HOSTED BY
ELSEVIER

CrossMark

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 2 (2016) 37–40

www.elsevier.com/locate/icte

GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky[☆]

Jie Huang[a], Letizia Lo Presti[a], Beatrice Motella[b,*], Marco Pini[b]

[a] Department of Electronics and Telecommunications, Politecnico di Torino, Torino, Italy
[b] Navigation Technologies, Istituto Superiore Mario Boella, Torino, Italy

Received 21 October 2015; received in revised form 25 January 2016; accepted 5 February 2016
Available online 15 February 2016

Abstract

Nowadays more and more applications rely on the information provided by Global Navigation Satellite Systems (GNSSs), but the vulnerability of GNSS signals to interference, jamming and spoofing is a growing concern. Among all the possible sources of intentional interference, spoofing is extremely deceptive and sinister. In fact, the victim receiver may not be able to warn the user and discern between authentic and false signals. For this reason, a receiver featuring spoofing detection capabilities might become a need in many cases. Different types of spoofing detection algorithms have been presented in recent literature. One of the first, referred to as Ratio Metric, allows for the monitoring of possible distortions in the signal correlation. The effectiveness of the Ratio Test has been widely discussed and demonstrated, while in this paper we analyze its performance, proposing a mathematical model that is used to assess the false alarm and detection probabilities.

Keywords: Spoofing; Ratio Test performance; Signal Quality Monitoring (SQM); Interference detection; Tracking

1. Introduction

Global Navigation Satellite Systems (GNSSs) are widely used by civilian users in a variety of applications. GNSSs are an important aid to navigate worldwide. In addition, they are useful for land surveying, can be employed in scientific applications or used to monitor fleet of vehicles. However due to the low level of the received power and to the known signal structure, GNSS civil signals are vulnerable to both unintentional and structured interference [1].

Jamming is the deliberate in-band emission of electromagnetic radiations, while the term *spoofing* refers to the transmission of GNSS-like signals, with the intent to produce false information in the victim receiver.

Recently, an increasing concern on intentional interference has been observed within the GNSS community. In fact, over the last decade, several techniques for spoofing detection have been proposed, also encouraged by the reports of successful spoofing attacks [2]. Some of them are based on power measurements, effective in the case the spoofing signal has a power advantage with respect to the genuine signal [3]. A detection method based on the correlation of the GNSS signals received by two civilian receivers is presented in [4]. Antenna arrays are still the most robust technique, providing strong protection against spoofing attack, as they can be used to detect the Angle of Arrival (AOA) or the signal phase difference. However the additional hardware and cost make them difficult to be used in mass-market applications. Spoofing detection method based on vector tracking has been also proposed [5], but so far the complexity of vector tracking loops restricts the field of implementation. A further class of methods for spoofing detection, referred to as Signal Quality Monitoring (SQM) techniques [6], aims at detecting the attack at the tracking stage, by monitoring the correlation peak quality [7–12]. A well-known method, belonging to this class, is the Ratio Test, presented in [10]. Such a metric works at the correlators' output and monitors the shape of the correlation

* Correspondence to: via P.C. Boggio 61, 10138 Torino, Italy. Tel.: +39 011 2276 416.
E-mail address: motella@ismb.it (B. Motella).

Peer review under responsibility of The Korean Institute of Communications Information Sciences.

☆ This paper is part of a special issue entitled "Positioning Techniques and Applications" guest edited by Prof. Sunwoo Kim, Prof. Dong-Soo Han, Prof. Chansu Yu, Dr. Francesco Potorti, Prof. Seung-Hyun Kong and Prof. Shiho Kim.

http://dx.doi.org/10.1016/j.icte.2016.02.006
2405-9595/

function. To conclude this brief overview of methods to tackle spoofing, it is worth mentioning the design of new signal structures. Authors of [13] introduce the concepts and methods for achieving authentication in GNSS operations, while Ref. [14] deals with cryptographic signals.

In this work we mathematically analyze the performance of the Ratio Test, when applied for spoofing detection purposes. The paper is organized as follows: Section 2 presents a classification of spoofing attacks and introduces the Ratio Test metric. The detection strategy based on the use of the Ratio Test is explained in Section 3, and the results of the theoretical analysis are summarized in Section 4. Section 5 draws the main conclusions of the work.

2. Ratio test for spoofing detection

According to [2], the different methods for generating a spoofing attack can be grouped in three main categories: simplistic, intermediate, and sophisticated attack. A simplistic attack can be easily implemented, but can be also detected by very basic countermeasures. On the contrary, a sophisticated attack is the most effective, but the associated complexity makes its realization less likely. Finally, an intermediate spoofer receives GNSS signals, makes controlled delayed-replicas and sends them to the victim receiver. It can be very effective and sinister, also because it can be realized with few inexpensive hardware components [2].

As mentioned, this paper focuses on the Ratio Test metric for spoofing detection, that was proposed in [10]. Before entering into the details of the performance analysis, the mathematical model for the detector is presented hereafter.

The Ratio Test metric is defined in [10] as:

$$M_1[k] = \frac{I_e[k] + I_l[k]}{\varepsilon I_p[k]} \tag{1}$$

where $I_e[k]$, $I_l[k]$ and $I_p[k]$ are the early, late and prompt correlations [15,16], and ε is a constant factor, that represents the slope of the correlation function. For example, for the GPS C/A code and a correlator spacing equal to the chip duration, ε is equal to 2.

In principle the Ratio Test metric can be defined over different types of Delay Lock Loop (DLL) schemes. If a coherent DLL is adopted, $I_e[k]$, $I_l[k]$ and $I_p[k]$ are the correlator outputs. While in a non-coherent DLL two solutions are possible: either the outputs of the in-phase branch, or the output of the two combined branches. In this paper we assume to work with the in-phase branch of a non-coherent DLL. In this case, $I_e[k]$, $I_l[k]$ and $I_p[k]$ can be modeled as independently and identically distributed (iid) Gaussian process. In fact, in the integration process, the independent white noise samples of the received signal generate statistically independent outputs, whose probability density function (pdf) is Gaussian.

We assume that a GNSS receiver, equipped with an anti-spoofing module, is able to evaluate all the parameters involved in the DLL before it is attacked by a spoofer.

In particular the metric $M_1[k]$ is noisy and we assume the receiver is able to estimate its variance as well as the power of the genuine signals. Moreover, we approximate $M_1[k]$ as an iid Gaussian process. Notice that $M_1[k]$ is the ratio between two Gaussian random processes $I_{el}[k] = I_e[k] + I_l[k]$ and $I_p[k]$, which is no longer Gaussian. However, if the noise at the output of the prompt correlator is negligible, $I_p[k]$ can be approximated by a known constant, whose value mainly depends on the signal power. This approximation seems hazardous, but is quite realistic in practice, especially when the receiver works in an open sky environment, with high value of carrier to noise ratio C/N_0. Furthermore, note that an intermediate spoofing attack is less likely on degraded signals with poor C/N_0, since the spoofer would struggle to synchronize and frequency align false and genuine signals, with the risk to fail the attack.

Under this hypothesis, the metric $M_1[k]$ can be written as:

$$M_1[k] = \mu_1[k] + N_1[k] \tag{2}$$

where $\mu_1[k]$ is the mean value due to the signal component, and $N_1[k]$ is a zero mean iid Gaussian process with known variance σ_1^2, due to the noise component. The value of σ_1^2 depends on the noise power, the DLL spacing, and the shape of the correlation function, which can be directly evaluated by the receiver. In fact, σ_1^2 can be estimated at the receiver side, in particular if Software Defined Radio (SDR) technologies are adopted. In fact, SDR GNSS receivers embed significant benefits in terms of flexibility, simplifying the analysis of the signal quality at different stages of the receiver chain [17].

3. Detection strategy

Once the metric has been calculated, a strategy is needed to decide the presence or absence of a spoofing attack. One possible method is to adopt a Neyman–Pearson (NP) detector [18], which implements a binary hypothesis test able to choose between H_0 (the genuine signal only hypothesis), and H_1 (the spoofing present hypothesis). These two hypotheses can be formulated as:

$$\mu_1[k] = \begin{cases} \mu_{1,0} \rightarrow H_0 \\ \mu_{1,1} \rightarrow H_1 \end{cases} \tag{3}$$

where $\mu_1[k]$ is the metric values at the epoch k, $\mu_{1,0}$ is the ratio test in the absence of noise when there is no spoofing, $\mu_{1,1}$ is the ratio test in the absence of noise and in the presence of spoofing. Notice that, for a given receiver structure and a given GNSS signal, $\mu_{1,0}$ is constant, while $\mu_{1,1}$ depends on the characteristics of the spoofing profile. In general we can affirm that the attack is effective if the correlation distortion reaches well defined values in the initial phase of the attack to force the tracking loops to unlock the genuine signals. $\mu_{1,1}$ can be defined on the basis of the signal model adopted for the spoofing. More in detail, for an intermediate spoofing attack, $\mu_{1,1}$ depends on the ratio between the spoofing and the genuine signal power, and the relative delay between the two signals. Once the two quantities are known, we can design the parameters of a classical NP detector. In general a NP decision strategy is based on the definition of a Likelihood Ratio (LR) to be compared against a threshold γ, from which a test applied to a set of observable data can be derived. In this situation the Likelihood Ratio Test (LRT) is expressed as:

$$L\left(M_1[k]\right) = \frac{p(M_1[k]; H_1)}{p(M_1[k]; H_0)} > \gamma_{L1} \tag{4}$$

where γ_{L1} is a threshold to be set, $p(M_1[k]; H_i)$ is the probability density function of the random variable $M_1[k]$ when the hypothesis H_i is true, $i = \{0, 1\}$, and $M_1[k]$ is the quantity measured at the current epoch k. It is possible to prove that this expression leads, at each epoch k, to the LRT

$$M_1[k] > \frac{\sigma_1^2 \ln \gamma_{L1}}{\mu_{1,1} - \mu_{1,0}} + \frac{\mu_{1,1} + \mu_{1,0}}{2} = \gamma_1 \tag{5}$$

valid for $\Delta\mu = \mu_{1,1} - \mu_{1,0} > 0$. A similar expression can be obtained for $\Delta\mu < 0$. Notice that the threshold γ_1 inversely depends on the ratio

$$\rho_s = \frac{\Delta\mu}{\sigma_1} \tag{6}$$

γ_1 tends to diverge towards infinite as ρ_s approaches zero (i.e. as $\mu_{1,1}$ approaches $\mu_{1,0}$). This depends on the fact that the ratio metric is effective only if the two values $\mu_{1,1}$ and $\mu_{1,0}$ are well distinct, since they have to be used to discriminate between the two hypotheses H_0 and H_1. If $\mu_{1,1} = \mu_{1,0}$, no discrimination is possible. On the contrary, high values of ρ_s, obtained when $\Delta\mu$ is high and the noise is negligible, correspond to lower thresholds.

4. Ratio test performance: theoretical analysis

It is well known that the performance of a detector can be evaluated in terms of detection probability P_D, and false alarm probability P_{FA} [18]. A way of summarizing the detection performance of a NP detector is to plot P_D versus P_{FA}, for given values of the threshold. Such type of plot is known as Receiver Operating Characteristic (ROC), and represents a tool to design the NP detector. The NP detection method consists in fixing the value of the false alarm probability, from which the threshold γ_{L1} is obtained. The NP theorem affirms that this maximizes the detection probability [18]. In practice, in many applications, the threshold to be applied to the measured data can be directly evaluated from the given P_{FA} value.

From Eq. (1) to (5), and by analyzing the statistical characteristics of $M_1[k]$, it is possible to theoretically derive the expressions of P_{FA} and P_D:

$$\begin{aligned} P_{FA} &= \int_{\gamma_1}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left[-\frac{(x-\mu_{1,0})^2}{2\sigma_1^2}\right] dx \\ &= \frac{1}{2}\operatorname{erfc}\left(\frac{\gamma_1 - \mu_{1,0}}{\sqrt{2}\sigma_1}\right) \\ P_D &= \int_{\gamma_1}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left[-\frac{(x-\mu_{1,1})^2}{2\sigma_1^2}\right] dx \\ &= \frac{1}{2}\operatorname{erfc}\left(\frac{\gamma_1 - \mu_{1,1}}{\sqrt{2}\sigma_1}\right). \end{aligned} \tag{7}$$

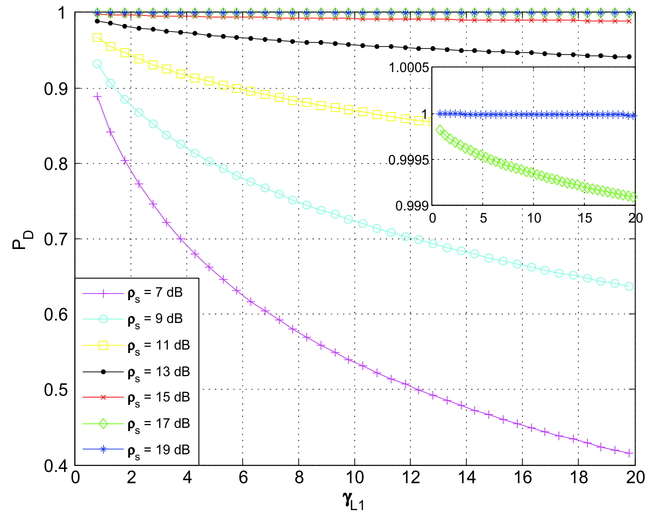

Fig. 1. P_D versus L1 for different values of ρ_s (from 7 dB to 19 dB).

In addition, it is easy to demonstrate that

$$\begin{aligned} \gamma_1 - \mu_{1,0} &= \frac{\sigma_1^2 \ln \gamma_{L1}}{\Delta\mu} + \frac{\Delta\mu}{2} \\ \gamma_1 - \mu_{1,1} &= \frac{\sigma_1^2 \ln \gamma_{L1}}{\Delta\mu} - \frac{\Delta\mu}{2} \end{aligned} \tag{8}$$

where $\Delta\mu$, introduced after Eq. (5) represents the discrimination interval between two situations: the presence and the absence of spoofing.

Finally,

$$\begin{aligned} P_{FA} &= \frac{1}{2}\operatorname{erfc}\left(\frac{\ln \gamma_{L1}}{\sqrt{2}\rho_s} + \frac{\rho_s}{2\sqrt{2}}\right) \\ P_D &= \frac{1}{2}\operatorname{erfc}\left(\frac{\ln \gamma_{L1}}{\sqrt{2}\rho_s} - \frac{\rho_s}{2\sqrt{2}}\right). \end{aligned} \tag{9}$$

In Fig. 1 the detection probability is plotted as a function of γ_{L1} for different values of ρ_s. Note that the curves tend to become flat, as ρ_s increases. Similarly, for lower values of ρ_s, both the detection probability and the false alarm probability decrease rapidly.

The results are represented in terms of ROC in Fig. 2. Each curve is plotted for a given ρ_s and by varying γ_{L1}. In our case, in fact, the ROC curves can be easily evaluated, since our random quantities are approximated as Gaussian variables with known parameters. This means that any desired value of (P_D, P_{FA}) can be selected and the corresponding threshold derived.

5. Conclusions and future work

This paper analyzes the performance of the Ratio Test when it is used as spoofing detector. The Ratio Test is a known metric, that is employed in GNSS signals quality monitoring to detect distortions of the signal correlation. In this paper we introduced a mathematical model used to evaluate the Ratio Test performance, in terms of probability of detection and probability of false alarm.

After recalling the main characteristics of the detection strategy, the paper reports the mathematical analysis and derives

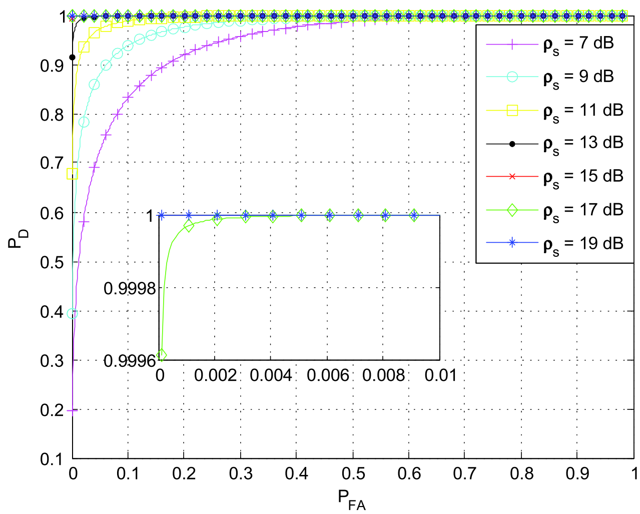

Fig. 2. ROC curves for different values of ρ_s (from 7 dB to 19 dB).

the ROC curves. Even if the proposed model is valid for high values of C/N_0, that is a condition encountered in open sky scenarios, it is valuable to predict the detector performance.

The ROC curves are the outcome of the theoretical model and need to be validated through proper simulation campaigns. Promising results have already been achieved, obtaining simulated ROC curves that fit the theoretical ones. Detailed study of this aspect will be the focus of authors' future activities on this work.

References

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

[2] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, P.M. Kintner, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, in: The Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008) Savannah GA, 2008, pp. 2314–2325.

[3] D.M. Akos, Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC), Navigation 59 (4) (2012) 281–290.

[4] B.W. O'Hanlon, M.L. Psiaki, T.E. Humphreys, J.A. Bhatti, Real-time spoofing detection using correlation between two civil GPS receiver, in: The Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012) Nashville TN, 2012, pp. 3584–3590.

[5] A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, G. Lachapelle, Detection and mitigation of spoofing attacks on a vector based tracking GPS receiver, in: The Proceedings of the 2012 International Technical Meeting of The Institute of Navigation, Newport Beach, CA, 2012, pp. 790–800.

[6] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle, GPS vulnerability to spoofing threats and a review of antispoofing techniques, Int. J. Navig. Obs. 2012 (2012).

[7] F. Dovis, X. Chen, A. Cavaleri, K. Ali, Detection of spoofing threats by means of signal parameters estimation, in: The Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011) Portland OR, 2011, pp. 416–421.

[8] K. Ali, E. Manfredini, F. Dovis, Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics, in: The Proceedings of the Position, Location and Navigation Symposium - PLANS, 2014 IEEE/ION, 2014, pp. 1240–1247.

[9] E.G. Manfredini, B. Motella, F. Dovis, Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests, in: The Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2015) Tampa FL, 2015, pp. 3100–3106.

[10] B.M. Ledvina, W.J. Bencze, B. Galusha, I. Miller, An in-line anti-spoofing device for legacy civil GPS receivers, in: The Proceedings of the International Technical Meeting of The Institute of Navigation (ION ITM 2010) San Diego CA, 2010, pp. 698–712.

[11] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, L. Lo Presti, Signal quality monitoring applied to spoofing detection, in: The Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 11) Portland Ore, 2011, pp. 1888–1896.

[12] A. Cavaleri, B. Motella, M. Pini, M. Fantino, Detection of spoofed GPS signals at code and carrier tracking level, in: The Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing NAVITEC, 2010, pp. 1–6.

[13] S. Lo, D.D. Lorenzo, P. Enge, D. Akos, P. Bradley, Signal authentication. A secure civil GNSS for today, Inside GNSS 4 (5) (2009) 30–39.

[14] T. Humphreys, Detection strategy for cryptographic GNSS antiSpoofing, IEEE Trans. Aerosp. Electron. Syst. 49 (2) (2013) 1073–1090.

[15] L. Lo Presti, Z. Xuefen, M. Fantino, P. Mulassano, GNSS signal acquisition in the presence of sign transition, IEEE J. Sel. Top. Sign. Proces. 3 (4) (2009) 557–570.

[16] D. Borio, L. Camoriano, L. Lo Presti, Impact of GPS acquisition strategy on decision probabilities, IEEE Trans. Aerosp. Electron. Syst. 44 (3) (2008) 996–1011.

[17] L. Lo Presti, E. Falletti, M. Nicola, M. Troglia Gamba, Software defined radio technology for GNSS receivers, in: The Proceedings of the 2014 IEEE Conference on Metrology for Aerospace (MetroAeroSpace), Benevento, Italy, 2014, pp. 314–319.

[18] S. Kay, Fundamentals of Statistical Signal Processing, Volume II: Detection Theory, Prentice Hall, 1998.