Detection of GNSS Spoofing by a Receiver in Space via Fusion of Consistency Metrics

Publisher:
Institute of Electrical and Electronics Engineers Inc.

Published version:
DOI: 10.1109/ICC40277.2020.9149061

Detection of GNSS spoofing by a receiver in space via fusion of consistency metrics

Leonardo Chiarello[*], Anna V. Guglielmi[*], Nicola Laurenti[*], Fabio Bernardi[†], Francesco Longhi[†], Samuele Fantinato[†]
[*]Dept. of Information Engineering, University of Padova, via Gradenigo 6B, 35131 Padova, Italy
email: {chiarell, guglielm, nil}@dei.unipd.it
[†]Qascom Srl, via Marinali 87, 36061 Bassano del Grappa, Vicenza, Italy
email: {fabio.bernardi, francesco.longhi, samuele.fantinato}@qascom.it

***Abstract*—We consider the problem of detecting spoofing attacks for a GNSS receiver in space, orbiting around the Earth. Since a receiver in space cannot leverage the presence of so called signals of opportunity, it must rely on detecting anomalies in the signal itself and checking the consistency of its measurements with the computed orbital position.**

We consider three different consistency checks: on the overall received GNSS signal power at the front-end; on the estimated carrier-to-noise ratio (C/N_0) for the signal coming from each satellite in view; on the final computed position at the receiver output. Moreover, we devise a fusion method that combines soft outputs from the three checks to provide a more reliable and robust detection.

The proposed techniques are tested in a realistic simulation environment showing that, although the position consistency check is by far the most reliable, the proper fusion of the soft information from all three allow to further improve the detection rates in different conditions significantly.

***Index Terms*—GNSS, security, signal integrity, space receiver, anti-spoofing, consistency check, fusion technique, GLRT, orbit propagation models, SGP4, TLE.**

I. Introduction

SATELLITES play a relevant role in several areas, such as communication, early warning systems, global broadcasting, meteorology, navigation, reconnaissance, remote sensing, and surveillance. Their services cover almost every sector, from mobile cellular communication to telemedicine, and as a consequence any interference with them could have a serious impact on the final user. Their services are a strategic asset for any country, therefore they are privileged targets for possible attacks. For this reason, new requirements are emerging aiming at optimizing physical and mechanical constraints, cost, consumption, performance, robustness, and assurance.

In the last decade, global navigation satellite systems (GNSSs) has become a major player for navigation in space. Initially designed for ground and aeronautics applications, the use in space applications has developed as a secondary unforeseen mission service, which enables the different applications, such as precise orbit determination, attitude determination, remote sensing, and tracking of lunchers or reentering spacecraft.

GNSS systems are typically vulnerable due to the fact that they have not been designed with security provisions, and only recently some systems, e.g. the European Galileo, are introducing cryptographic authentication and integrity protection mechanisms. The common unjustified assumption is that risk of space based threats is low or even negligible. However, several examples contradicting this conclusion can be found. In a maritime setup, space-based monitoring systems are regularly being jammed or spoofed by vessel operators that falsify their information to conceal their illegal activities. More in general, the huge amount of data spread through satellites makes it easy to impair accuracy and reliability with a low probability of detection. Particularly, integrity checks involving large amounts of data transferred between interested parties are needed.

In this paper, we focus on GNSS spoofing threats that are intentional interference that can mislead a target receiver to compute false position and time. The motivation for spoofing attacks arise from the pervasiveness of GNSS and their feasibility is due to the availability of both the most public civilian GNSS signal structure and the advancement in software defined radio (SDR) technology. In general, spoofing attacks are classified according to the receiver state, environment, etc. Without going too much into the details here, [2]–[4] list the most significant attack types.

Recently, research has focused on GNSS interference countermeasures and several works have been published [5]. However, current spoofing countermeasure techniques refer to scenarios in which the target receiver is placed on the ground, e.g., by using signals of opportunity and side information from other measurements systems. Our purpose is to understand how to adapt them to the receivers considering the different constraints and limitations given by the different environment, i.e., receiver in space.

The rationale of our work is based on the fact that some parameters or characteristics of GNSS satellites and GNSS signals are publicly known or at least predictable and therefore can be used to design consistency checks. Among all, some of the most common parameters are the carrier-to-noise ratio (C/N_0) and the received power. Indeed, the C/N_0 and the range of values of the GNSS power are partially predictable. Abnormal values can be considered as warning that there may be something wrong. Moreover, GNSS satellites follow orbits that are known to the receiver and that can compared to the current estimated receiver position. Indeed, by means of a model for orbit prediction the receiver should be able to estimate its orbit and, consequently, the expected power and the C/N_0. In

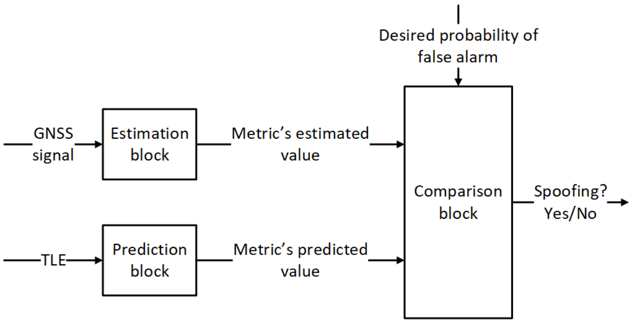


Fig. 1. General block scheme considered for the consistency checks.

this context, the purpose of this paper is to provide a statistical analysis and develop these consistency checks.

The approach described in this paper has been implemented and tested in the frame of the ENSPACE (Enhanced Navigation in Space) demonstrator (H2020-GALILEO-GSA-2017, Grant Agreement Nr. 776405). The aim of the ENSPACE project is to develop innovative software suites for enhanced navigation, positioning and time in space with the following objectives: (i) become a reference product for navigation, positioning and time in space for different missions that require low cost, security and a flexible software solution, and (ii) become a reference product for existing high-grade space applications that can be added to enhance security. With this target, the main drivers have been the design and development of a product with the following cutting edge features: multi applications, multi mission, low cost, secure and robust, and fully software solution. In [1], the implementation of the snapshot processing technique, that is one of the processing modes supported by the ENSPACE demonstrator, has been presented.

The paper is organized as follows. Section II provides the statistical analysis and the design scheme for each consistency metric checks. In Section III, the fusion technique used to merge the soft outputs of the consistency checks is presented. Section IV shows the results obtained by means of simulations. Finally, Section V concludes the paper and discuss some future perspective.

II. Consistency checks scheme

First of all, it is worth noting that even if these checks cannot be considered as cryptographic integrity protection anti-spoofing procedures, they can be seen as flags stating that a potential threat is present. The generic block scheme considered for the consistency checks is reported in Figure 1.

The aim of the estimation block is to return an estimate of a certain parameter given a number of observations. This is done exploiting the estimation theory. Let $\mathbf{Y}$ be a random vector of dimension N, whose components are Y_i, $i = 1, ..., N$, and given $\mathbf{y}$ as the vector containing the observations, y_i, $i = 1, ..., N$. It is assigned a family of probability density functions to $\mathbf{Y}$, $p_{\mathbf{Y}}(\mathbf{y}|\theta)$, parameterized by an unknown vector $\boldsymbol{\theta} \in \boldsymbol{\Theta} \subseteq \mathbb{R}^M$. The objective of parameter estimation is to use the realizations of $\mathbf{Y}$ to determine the value of $\boldsymbol{\theta}$. In particular, the true value of $\boldsymbol{\theta}$ is assumed deterministic but unknown and indicated as $\boldsymbol{\theta}_0$, defining the exact probability of $\mathbf{Y}$.

Regarding the model used for the prediction of the metrics values, the simplified general perturbations (SGP) models aim to predict satellite position and velocity. They take as input a two-line element set (TLE) and propagate the orbit from their epoch to the instant of interest. Their development began in 1960s [6] and culminated with the publication of Spacetrack Report Number 3 [7] where five propagation models are described. Among them, the SGP4 model is designed for near-Earth (period less than 225 minutes) satellites. Once the position is provided, it is possible to evaluate the predictions for any other metric needed for the consistency checks.

The aim of the comparison block is to compare the estimated and expected value for each metric to return a soft output as an indication on the distance between the two values. This is done in terms of the likelihood ratio test (LRT), that is a hypothesis test used to quantify how well two models fits a set of observations. We need to define two hypotheses

$$\begin{cases} H_0 : \widetilde{\theta} = \theta + \widetilde{w} \\ H_1 : \text{otherwise} \end{cases} \tag{1}$$

where $\widetilde{\theta}$ is the metrics expected value, $\widetilde{w}$ is the prediction noise, H_0 is the simple null hypothesis, and H_1 is the composite alternative hypothesis. Because of H_1 being composite we need to resort the generalized LRT (GLRT) [8].

The likelihood function $L(\theta|\widehat{\theta}) = p(\widehat{\theta}|\theta)$ is a function of θ with $\widehat{\theta}$ fixed to the value that is observed, i.e., the estimate. The GLRT statistic is

$$\Lambda(\widehat{\theta}) = \frac{L(\widetilde{\theta}|\widehat{\theta})}{\sup\{L(\theta|\widehat{\theta}) : \theta \in \Theta\}} = \frac{L(\widetilde{\theta}|\widehat{\theta})}{L(\widehat{\theta}|\widehat{\theta})} = \frac{p(\widehat{\theta}|\widetilde{\theta})}{p(\widehat{\theta}|\widehat{\theta})}. \tag{2}$$

The LRT provides the decision rule as follows: (i) if $\Lambda > c$, accept H_0, (ii) if $\Lambda \leq c$, reject H_0, with c representing a threshold chosen in order to obtain a specified probability of false alarm P_{fa}. In other terms,

$$P[\Lambda(\widehat{\theta}) < c] = \int_{-\infty}^{c} P[\Lambda(\widehat{\theta}) = \lambda] = P_{\text{fa}}, \tag{3}$$

with $P[\Lambda(\widehat{\theta}) = \lambda]$ the probability density function (PDF) of $\Lambda(\widehat{\theta})$ during the authentic scenario.

The following subsections will describe the algorithm for the design of the consistency checks.

A. *Position consistency check*

The position estimation is provided by the navigation solution considering as inputs the GNSS signals and the ephemeris. The position estimator block returns the receiver position $\widehat{r} = (\widehat{x}, \widehat{y}, \widehat{z})$ in earth-centered earth-fixed (ECEF) coordinates. By means of the Kolmogolov-Smirnov test with significance level $\alpha = 5\%$, we found that $\widehat{x}$, $\widehat{y}$, and $\widehat{z}$ are independent Gaussian random variables with means equal to $\widetilde{x}$, $\widetilde{y}$, $\widetilde{z}$ and variances $\sigma^2_{\widehat{x}}$, $\sigma^2_{\widehat{y}}$, $\sigma^2_{\widehat{z}}$, where $\widetilde{r} = (\widetilde{x}, \widetilde{y}, \widetilde{z})$ is the predicted position, with variances $\sigma^2_{\widetilde{x}}$, $\sigma^2_{\widetilde{y}}$, $\sigma^2_{\widetilde{z}}$. Consequently,

$$\widehat{r}' = \left[\left(\frac{\widehat{x}-\widetilde{x}}{\sqrt{\sigma^2_{\widehat{x}}+\sigma^2_{\widetilde{x}}}} \right)^2 + \left(\frac{\widehat{y}-\widetilde{y}}{\sqrt{\sigma^2_{\widehat{y}}+\sigma^2_{\widetilde{y}}}} \right)^2 + \left(\frac{\widehat{z}-\widetilde{z}}{\sqrt{\sigma^2_{\widehat{z}}+\sigma^2_{\widetilde{z}}}} \right)^2 \right]^{\frac{1}{2}} \tag{4}$$

follows a Chi distribution with parameter $k = 3$ and therefore

$$p(\widehat{r}'|\widetilde{r}) = \frac{1}{\sqrt{2}\Gamma(\frac{3}{2})}(\widehat{r}')^2 \mathrm{e}^{-\frac{(\widehat{r}')^2}{2}} . \tag{5}$$

The position predictor block takes as input the TLE of a space object and a desired prediction time, and it outputs the expected position $\widetilde{r}$ in ECEF coordinates of the receiver by means of the SGP4 model.

B. Power content consistency check

The total received power estimator block takes as input L pre-correlation samples, i.e., the samples between front-end and baseband processing blocks of a receiver, and it outputs the estimated received power $\widehat{P}_{\mathrm{rx}}$. This block assumes that the receiver has a sufficient dynamic range to avoid the need for an automatic gain control (AGC), which is a reasonable hypothesis for a receiver located in space where power variations are slow and predictable. By following the analysis done in [9], given $x(k_i), i = 1, \dots, L$ the front-end output samples, the estimated power is computed as

$$\widehat{P}_{\mathrm{rx}} = \frac{1}{L}\sum_{i=1}^{L} |x(k_i)|^2 \ . \tag{6}$$

In the case the receiver front-end is equipped with an AGC, $\widehat{P}_{\mathrm{rx}}$ can still be measured indirectly through the AGC setpoint [14].

In order to derive the probability distribution of $\widehat{P}_{\mathrm{rx}}$, the first step it to characterize the samples $x(k_i), i = 1, \dots, L$. In particular, each received sample can be written in the following form:

$$x(k_i) = \sum_{n=1}^{N_{\mathrm{s}}} A_n \mathrm{e}^{j\phi_n} C_n(k_i - \tau_n) + w(k_i) \, , \tag{7}$$

where N_{s} is the number of visible satellites, $w(k)$ is the complex additive white Gaussian noise with zero mean and variance σ^2_w. Moreover, A_n is the amplitude, ϕ_n the phase, C_n the spreading code and τ_n the code delay. By substituting Eq. 7 into Eq. 6, the total received power can be written as $P = P_1 + P_2$ (neglecting the subscript 'rx' and the $\hat{}$ for simplicity), with

$$\begin{aligned} P_1 = & \sum_{n=1}^{N_{\mathrm{s}}} A_n^2 \\ & + \frac{2}{L}\,\mathrm{Re}\left[\sum_{i=1}^{L}\sum_{n=1}^{N_{\mathrm{s}}} A_n \mathrm{e}^{j\phi_n} C_n(k_i-\tau_n) w^*(k_i) \right] \\ & \sim \mathcal{N}\left(\sum_{n=1}^{N_{\mathrm{s}}} A_n^2, \frac{n\sigma^2_w}{L} \sum_{n=1}^{N_{\mathrm{s}}} A_n^2 \right) , \end{aligned} \tag{8}$$

$$P_2 = \frac{1}{L}\sum_{i=1}^{L} |w(k_i)|^2 \sim \frac{\sigma^2_w}{2L}\chi^2(2L) \, , \tag{9}$$

where $\chi^2(2L)$ is a chi-squared distribution with $2L$ degree of freedom. The mean and the variance of the total distribution are

$$\mu_P = \mathbb{E}\left[P_1 + P_2\right] = \sum_{n=1}^{N_{\mathrm{s}}} A_n^2 + \sigma^2_w \, , \tag{10}$$

$$\sigma^2_P = \mathrm{Var}\left[P_1 + P_2\right] = \frac{\sigma^4_w}{L} + \frac{2\sigma^2_w}{L}\sum_{n=1}^{N_{\mathrm{s}}} A_n^2 \, . \tag{11}$$

As proposed in [9], converting the power in dBW (denoted with $\bar{}$ in the following), the total distribution can be modelled as a Gaussian distribution with mean and variance

$$\begin{aligned} \mu_{\bar{P}} & \approx g(\mu_P) + \frac{\ddot{g}(\mu_P)}{2}\sigma^2_P \\ & = 10\log_{10}\frac{\mu_P}{P_0} - \frac{\sigma^2_P}{2\mu^2_P} \, , \end{aligned} \tag{12}$$

$$\begin{aligned} \sigma^2_{\bar{P}} & \approx \left[\dot{g}(\mu_P)\right]^2 \sigma^2_P + \frac{\left[\ddot{g}(\mu_P)\right]^2}{4}\left(\sigma^2_P\right)^2 \\ & = 100\frac{\sigma^2_P}{\mu^2_P} + \frac{\sigma^4_P}{4\mu^4_P} \, , \end{aligned} \tag{13}$$

where $g(\cdot) = \log_{10}(\cdot/P_0)$ and $P_0 = 1\,\mathrm{W}$. Finally, the PDF of total received power can be written as

$$p\left(\bar{\widehat{P}}_{\mathrm{rx}}|\bar{\widetilde{P}}_{\mathrm{rx}}\right) = \frac{1}{\sqrt{2\pi\sigma^2_{\bar{P}}}} \mathrm{e}^{-\frac{\left(\bar{\widehat{P}}_{\mathrm{rx}}-\mu_{\bar{P}}\right)^2}{2\sigma^2_{\bar{P}}}} \, . \tag{14}$$

where $\mu_{\bar{P}}$ and $\sigma^2_{\bar{P}}$ can be derived by using the orbit prediction model.

The power predictor block takes as input the receiver position and all the GNSS satellites predicted positions in ECEF coordinates and, by means of the link budget, it outputs the expected total received power.

C. C/N_0 based consistency check

The C/N_0 estimator block takes as input N prompt correlator outputs and it returns its estimate. Hereafter, we denote the C/N_0 variable as Γ for notation simplicity. In [10], the authors have selected and investigated several signal-to-noise ratio (SNR) estimation algorithms and, based on their results, we considered four of them, that is real signal-complex noise (RSCN), signal-to-noise variance (SNV) [11], [12], moment method (MM) [11] and narrowband-wideband power ratio (NWPR) [13]. The pro-

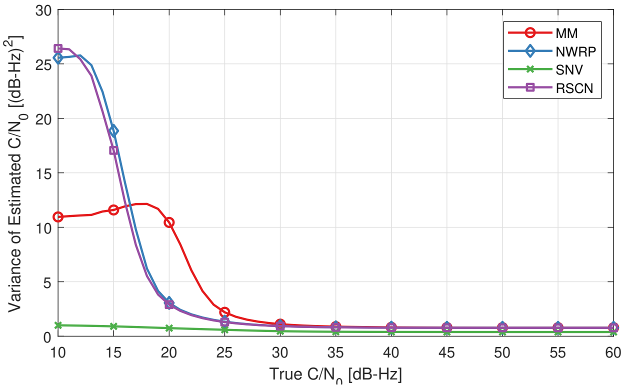


Fig. 2. Variance value for the considered C/N_0 estimators.

posed estimators are biased for some Γ values. However, since the true Γ value is evaluated by the predictor block with a certain inaccuracy, the bias from the estimated value $\widehat{\Gamma}$ can be removed defining $\widehat{\Gamma}'(dB) = \widehat{\Gamma} - \text{Bias}_{\widetilde{\Gamma}}(\widehat{\Gamma})$, with $\widetilde{\Gamma}$ the predicted value and $\text{Bias}_{\widetilde{\Gamma}}(\widehat{\Gamma}) = \text{E}_{\widetilde{\Gamma}}[\widehat{\Gamma}] - \widetilde{\Gamma}$. Therefore, the choice of the C/N_0 estimator depends only on the variance that, as it can be seen in Figure 2, is minimum for the SNV estimator.

According to the Kolmogolov-Smirnov test with significance level $\alpha = 5\%$, we found that $\widehat{\Gamma}'$ can be approximated with a Gaussian distribution with mean $\widetilde{\Gamma}$ and variance σ^2_{SNV} empirically calculated, so that

$$p(\widehat{\Gamma}'|\widetilde{\Gamma}) = \frac{1}{\sqrt{2\pi\sigma^2_{\text{SNV}}}} \mathrm{e}^{-\dfrac{(\widehat{\Gamma}' - \widetilde{\Gamma})^2}{2\sigma^2_{\text{SNV}}}}. \tag{15}$$

The C/N_0 predictor block takes as input the receiver and a GNSS satellite predicted positions in ECEF coordinates and it outputs the expected C/N_0, $\widetilde{\Gamma}$. This block performs the same steps of the total received power predictor block using the link budget formula. Then, given a certain receiver noise spectral density N_0, $\widetilde{\Gamma} = \bar{P}_{\text{rx},i} - N_0$, where $\bar{P}_{\text{rx},i}$ is the power received from the i-th satellite.

The description of the comparison block for each consistency check is missing. The reason is that its general characterization, as already discussed, can be made more specific for each check by substituting the general PDF expression with the specific PDF of the considered check.

III. Fusion technique

Each consistency check provides its own soft output that can then be combined to return a unique hard output as a flag stating that a potential threat is present. The idea is to use a method based on Dempster-Shafer theory (DST) to fuse multiple detectors as done in [15].

We followed their analysis, with the only difference that we considered the following belief function:

$$f(\Lambda_i, c_i) = \alpha f_1(\Lambda_i, c_i) + (1 - \alpha) f_2(\Lambda_i, c_i) \tag{16}$$

with

$$f_1(\Lambda_i, c_i) = \left(\frac{1}{2}\right)^{\frac{c_i}{\Lambda_i}}, \tag{17}$$

$$f_2(\Lambda_i, c_i) = \begin{cases} 1 - \frac{c_i}{2\Lambda_i} & \Lambda_i > c_i/2 \\ 0 & \Lambda_i \le c_i/2 \end{cases}, \tag{18}$$

where α is the weight of f_1.

TABLE I
Probability of false alarm for the fusion check.

$\sigma_{\widehat{x}}$, $\sigma_{\widehat{y}}$, $\sigma_{\widehat{z}}$	$\sigma_{\widetilde{x}}$, $\sigma_{\widetilde{y}}$, $\sigma_{\widetilde{z}}$	σ_{SNV}
10 m	1000 m [16]	1 dB-Hz

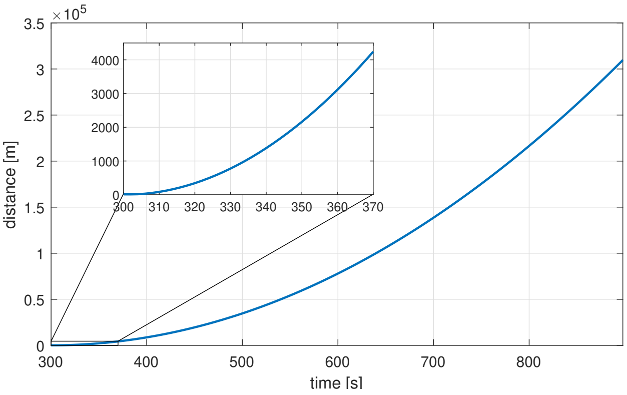


Fig. 3. Distance between spoofed and authentic position.

IV. Results

In order to test the proposed anti-spoofing mechanism, we considered a trajectory spoofing attack lasting for 15 minutes on a low Earth orbit (LEO) satellite. The spoofer starts its attack at minute 5 aligned with the authentic trajectory and it gradually diverges to the desired orbit. The values of the different variances that has been used are reported in Table I.

In Figure 3 the distance between authentic and spoofed position is shown as a function of time. Moreover, a zoomed view of the initial instants is reported, and this will be useful in understanding the performance of the position check and of the fusion technique.

In Figure 4 the difference between the spoofed and the authentic C/N_0 as a function of time is shown for all the visible satellites of the global positioning system (GPS) constellation. At every snapshot only the satellites that are visible from both the authentic and spoofed trajectories are shown. Indeed, the C/N_0 of the non-visible satellites would be undefined, so would be the difference. During all the scenario, the C/N_0 difference in the six satellites visible from both the trajectories varies between 2 dB and 6 dB. Moreover, even if the observation window is quite short, three satellites have disappeared from visibility cone

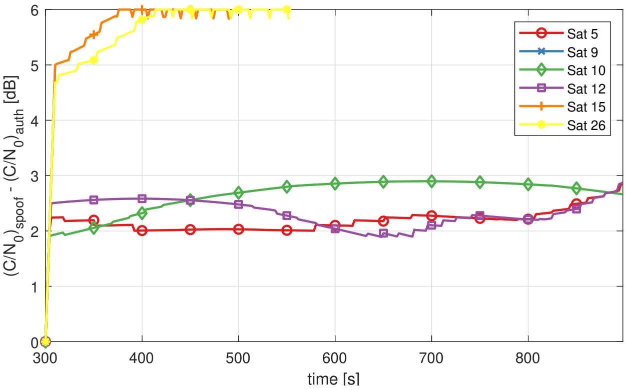


Fig. 4. Difference between spoofed and authentic C/N_0.

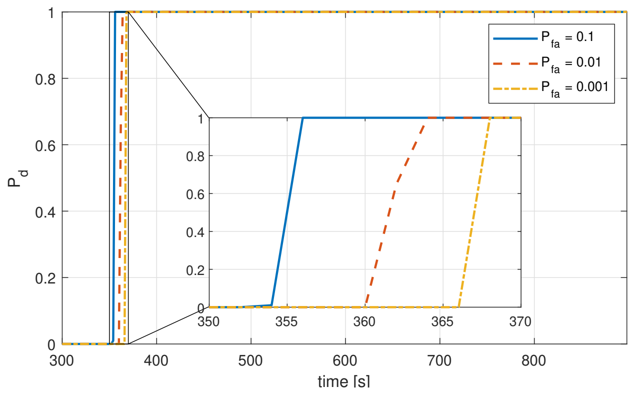


Fig. 5. Probability of detection as a function of time for the position check.

of one of the two (or both) trajectory.

The performance evaluation of the consistency checks has been carried out by fixing three target values for the false alarm probability ($P_{\mathrm{fa}} = 10^{-1}, 10^{-2}, 10^{-3}$) and by measuring the corresponding probability of detection P_{d} for all the snapshots in the scenario.

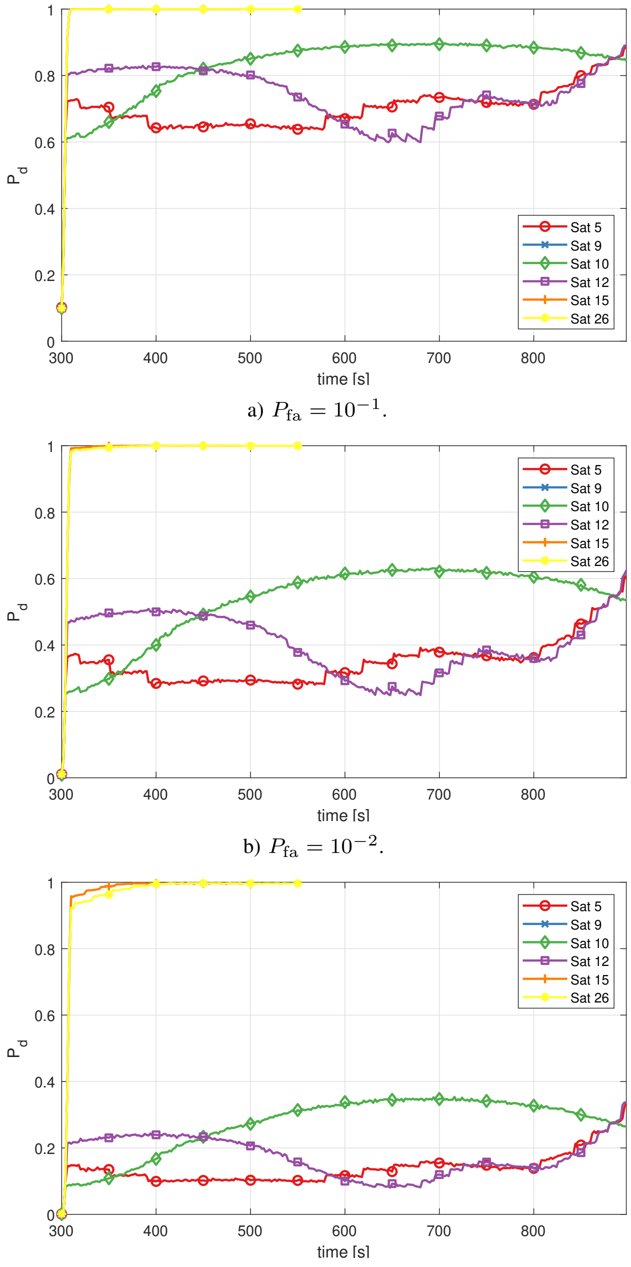
The performance of the position check is reported in Figure 5. The check works very well starting from time 370 s, while, in the previous snapshots, since the two trajectories are close to each other, the check does not detect the spoofing attack with acceptable performance.

The performance of the C/N_0 check is reported in Figure 6, for the three different probabilities of false alarm. The detection probability curves of this check mirror the trend of the curves in Figure 4. In this case, the performance related to satellites 15 and 26 are very good, while the probability of detection for the remaining four satellites are not acceptable.

The performance of the power check is reported in Figure 7. The performance is quite poor during the observation window, in particular when satellites 5, 9, 10 and 12 are the only visible satellites.

Finally, the performance of the fusion check is reported in Figure 8, where $\alpha = 0.5$ has been used. During the initial instants of spoofing the probability of detection is low (in particular during the first time instants, in which the spoofer signal is still aligned with the authentic signal) and it approaches 1 at time 342 s, when the position drift is more or less 1500 m (see Figure 3).

In this scenario the attacker makes sure that the receiver position drifts away from the authentic one very smoothly. Moreover, during the misalignment, the attacker keeps the C/N_0 of the forged signal stronger than the authentic one in order to take possession of the tracking loop, but not strong enough to be detected by the receiver with high probability. Finally, in Table II is reported the mapping between the desired P_{fa} of the single checks and the corresponding P_{fa} of the fusion checks derived empirically. It can be observed that the second ones are smaller than the first ones.



a) $P_{\mathrm{fa}} = 10^{-1}$.

b) $P_{\mathrm{fa}} = 10^{-2}$.

c) $P_{\mathrm{fa}} = 10^{-3}$.

Fig. 6. Probability of detection as a function of time for the C/N_0 check.

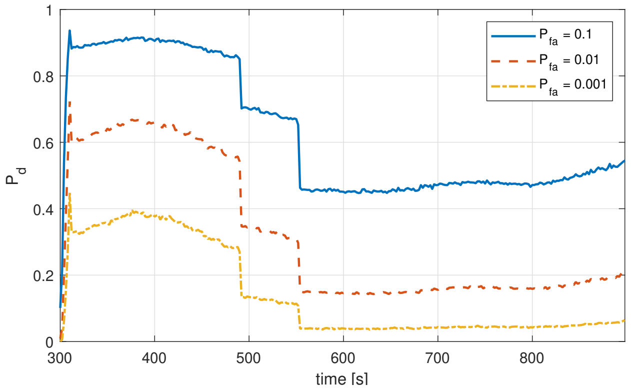


Fig. 7. Probability of detection as a function of time for the power check.

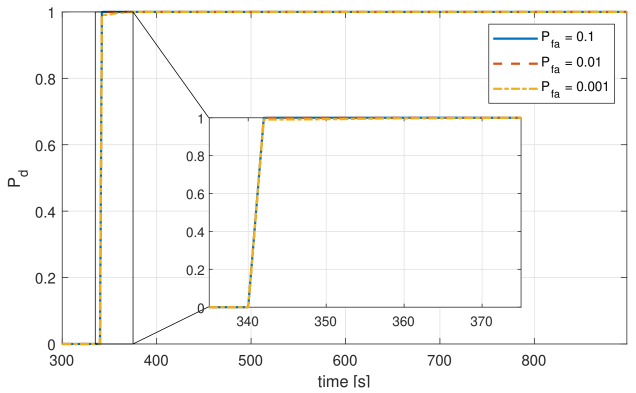


Fig. 8. Probability of detection as a function of time for the fusion check.

TABLE II
PROBABILITY OF FALSE ALARM FOR THE FUSION CHECK.

P_{fa} of the single checks	10^{-1}	10^{-2}	10^{-3}
P_{fa} of the fusion check	$6 \cdot 10^{-2}$	$2 \cdot 10^{-3}$	10^{-4}

V. Conclusion

In the framework of securing GNSS services, much attention has been given to ground applications, whereas few requirements are considered for the protection and robustness enhancement of space based GNSS receivers, that is the scenario considered in this work.

A spoofing detection mechanism based on the consistency check of three different metrics (position, C/N_0 and total received power) has been developed. In particular, the metric value estimated from the GNSS signal and the one predicted using an orbit propagation model are compared by means of the GLRT. Then, the soft detection results of the single checks are fused together to provide a spoofing decision.

The proposed mechanism has been tested on a trajectory spoofing scenario for a LEO satellite. The performance of the position check is very good only when the position drift imposed by the attacker is at least $4000\ \mathrm{m}$; this is due to the low precision of the orbit propagation model. On the other hand, the C/N_0 check is effective only for the satellites for which the spoofing signal is $6\ \mathrm{dB}$ more powerful than the expected authentic signal. As regards the total received power check, its usefulness is limited, apart from preventing the attacker from using a high power spoofing signal and capture the receiver tracking loop to lock onto it. Finally, the performance of the fusion check is close to that of the position check when the latter performs well. However, it exhibits very good performance also for a position drift as low as $1500\ \mathrm{m}$.

As a future work, it might be useful not only to compare the actual values with their current estimations, but also with their past estimations. Indeed, satellites move uniformly, therefore it is reasonable that the estimated values change smoothly and any discontinuity may be a sign of anomaly. Moreover, composite security requirements can be formulated that take into account different weights for orbit displacement in different directions (for example, the drift on the radial and on the cross-track directions vs that on the along-track direction). Finally, the proposed mechanism should be tested for satellites that orbit on the medium Earth orbit (MEO) and, in particular, on the geostationary orbit (GEO), that is above the GNSS satellites orbits.

Acknowledgment

This work was funded by the European GNSS Agency (GSA) under the *Enhanced Navigation in Space (ENSPACE)* project (H2020-GALILEO-GSA-2017, Grant Agreement Nr. 776405).

References

[1] S. Fantinato, G. Da Broi, F. Bernardi, A. Dalla Chiara, O. Pozzobon, A.V. Guglielmi, N. Laurenti, *Emerging applications of snapshot navigation in space,* NAVITEC, 2018.

[2] Ioannides et al., *Known vulnerabilities of global navigation satellite systems. Status and potential mitigation techniques,* Proc. of the IEEE, 2016.

[3] Psiaki et al., *GNSS spoofing and detection,* Proc. of the IEEE, 2016.

[4] Moeness et al., *Vulnerabilities, threats, and authentication in satellite-based navigation systems,* Proc. of the IEEE, 2016.

[5] Xiao et al., *GNSS receiver anti-spoofing techniques: a review and future prospects,* Springer Electronics, Communications and Networks V, 2016.

[6] M. H. Lane, *The development of an artificial satellite theory using a power-law atmospheric density representation,* in 2nd Aerospace Sciences Meeting, New York, NY, USA, 1965.

[7] F. R. Hoots, R. L. Roehrich and T. Kelso, *Spacetrack report no. 3,* Project Spacetrack Reports, Office of Astrodynamics, Aerospace Defense Center, ADC/DO6, Peterson AFB, CO, vol. 80914, p. 14, 1980.

[8] S. M. Kay, *Fundamentals of statistical signal processing, volume II: detection theory,* Prentice Hall, 1993.

[9] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, *GNSS signal authentication via power and distortion monitoring,* IEEE Transactions on Aerospace and Electronic Systems, vol. 54, n. 2, pp. 739–754, 2018.

[10] E. Falletti, M. Pini, and L. Lo Presti, *Low complexity carrier-to-noise ratio estimators for GNSS digital receivers,* IEEE transactions on aerospace and electronic systems, vol. 47, n. 1, pp. 420–437, 2011.

[11] D.R. Pauluzzi, and N. C. Beaulieu, *A comparison of SNR estimation techniques for the AWGN channel,* IEEE Transactions on communications, vol. 48, n. 10, pp. 1681–1691, 2000

[12] N. C. Beaulieu, A. S. Toms, and D. R. Pauluzzi, *Comparison of four SNR estimators for QPSK modulations,* IEEE Communications Letters, vol. 4, n. 2, pp. 43–45, 2000

[13] A. J. Van Dierendonck, GPS receivers. In B. W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge (Eds.), *Global positioning system: theory and applications,* vol. 1, AIAA, Reston, VA, 1996

[14] D. M. Akos, *Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC),* Navigation: Journal of the Institute of Navigation, vol. 59, n. 4, pp. 281–290, 2012.

[15] H. Tao, H. Li, M. and Lu, *A method of detections' fusion for GNSS anti-spoofing,* Sensors, vol. 16, n. 12, 2016.

[16] S. Aida, and M. Kirschner, *Accuracy assessment of SGP4 orbit information conversion into osculating elements,* Sixth European Conference on Space Debris, ESA/ESOC, Darmstadt, Germany, pp. 22–25, 2013