GNSS Spoofing Detection Based on Combined Monitoring of Acquisition Function and Automatic Gain Control

Tao Zhang[1], Xin Chen[1](✉), Weihua Xie[2], Wenxian Yu[1], and Weimin Zhen[3]

[1] Shanghai Key Laboratory of Navigation and Location Based Services, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
xin.chen@sjtu.edu.cn

[2] Beijing Satellite Navigation Center, Beijing 100094, China

[3] China Research Institute of Radiowave Propagation, Qingdao 266107, China

Abstract. Due to long-distance transmission from satellite to Earth, the received power of GNSS signals is extremely weak, causing that receivers are vulnerable to spoofing attack. Monitoring multiple correlation peaks in the acquisition function and abnormal deviation in the AGC values are two common methods to detect the presence of spoofing. However, it is found that the combination mode of these two methods and the corresponding combined performance have not been fully analyzed and verified. In this paper, the detection performances of these two methods are first analyzed. Next, a combined monitoring based on these two methods is proposed, and its combined performance is analyzed. Finally, a set of experiments are conducted to verify the correctness of theoretical analysis and test the combined detection performance.

Keywords: Combined spoofing detection · Acquisition function · Automatic gain control

1 Introduction

Relying on the precise ability of positioning, navigation and timing, GNSS is widely used in various fields of both national security and social economy. However, due to long-distance transmission from satellite to Earth, the received power of GNSS signals is extremely weak, causing that receivers are vulnerable to spoofing attack [1]. If the victim receiver misinterprets spoofing signals as authentic ones, it might deduce a false position fix, a false clock offset, or both [2]. Therefore, spoofing attack will pose a serious threat to the navigation security.

Several anti-spoofing methods have been proposed in open literature, and they can be divided into two broad categories: spoofing detection and spoofing mitigation [3]. Spoofing detection aims at detecting the presence of spoofing signals and delivering a warning to victim receivers, while spoofing mitigation mainly concentrates on retrieving the positioning and navigation abilities of receivers [4]. Acquisition function refers to a two-dimensional function about the code phase and Doppler frequency, that is obtained

C. Yang and J. Xie (Eds.): *China Satellite Navigation Conference (CSNC 2021) Proceedings*, LNEE 774, pp. 324–333, 2021.
https://doi.org/10.1007/978-981-16-3146-7_30

by correlating received signals with local replicas. When spoofing signals and authentic signals are both present, there will be two correlation peaks in acquisition function. This metric can be used to detect the spoofing presence. However, as the power of spoofing signals increases, the elevation of noise floor will obscure the authentic correlation peaks [5].

AGC is widely used in the RF front-end circuit to optimize the gain such that the amplitude of the incoming signal can utilize the entire range of the analog-to-digital converter (ADC). Since the power of received authentic GNSS signals on Earth is below that of the ambient thermal noise, when the power of spoofing signals is weak, AGC is driven mostly by the power of ambient thermal noise [6], leading to no significant change in AGC gains. When the power of spoofing signals is significantly stronger than that of authentic signals, AGC gains will deviate from the normal values.

Although the spoofing detection methods based on acquisition function or AGC have been discussed in literatures [6–8], it is found that the combination mode of these two methods and the corresponding combined performance have not been fully analyzed and verified. In this paper, the detection performances of these two methods are first analyzed. Next, a combined monitoring based on these two methods is proposed, and its combined performance is analyzed. Finally, a set of experiments are conducted to verify the correctness of theoretical analysis and test the combined detection performance.

The following sections are organized as follows. The performance analyses of acquisition function monitoring and AGC monitoring are respectively introduced in Sect. 2 and Sect. 3. The combined monitoring method and its theoretical detection performance are described in Sect. 4. Experimental results are analyzed and summarized in Sect. 5. Finally, conclusions are drawn in Sect. 6.

2 Performance Analysis of Acquisition Function Monitoring

2.1 Signal Model

After being down-converted and filtered by the RF front-end circuit in a GNSS receiver, the received signals under spoofing attack can be modeled as:

$$\begin{aligned} r(t) = & \sum_{i \in AU} \sqrt{2P_{au}^{i}} C^{i}\left(t - \tau_{au}^{i}\right) D^{i}\left(t - \tau_{au}^{i}\right) \cos\left[2\pi (f_{IF} + f_{d,au}^{i})t + \varphi_{au}^{i}\right] \\ & + \sum_{j \in SP} \sqrt{2P_{sp}^{j}} C^{j}\left(t - \tau_{sp}^{j}\right) D^{j}\left(t - \tau_{sp}^{j}\right) \cos\left[2\pi (f_{IF} + f_{d,sp}^{j})t + \varphi_{sp}^{j}\right] + \eta(t) \end{aligned} \quad (1)$$

where AU and SP represent visible satellite numbers, respectively, in authentic signals and spoofing signals. au and sp indicate the authentic signal and spoofing signal respectively. $C(t)$ is the spreading code sequence. $D(t)$ is the navigation message. τ, f_{IF}, f_d, φ denote, respectively, the code delay, receiver intermediate frequency, Doppler frequency and initial carrier phase. $\eta(t)$ is assumed to be Additive White Gaussian Noise with power spectral density of $N_0/2$.

Next, the signal acquisition is followed. For the k-th coherent integration period, the coherent integration outputs on the in-phase and quadrature branches are given by:

$$I_k = \frac{1}{2}\sqrt{2P_{au}^l}\cos\left(\varphi_{au}^l\right) + \sum_{\substack{i\in AU \\ i\neq l}} \frac{1}{2}\sqrt{2P_{au}^i}\psi_c^{(i,l)} + \sum_{j\in SP} \frac{1}{2}\sqrt{2P_{sp}^j}\psi_c^{(j,l)} + \eta_I(t) \tag{2}$$

$$Q_k = \frac{1}{2}\sqrt{2P_{au}^l}\sin\left(\varphi_{au}^l\right) + \sum_{\substack{i\in AU \\ i\neq l}} \frac{1}{2}\sqrt{2P_{au}^i}\psi_s^{(i,l)} + \sum_{j\in SP} \frac{1}{2}\sqrt{2P_{sp}^j}\psi_s^{(j,l)} + \eta_Q(t) \tag{3}$$

where T_{coh} is the coherent integration time. τ^l and f_d^l are, respectively, the code phase and Doppler frequency of the local replica. $\eta_I(t)$ and $\eta_Q(t)$ are the uncorrelated Gaussian noise components at the in-phase and quadrature branches, respectively. The Gaussian noise components are both zero mean and have the variances of σ_n^2, the variance is given by $\sigma_n^2 = N_0/(2T_{coh})$ [9].

$\psi_c^{(*,l)}$ and $\psi_s^{(*,l)}$ are the cross-correlation interferences between received signal and local replica, respectively, on the in-phase and quadrature branches. They are given as follows:

$$\psi_c^{(*,l)} = R_c\left(\Delta\tau^{(*,l)}\right)\sin c\left(\pi\Delta f_d^{(*,l)}T_{coh}\right)\cos\left(\pi\Delta f_d^{(*,l)}T_{coh} + \varphi^*\right) \tag{4}$$

$$\psi_s^{(*,l)} = R_c\left(\Delta\tau^{(*,l)}\right)\sin c\left(\pi\Delta f_d^{(*,l)}T_{coh}\right)\sin\left(\pi\Delta f_d^{(*,l)}T_{coh} + \varphi^*\right) \tag{5}$$

where $R_c\left(\Delta\tau^{(*,l)}\right)$ is the cross-correlation function of the spreading code. $\Delta\tau^{(*,l)}$ and $\Delta f_d^{(*,l)}$ are, respectively, the code phase difference and Doppler frequency difference between received signal and local replica.

After coherent integration and non-coherent accumulation, the acquisition function can be expressed as:

$$Y\left(\tau^l, f_d^l\right) = \sum_{k=1}^{K}\left(I_k^2 + Q_k^2\right) \tag{6}$$

where K is the number of non-coherent accumulation. Each (τ^l, f_d^l) point defines a searching cell in the acquisition function.

2.2 Hypothesis Testing Model

According to the presence or absence of the target acquiring signal, the following hypotheses can be established. For each hypothesis, the expressions of the in-phase and quadrature components are given with their probability distributions:

- H_0: signal is absent or not correctly aligned with local replica

$$I_k \sim N\left(0, \sigma^2\right); Q_k \sim N\left(0, \sigma^2\right) \tag{7}$$

$$Z\left(\tau^l, f_d^l\right) = \frac{Y\left(\tau^l, f_d^l\right)}{\sigma^2} = \frac{1}{\sigma^2}\sum_{k=1}^{K}\left(I_k^2 + Q_k^2\right) \sim \chi^2(2K) \tag{8}$$

- H_1: signal is present, only authentic signal is correctly aligned with local replica

$$I_k \sim N\left(\frac{1}{2}\sqrt{2P_{au}^l}\cos\left(\varphi_{au}^l\right), \sigma_a^2\right); Q_k \sim N\left(\frac{1}{2}\sqrt{2P_{au}^l}\sin\left(\varphi_{au}^l\right), \sigma_a^2\right) \tag{9}$$

$$Z\left(\tau^l, f_d^l\right) = \frac{Y\left(\tau^l, f_d^l\right)}{\sigma_a^2} = \frac{1}{\sigma_a^2}\sum_{k=1}^{K}\left(I_k^2 + Q_k^2\right) \sim \chi^2\left(2K, \frac{P_{au}^l K}{2\sigma_a^2}\right) \tag{10}$$

- H_2: signal is present, only spoofing signal is correctly aligned with local replica

$$I_k \sim N\left(\frac{1}{2}\sqrt{2P_{sp}^l}\cos\left(\varphi_{sp}^l\right), \sigma_s^2\right); Q_k \sim N\left(\frac{1}{2}\sqrt{2P_{sp}^l}\sin\left(\varphi_{sp}^l\right), \sigma_s^2\right) \tag{11}$$

$$Z\left(\tau^l, f_d^l\right) = \frac{Y\left(\tau^l, f_d^l\right)}{\sigma_s^2} = \frac{1}{\sigma_s^2}\sum_{k=1}^{K}\left(I_k^2 + Q_k^2\right) \sim \chi^2\left(2K, \frac{P_{sp}^l K}{2\sigma_s^2}\right) \tag{12}$$

where $\chi^2(a, b)$ denotes chi-square distribution. a is the degree of freedom. b is the non-central parameter.

According to the statistical analysis of the cross-correlation interferences, the variances of these hypotheses are given by:

$$\sigma_a^2 \approx \sigma_s^2 \approx \sigma^2 = \sigma_n^2 + Var\left(\sum_{i \in AU}\frac{1}{2}\sqrt{2P_{au}^i}\psi_c^{(i,l)} + \sum_{j \in SP}\frac{1}{2}\sqrt{2P_{sp}^j}\psi_c^{(j,l)}\right) \tag{13}$$

2.3 Detection Threshold and Theoretical Detection Performance

The false alarm probability on a searching cell and the overall false alarm probability in acquisition function are defined as [9]:

$$P_{fa-cell} = \int_{Z_{th}}^{\infty} f\left(Z\left(\tau^l, f_d^l\right)|H_0\right)dZ;\ P_{fa} = 1 - \left(1 - P_{fa-cell}\right)^{N_c} \tag{14}$$

where Z_{th} is the detection threshold for normalized amplitude of acquisition function. N_c is the total number of searching cells in acquisition function.

Based on Eq. (8) and (14), the detection threshold for normalized amplitude of acquisition function is given by:

$$Z_{th} = Y_{th}/\sigma^2 = F^{-1}\left(2K, (1 - P_{fa})^{1/N_c}\right) \tag{15}$$

where $F^{-1}\left(2K, (1-P_{fa})^{1/N_c}\right)$ is the inverse cumulative distribution function of the chi-square distribution with $2K$ degrees of freedom and evaluated at the probability value in $(1-P_{fa})^{1/N_c}$.

When authentic peak and the spoofing peak are simultaneously detected, the presence of spoofing signals will be determined. Therefore, the detection probability of spoofing presence in acquisition function monitoring can be expressed by:

$$P_D = \left(\int_{Z_{th}}^{\infty} f\left(Z\left(\tau^l, f_d^l\right)|H_1\right)dZ\right) \bullet \left(\int_{Z_{th}}^{\infty} f\left(Z\left(\tau^l, f_d^l\right)|H_2\right)dZ\right) \quad (16)$$

Simulation test is conducted to analyze the theoretical detection performance. It is assumed that the received signals include 10 authentic signals with the power of −128 dBm for each (typical received power for authentic GPS signals), and 10 spoofing signals with equal powers. The overall false alarm probability is set to 0.001, and the total number of searching cells is 21 * 50000.

As is shown in Fig. 1, the spoofing to authentic power ratio is defined as the power ratio between single spoofing signal and single authentic signal. It can be observed that as the number of non-coherent accumulation increases, the detection range of spoofing signal power is extended, and the detection probability is improved.

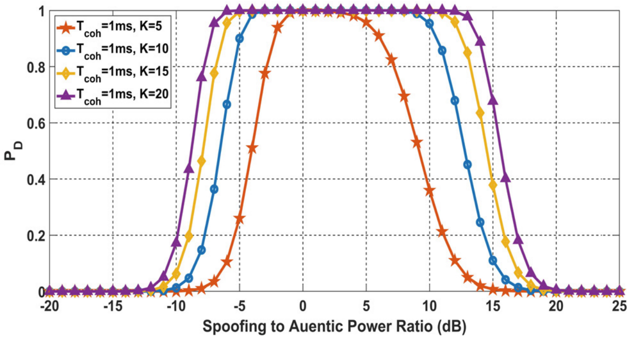

Fig. 1. Theoretical detection performance of acquisition function monitoring

3 Performance Analysis of AGC Monitoring

Null hypothesis significance testing (NHST) is a method of statistical inference [10], where P-value is an important concept that refers to the probability of occurrence for the observation sample if the null hypothesis were true. A low P-value indicates that the sample result would be unlikely present if the null hypothesis were true, leading to the rejection of the null hypothesis. This method is extremely suitable for detecting abnormal AGC gains under high power spoofing attack.

Assuming that G_A denotes the AGC gains obtained from the RF front-end circuit when no spoofing signal is present, G_A^i $(i = 1, 2, ..., m)$ are random samples of size m

in G_A, $\overline{G}_A$ and S_A^2 denote the sample mean and sample variance respectively; while G_E denotes the AGC gains obtained from the RF front-end circuit under unknown conditions, G_E^i $(i = 1, 2, ..., n)$ are random samples of size n in G_E, $\overline{G}_E$ and S_E^2 denote the sample mean and sample variance respectively.

Since the samples in G_A and G_E are independent of each other, when m and n are large (both $m > 40$ and $n > 40$), the test static as follows is approximately standard normal distributed according to Central Limit Theorem [10]:

$$V = \frac{\overline{G}_E - \overline{G}_A - (\mu_E - \mu_A)}{\sqrt{\frac{S_E^2}{n} + \frac{S_A^2}{m}}} \sim N(0, 1) \tag{17}$$

where μ_A and μ_E are, respectively, the population mean of G_A and G_E.

Therefore, the test statistic value and corresponding P-value can be expressed by:

$$v = \frac{\overline{G}_E - \overline{G}_A}{\sqrt{\frac{S_E^2}{n} + \frac{S_A^2}{m}}};\ P\text{-}value\ = \int_{-\infty}^{v} f(V)dV \tag{18}$$

where the lower the P-value, the higher the probability of spoofing presence. Typical P-value threshold can be set to 10^{-4}.

4 Combined Monitoring of Acquisition Function and AGC

Based on the preceding analyses, a combined monitoring based on acquisition function and AGC is proposed, and its block diagram is shown in Fig. 2.

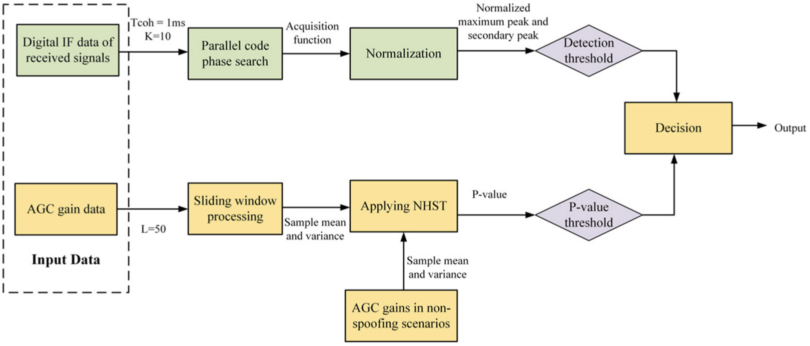

Fig. 2. Block diagram of combined monitoring

First, the digital intermediate frequency (IF) data of received signals and the corresponding AGC gains are recorded. Second, parallel code phase search is conducted to the digital IF data to obtain acquisition function, the coherent integration time is set to 1 ms, and the number of non-coherent accumulation is set to 10. And then the normalized maximum peak and secondary peak are calculated. Besides, sliding window is used to process the AGC gain samples, the window length L is set to 50 to ensure that it satisfies the Central Limit Theorem. The P-value of each sliding window is calculated by the NHST method. Finally, if the normalized maximum peak and secondary peak are both above the detection threshold, or the P-value of current sliding window is below the P-value threshold (10^{-4}), the presence of spoofing signals will be determined.

Simulation test is conducted to analyze the theoretical detection performance of the combined monitoring, which is shown in Fig. 4. It can be observed that the combination of acquisition function monitoring and NHST based AGC monitoring can compensate for each other's limitations, which can not only extend the detection range of spoofing signal power, but also improve the detection probability.

5 Experimental Tests

5.1 Experimental Validation for Theoretical Analysis

In order to verify the correctness of theoretical analysis, a simulator test is conducted, which is shown in Fig. 3. Two simulators are used to generate authentic signals and spoofing signals respectively, and the GNSS signal record system is used to record the digital intermediate frequency (IF) data of mixed signals and the corresponding AGC gains.

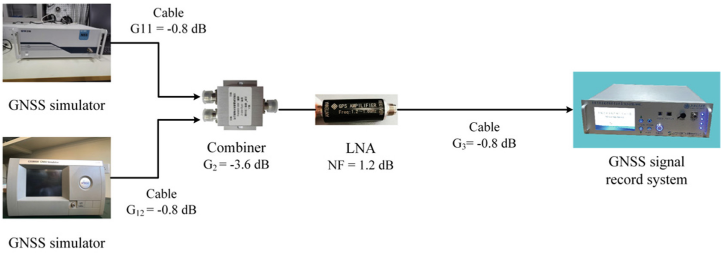

Fig. 3. Experimental setup of the simulator test

Next, acquisition function monitoring and AGC monitoring are applied to the recorded digital IF data and AGC gains. For acquisition function monitoring, the coherent integration time is 1 ms, the number of non-coherent accumulation is 10, the overall false alarm probability is 0.001, the total number of searching cells is 21 * 50000. For AGC monitoring, the length of sliding window is 50 and the P-value threshold is set to 10^{-4}. The comparison of experimental results and theoretical analysis is shown in Fig. 4.

It can be observed that for acquisition function monitoring, AGC monitoring and combined monitoring, experimental results show high consistence with the theoretical analysis, the average errors of detection probability are all less than 0.03, which verifies the correctness of theoretical analysis.

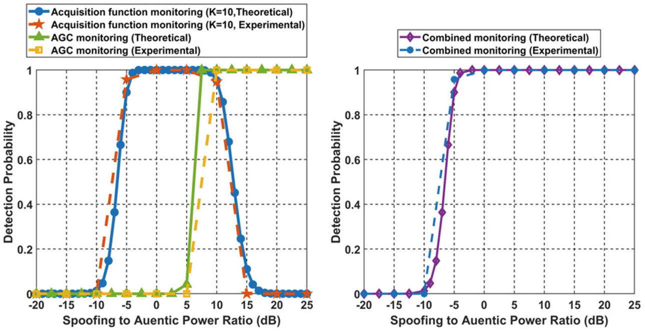

Fig. 4. Comparison of experimental results and theoretical analysis

5.2 Performance Test of Combined Monitoring for Static Receivers

To test the detection performance of the combined monitoring method for static receivers, as is shown in Fig. 5, a receiving antenna on the roof is used to receive authentic satellite signals, and then spoofing signals are generated by applying certain time delays and Doppler variations to the authentic signals through the spoofer. Finally, the spoofing signals are broadcast to the static receiving antenna.

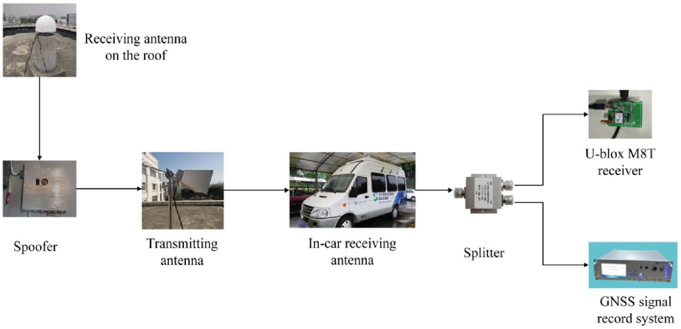

Fig. 5. Experimental setup of the static in-car test

Three different spoofing power settings are configured: low power spoofing, matching power spoofing and high power spoofing, the corresponding spoofing to authentic power ratios are −5 dB, 3 dB and 10 dB respectively. Next, the proposed combined monitoring method is applied to the recorded digital IF data and AGC gains, and the experimental detection results are shown in Fig. 6.

Under low power spoofing or matching power spoofing, since the spoofing signals and authentic signals are closely aligned in both code phase and Doppler frequency at the beginning of spoofing attack, it takes a period of time to detect the multiple peaks in the acquisition function. Under high power spoofing, the performance of combined monitoring mainly depends on the AGC monitoring, hence it is not affected by the

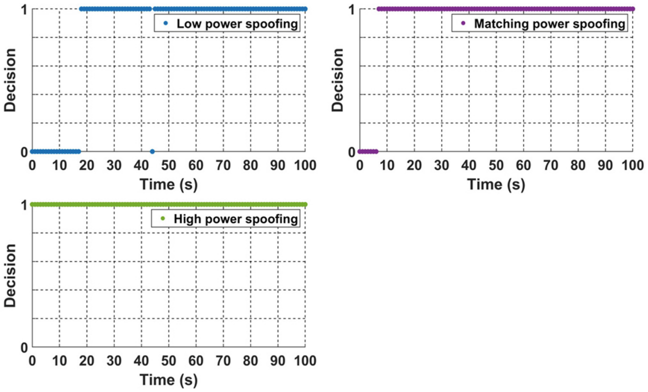

Fig. 6. Experimental detection results of the combined monitoring method

alignment between spoofing signals and authentic signals, and the spoofing presence can be detected throughout the spoofing attack.

6 Conclusion

In this paper, a combined monitoring based on acquisition function and AGC is proposed, its detection performance is analyzed and tested. The average errors of detection probability between experimental results and theoretical analysis are less than 0.03, which verifies the correctness of theoretical analysis. Besides, the proposed combined monitoring can effectively detect the spoofing presence even though the power of spoofing signals is 5 dB lower than that of authentic signals.

Acknowledgements. The research work was funded by the National Key Research and Development Program of China (No: 2018YFB0505103); Science and Technology Project of State Grid Corporation of China (No. SGSHJX00KXJS1901531).

References

1. Ioannides, R.T., Pany, T., Gibbons, G.: Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. Proc. IEEE **104**(6), 1174–1194 (2016)
2. Psiaki, M.L., Humphreys, T.E.: GNSS spoofing and detection. Proc. IEEE **104**(6), 1258–1270 (2016)
3. Wang, F., Hu, C., Wu, S., Tao, Y., Xu, Y.: Research on BeiDou anti-spoofing technology based on comprehensive radio determination satellite service. Satell. Navig. **1**(1), 1–9 (2020). https://doi.org/10.1186/s43020-019-0004-2
4. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G.: GPS vulnerability to spoofing threats and a review of antispoofing techniques. Int. J. Navig. Obs. **2012**, 1–16 (2012)
5. Jafarnia Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G.: GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N$_0$ measurements. Int. J. Satell. Commun. Netw. **30**(4), 181–191 (2012)

6. Akos, D.M.: Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). Navig. J. Inst. Navig. **59**(4), 281–290 (2012)
7. Hegarty, C., Odeh, A., Shallberg, K., Wesson, K., Walter, T., Alexander, K.: Spoofing detection for airborne GNSS equipment. In: Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2018), pp. 1350–1368, September 2018
8. Hegarty, C., O'Hanlon, B., Odeh, A., Shallberg, K., Flake, J.: Spoofing detection in GNSS receivers through cross-ambiguity function monitoring. In: Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2019), 20 September 2019, pp. 920–942 (2019)
9. Borio, D.: A statistical theory for GNSS signal acquisition. Ph.D. dissertation, Polytecnico di Torino (2008)
10. Devore, J.L.: Probability and Statistics for Engineering and the Sciences. Duxbury Press, Belmont (2008)