/2980611

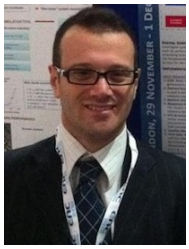
[25] Abramowitz, M. and Stegun, I. A., Eds., *Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables*, ser. Dover Books on Mathematics. Dover Publications, Jun. 1965.

[26] *u-blox 6 Receiver Description Including Protocol Specification*, ublox AG, Thalwil, Switzerland, Apr. 2013.

[27] Riley, W. J., *Handbook of Frequency Stability Analysis*, ser. NIST Special Publications. Boulder, CO: National Institute of Standards and Technology (NIST), Jul. 2008.

BIOGRAPHIES

D aniele Borio received the M.S. and the Ph.D degree in Communications Engineering from Politecnico di Torino, Italy in 2004 and 2008, respectively. From January 2008 to September 2010, he was a senior research associate in the PLAN group of the University of Calgary, Canada. He is currently a scientific and policy officer at the Joint Research Centre of the European Commission in the fields of digital and wireless communications, location and navigation.



C iro Gioia received the M.S. degree in Nautical Sciences from Parthenope University, Italy, in 2009. In April 2014, he successfully defended his PhD thesis at the same University. From May 2013 to April 2014, he was a visiting student at the European Commission Joint Research Centre (JRC). Since May 2014 he has been working for Piksel s.p.a., Milano, Italy. His research interests focus on location and navigation with special emphasis on geomatics aspects.