A Repeater Spoofing Detection Method Based on In-Phase Correlation Values

Pengcheng Ma, Xiaomei Tang, Zengjun Liu(✉), Baiyu Li, and Gang Ou

College of Electronic Science, National University of Defense Technology, Changsha, Hunan, People's Republic of China
zjunliu@126.com

Abstract. GNSS (Global Navigation Satellite System) spoofing has a great impact on the receiver getting trusted position, navigation and timing information, letting the receiver output erroneous information without any notice and causing an incalculable loss to the user. Since the spatial location of the spoofing interference source, the relative position between the repeater and the user, the parameter characteristics of the deceptive signal are different from the authentication signal, the research on the all above difference are getting great improvements. In the complex electromagnetic interference environment, the carrier-to-noise ratio (CN0) estimation will decrease with the increase of the jamming power. However, the CN0 will not follow this rule under the repeater spoofing scene, which may give rise to false missing probability of the spoofing detection method based on CN0 estimation. In addition, the spoofing detection method based on absolute total power measurements will get higher false alarm probability under the jamming interference scene. This paper proposes a constant false-alarm rate (CFAR) repeater spoofing detection method based on In-Phase correlation values under common signal power scenarios and power-enhanced signal scenarios. This method is realized and verified by simulation under various scenes.

Keywords: GNSS spoofing · Signal detection · In-phase correlation · Constant false-alarm rate

1 Introduction

GNSS can provide precise positioning, navigation and timing services in all time and space, and it plays an important role in military and daily life. With the occurrence of more and more GNSS spoofing incidents, spoofing has become one of the biggest threats to the trusted positioning of GNSS. Spoofing refers to the fact that the receiver outputs the wrong location and time without being aware of it, causing the user to suffer huge losses. The WelNavigate GS720 signal source was once placed on the former truck to deceive the target receiver on the next truck [1]. In 2008, Todd Humphreys and his team designed and manufactured a spoofing interference source to demonstrate the feasibility of spoofing interference [2]. In 2012 and 2013, Humphreys successfully deceived drones and ships using GPS civilian signals [3–5]. On the military side, in

J. Sun et al. (Eds.): CSNC 2020, LNEE 652, pp. 634–645, 2020.
https://doi.org/10.1007/978-981-15-3715-8_57

December 2011, Iranian media claimed that the Iranian air forces captured an American unmanned aircraft "RQ-170" on the eastern border of the country [6], which has drawn intense attention from all over the world.

Because the real signal in the GNSS receiver behaves self-consistently, the deceptive signal will always break this self-consistent state more or less, so it can be judged whether the receiver has been spoofed according to the abnormality behavior of the receiver. GNSS receiver spoofing detection technology can be classified as follows based on the detection information source process: incoming signal direction detection based on the antenna array [7], RF channel AGC change detection [8], signal processing layer detection [9–11] and external sensor-assisted detection [12, 13].

For ordinary low-cost receivers, a small number of circuits are usually added to the signal processing layer to perform fraud detection without additional hardware such as an antenna array and external sensors. The spoofing detection method based on the In-phase correlation values in this paper is aimed at the application of ordinary low-cost receivers, which is improved on the CN0 detection method. There have been some researches based on CN0 and noise power. Nielsen proposed a detection criterion based on the CN0 [14], but for repeater spoofing, the CN0 is basically the same as normal conditions, which will cause false alarms. Total signal power detection will bring a large false alarm [15]. Jahromi proposed a method of deceptive interference detection based on the total signal power and CN0 [16], but did not give a theoretical analysis of the performance under the repeater deceptive interference. Based on the current research basis, this paper proposes a repeater spoofing detection method based on the correlation value of the in-phase branch, which can not only avoid false alarms caused by interference, but also effectively perform repeater deception detection.

The structure of this article is as follows. Section 2 gives the repeater spoofing and the received signal model; Sect. 3 gives the correlation value mathematical model, and then introduces the detection method with its performance analysis. The performance under different scenarios was simulated and verified. Finally, it was summarized.

2 Signal Model

The received signal is a mixture of the deception interference signal and the real signal when there is repeater spoofing interference.

2.1 Repeater Spoofing Signal Model

Repeater deceptive interference uses the GNSS signal repeater to directly retransmitting the received signal to the target receivers. The scene is shown as the following Fig. 1.

The signal received by the repeater is expressed as

$$x_R(t) = s_R(t) + n_R(t) \tag{1}$$

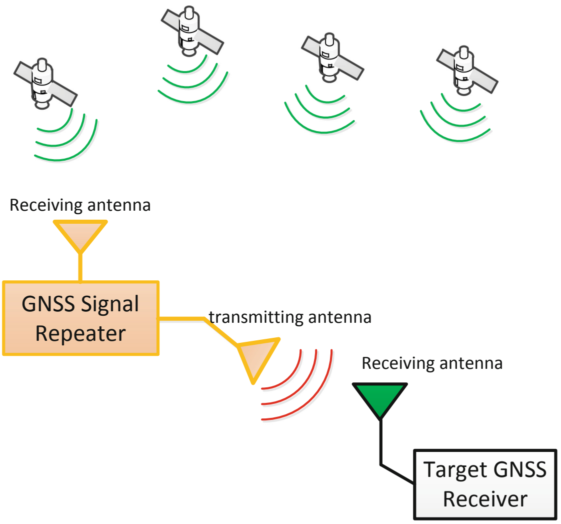

Fig. 1. Repeater spoofing

The subscript R represents the repeater. $s_R(t)$ is the navigation signal and can be expressed as

$$s_R(t) = A_R c(t - \tau_R) D(t - \tau_R) \cos(2\pi(f_0 + f_R)t + \theta_R) \tag{2}$$

Among them, A_R indicates the amplitude of the navigation signal, $c(t)$ indicates the pseudo-code sequence, and the chip width is T_c, τ_R indicates the signal delay, $D(t)$ indicates the navigation message, f_0 indicates the carrier frequency, and f_R indicates the doppler frequency and θ_R is the initial phase of the carrier. $n_R(t)$ is the unavoidable noise introduced by the repeater receiving RF channel, and the power spectral density is $\frac{N_0}{2}$. In reality, there will be multiple satellite signals. Here one satellite signal is used for analysis.

2.2 Receiving Signal Model

The signal received by the final target receiver is

$$x(t) = s(t) + n(t) + G_T x_R(t) = s(t) + n(t) + G_T[s_R(t) + n_R(t)] \tag{3}$$

Among them, G_T is the transmitting gain of the repeater. The expression of the real navigation signal is

$$s(t) = Ac(t - \tau_A) D(t - \tau_A) \cos(2\pi(f_0 + f_A)t + \theta_A) \tag{4}$$

The subscript A represents the Authentic signal. For receiver thermal noise $n(t)$, the power spectral density is consistent with $n_R(t)$. Other symbols have the same meaning as the formula (2). In addition, assume that the real navigation signal is received by an omnidirectional antenna with a gain of 0 dB.

3 Correlation Values

The receiver needs to perform filtering, amplification, down conversion, gain control, sampling quantization, quadrature down conversion, matched filter detection, and coherent integration on the received signal to obtain the correlation values.

3.1 Receiver Processing

The simplified process of navigation receiver signal processing is as Fig. 2.

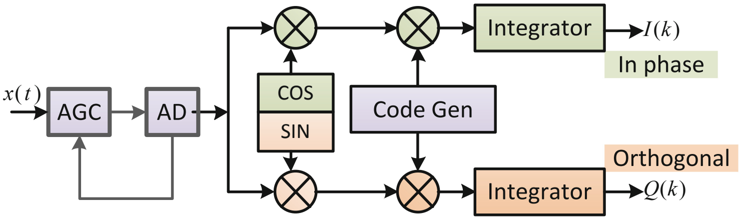

Fig. 2. Simple implementation block diagram of the receiver

The receiver performs power adjustment and quantization of the received signal, and performs digital orthogonal down conversion, and then correlates with the local pseudo code, then product results enters the integrator for accumulation. The integration time is T_{coh}, and finally the relevant accumulated value is obtained. The cumulative value of two orthogonal correlations is shown below.

$$\begin{cases} I(k) = AD(k)\cos[\varphi(k)] + n_I(k) \\ Q(k) = AD(k)\sin[\varphi(k)] + n_Q(k) \end{cases} \tag{5}$$

Among them, $\varphi(k)$ indicates the phase error between the navigation signal and the local reference signal during normal tracking. The correlation value $I(k)$, $Q(k)$ follows a Gaussian distribution, and the average value is determined by the signal power. In order to simplify the analysis, the correlation value loss caused by factors such as frequency estimation errors and pseudo-code phase errors are ignored here.

The noise accumulated value is as follows.

$$\begin{cases} n_I(k) = \frac{1}{T_{coh}} \int\limits_{kT_{coh}}^{(k+1)T_{coh}} n_I(t)c(t)dt \\ n_Q(k) = \frac{1}{T_{coh}} \int\limits_{kT_{coh}}^{(k+1)T_{coh}} n_Q(t)c(t)dt \end{cases} \tag{6}$$

It is assumed that the interference power caused by cross-correlation is much lower than the noise power and is ignored here.

3.2 Correlation Value Analysis

When the receiver tracks the real navigation signal or spoofing signal, the correlation value characteristics are obviously different. The correlation value characteristics in the two cases are theoretically derived below.

When the receiver tracks the authentic navigation signal, the correlation value results expression is the same as formula (5). The variance of $n_I(k)$ and $n_Q(k)$ is $\frac{N_0}{2T_{coh}}$ respectively. When the receiver tracks the repeater spoofing signal, the correlation value can be expressed as follows.

$$\begin{cases} I_R(k) = G_T A_R D(k)\cos[\varphi(k)] + n_{RI}(k) \\ Q_R(k) = G_T A_R D(k)\sin[\varphi(k)] + n_{RQ}(k) \end{cases} \tag{7}$$

The two noise correlation accumulation processes are as follows.

$$\begin{cases} n_{RI}(k) = \frac{1}{T_{coh}} \int\limits_{kT_{coh}}^{(k+1)T_{coh}} (n(t) + G_T n_R(t))c(t)dt \\ n_{RQ}(k) = \frac{1}{T_{coh}} \int\limits_{kT_{coh}}^{(k+1)T_{coh}} (n(t) + G_T n_R(t))c(t)dt \end{cases} \tag{8}$$

When the receiver tracks the repeater signal, the two noises obey the Gaussian distribution, and the variance is $\left(G_T^2 + 1\right)\frac{N_0}{2T_{coh}}$ respectively, which can be derived by referring to [17].

4 Spoofing Detection Based on In-Phase Correlation Values

Successful spoofing attack usually requires higher absolute power level than the authentic signal. Because the repeater directly retransmits the received signal, the repeater transmission gain must be maintained at a certain level to ensure that the absolute level of the spoofing signal is higher than the absolute level of the real signal.

If the repeater uses a high gain receiving antenna, the repeater transmission gain can be lower than the omnidirectional receiving antenna. Different from the traditional spoofing detection method based on the total received signal power and the CN0 measurements, this paper establishes a constant false alarm repeater spoofing detection value based on the in-phase branch correlation values, which is essentially a method for detecting the absolute power level of the tracking signal.

4.1 Spoofing Detection Statistics

Ignoring the effects of message symbols and phase errors, the in-phase branch data can be modeled as

$$I(k) = A + n_I(k), k \in N \tag{9}$$

The binary detection problem is

$$\begin{aligned} &\mathrm{H}_0 : I(k) = A_S + n_{SI}(k) \\ &\mathrm{H}_1 : I(k) = G_T A_R + (G+1) n_{SI}(k) = G_T A_R + n_{RI}(k) \end{aligned} \tag{10}$$

When noise suppression interference exists,

$$\begin{aligned} &\mathrm{H}_0 : I(k) = A_S + n_{SI}(k) + n_J(k) \\ &\mathrm{H}_1 : I(k) = G_T A_R + n_{RI}(k) + n_J(k) \end{aligned} \tag{11}$$

Among them, $n_J(k)$ represents the noise interference, $A_S = G_R A_0$, where A_0 represents the prior information of the authentic signal amplitude and G_R represents the repeater receiving antenna gain. All above signal level is compensated according to the AGC value G_A measured by the current receiving RF channel. If

$$T(\mathbf{x}) = (N-1)\frac{(\bar{I} - G_A A_0)^2}{\frac{1}{N}\sum_{k=1}^{N}(I(k) - \bar{I})^2} > \gamma \tag{12}$$

The GLRT judges H_1 [18]. $\bar{I}$ represents the mean of in-phase branch correlation values:

$$\bar{I} = \frac{1}{N}\sum_{k=1}^{N} I(k) \tag{13}$$

4.2 Detection Performance Analysis

The detection performance can be shown as follows:

$$\begin{aligned} P_{FA} &= Q_{F_{1,N-1}}(\gamma) \\ P_D &= Q_{F_{1,N-1}(\lambda)}(\gamma) \end{aligned} \tag{14}$$

Among them, P_{FA} represents false alarm probability, P_D represents detection probability theoretical value, $F_{1,N-1}$ represents F distribution, which has 1 freedom and $N-1$ degrees of freedom, $F_{1,N-1}(\lambda)$ represents non-central F distribution, which has 1 freedom and $N-1$ degrees of freedom, and non-central parameter λ with the value

$$\lambda = \frac{N(A-A_0)^2}{\sigma^2} \tag{15}$$

Among them, σ^2 represents the noise variance. The false alarm probability is calculated based on the distribution and does not depend on the noise variance, so it is the constant false alarm detection amount. From the above formula, it can be seen that the detection performance under a certain false alarm probability is affected by factors such as data length, noise power, and amplitude value offset.

5 Simulation Verification and Analysis

There are several factors needed to be considered before simulation. Under special conditions, the navigation satellite will perform signal power enhancement to lift anti-interference ability of the receiver. For spoofing attackers, the retransmission gain needs to be controlled in order to achieve better deceiving affects, and the gain of the receiving antenna is specially designed to obtain a higher CN0 of the spoofing signal, which can reduce the transmission power of the repeater.

In summary, the simulation scene parameter settings can be traversed as the following. The normal power level is set to −160 dBW and the power enhancement is set to −155dBW. The repeater transmit gain is set to three levels of 0 dB, 3 dB, and 6 dB, and the repeater receive antenna gain is set to three levels of 0 dB, 3 dB, and 6 dB. The jamming-signal-ratio (JSR) is set to four levels of no jamming, 5 dB, 10 dB and 20 dB. In the simulation process, correlation value data is generated every 1 ms, and Monte Carlo simulation is performed 100,000 times.

5.1 Impact of Signal Power Enhancement

The following figure is the impact of navigation signal power enhancement on detection performance. The correlation data length is 4 ms.

It can be seen from the Fig. 3 that power enhancement can improve the detection performance. That is, under the same power difference condition, the higher of the absolute signal level, the easier is to be detected.

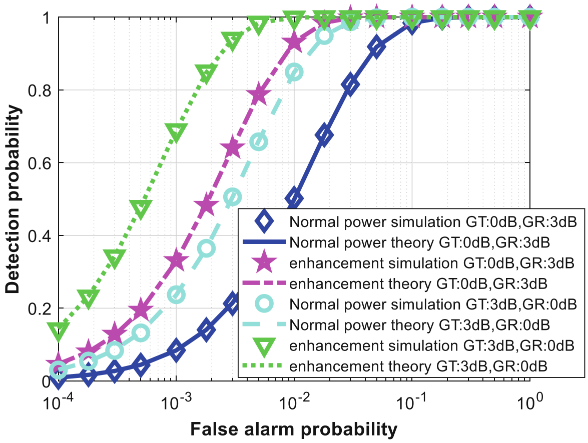

Fig. 3. Detection performance in power enhanced scenarios

5.2 Effect of Repeater Transmit Gain

The effect of the repeater transmit gain on the detection performance is shown as Fig. 4. The correlation data length is 4 ms.

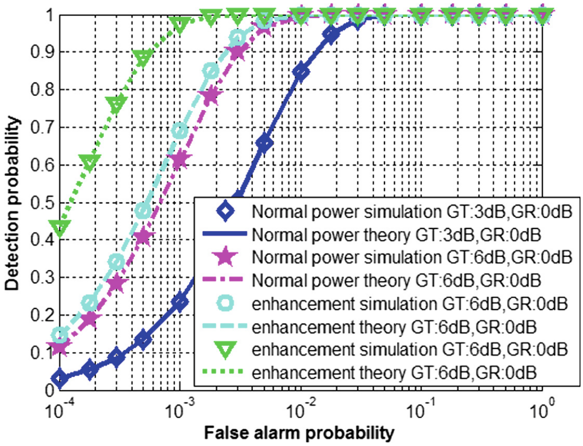

Fig. 4. Effect of transmit gain on detection performance

As can be seen from the figure above, with the increase of the repeater transmission gain, the absolute power level also increases, and the receiver more easily detects the existence of spoofing interference.

5.3 Effect of Repeater Receive Antenna Gain

The influence of the repeater receiving antenna gain on the detection performance is shown as Fig. 5. The correlation data length is 4 ms.

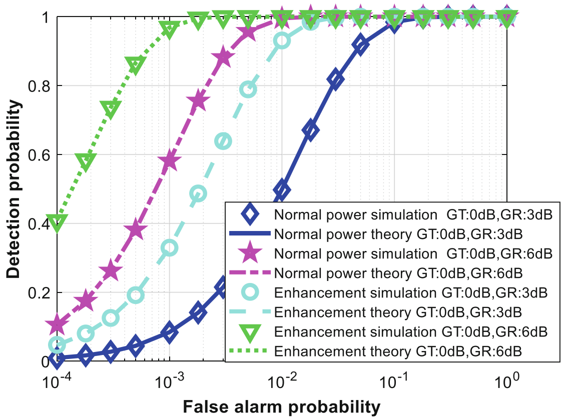

Fig. 5. Effect of receive antenna gain on detection performance

Comparing Figs. 4 and 5, it can be found that the method of increasing the repeater receiving gain is more concealed than increasing the repeater transmitting gain. For example, the detection probability shown by Fig. 5 is lower than that shown by Fig. 4 when the gain value is identical and false alarm probability is at 0.1%.

5.4 Effect of Coherent Integration Data Length

The influence of the length of the coherent integration data on the detection performance is illustrated in Fig. 6. The repeater receiving antenna gain is 0 dB and the transmission gain is 3 dB.

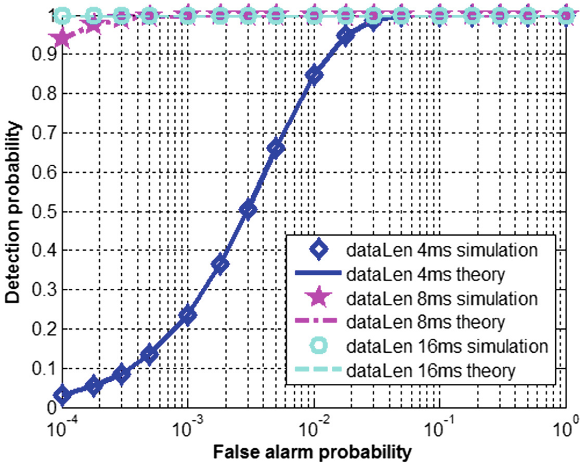

Fig. 6. Effect of coherent integration data length on detection performance

As can be seen from the above figure, under the condition of no interference, the receiver can achieve higher detection performance when the coherent integration data length exceeds 8 ms.

5.5 Impact of Noise Jamming Interference

The impact of noise jamming interference on detection performance is illustrated in Fig. 7. The correlation value data length is 4 ms.

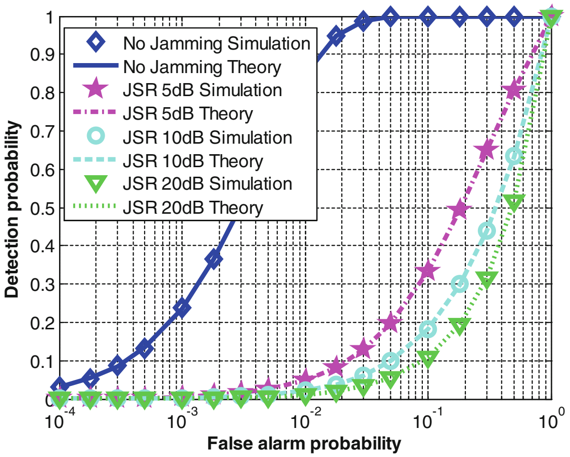

Fig. 7. Effect of interference on detection performance

As can be seen from the figure above, interference will greatly decline the detection performance. In order to improve the detection performance of the detector under interference scenarios, the receiver needs to increase the length of the coherent integral data. The detection performance of different coherent integral data length under different JSR scenes is shown in Fig. 8.

It can be seen from Fig. 8, when the coherent integral data length exceeds 1 s, a detection probability of 90% can be obtained as the false alarm probability is 0.1% and the JSR is 20 dB.

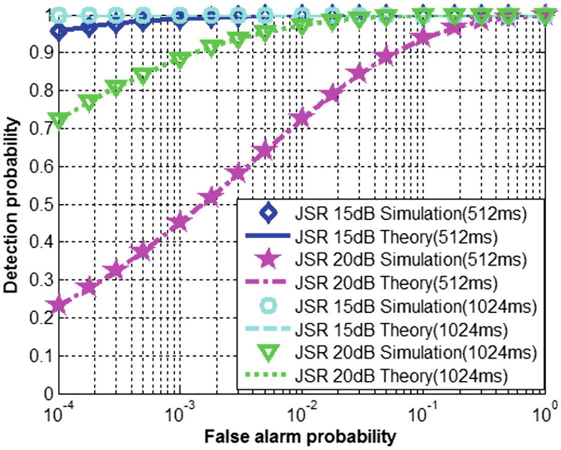

Fig. 8. Detection performance of different coherent length under jamming

6 Conclusions

This paper addresses the problem of high missing alarms using the CN0 detection method under the condition of repeater spoofing interference and the high false alarms in the jamming scenario based on the total signal power measurement. The repeater spoofing interference detection method based on the correlation value of in-phase branches realizes the constant false alarm detection under different noise jamming power. The effects of navigation signal power enhancement, repeater transmitting gain, receiving antenna gain, coherent integral data length and different noise jamming power on the detection performance are analyzed through simulation. For anti-spoofing receiver design, the recommendations of different coherent integration data length are given.

Acknowledgments. This work is supported by National Science Foundation of China (61601485, 41604016).

References

1. Warner, J., Johnston, R.: A simple demonstration that the global positioning system is vulnerable to spoofing. J. Secur. Adm. **25**(2), 19–27 (2002)
2. Humphreys, T., Ledvina, B., Psiak, M., et al.: Assessing the spoofing threat: development of a portable gps civilian spoofer. In: ION GNSS, pp. 2314–2325 (2008)
3. Shepard, D., Bhatti, J., Humphreys, T.: Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In: ION GNSS, pp. 3591–3605 (2012)
4. Shepard, D., Bhatti, J., Humphreys, T.: Drone hack: spoofing attack demonstration on a civilian unmanned aerial vehicle. GPS World **23**(8), 30–33 (2012)
5. Bhatti, J., Humphreys, T.: Hostile control of ships via false GPS signal: demonstration and detection. J. Navig. **64**(1), 51–66 (2017)

6. Rawnsley, A.: Iran's alleged drone hack: tough, but possible (2011). http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/
7. Montgomery, P., Humphreys, T., Ledvina B.: Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In: ITM, pp. 124–130 (2009)
8. Wen, H., Huang, P., Dyer, J., et al.: Countermeasures for GPS signal spoofing. In: ION GNSS, pp. 1285–1290 (2005)
9. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., et al.: GPS vulnerability to spoofing threats and a review of anti-spoofing techniques. Int. J. Navig. Obs. (2012)
10. Gao, Y., Li, H., Mingquan, L., et al.: Intermediate spoofing strategies and countermeasures. Tsinghua Sci. Technol. **18**(6), 599–605 (2013)
11. Ledvina, B.M., Bencze, W.J., et al.: An in-line anti-spoofing device for legacy civil GPS receivers. In: ITM, pp. 698–712 (2010)
12. Manickam, S., O'Keefe, K.: Using tactical and MEMS grade INS to protect against GNSS spoofing in automotive applications. In: ION GNSS, pp. 1–11 (2016)
13. Lo, S., Chen, Y.H., Reid, T., et al.: The benefit of low cost accelerometers for GNSS anti-spoofing. In: ION Pacific PNT Meeting (2017)
14. Nielsen, J., Dehghanian, V., Lachapelle, G.: Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements. Int. J. Navig. Obs. 1–9 (2012). https://doi.org/10.1155/2012/501679
15. Dehghanian, V., Nielsen, J., Lachapelle, G.: GNSS spoofing detection based on signal power measurements: statistical analysis. Int. J. Navig. Obs. (2012). https://doi.org/10.1155/2012/313527
16. Jahromi, A.J., Broumandan, A., Nielsen, J., Lachapelle, G.: CPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements. Int. J. Satell. Commun. Netw. **30**, 181–191 (2012)
17. Holmes, J.K.: Spread Spectrum System in GNSS and Wireless Communication, pp. 298–299. Electronic Industry Press (2013)
18. Kay, S.M.: Basics of Statistical Signal Processing—Estimation and Detection Theory, p. 604. Electronic Industry Press (2014)