Research on Spoofing Detection Technology Based on Circular Correlation Capture

Fan Guangwei[1, 2 a], Wang Zhenhua [1,2]

[1]State Key Laboratory of Satellite Navigation System and Equipment Technology, Hebei, China

[2]The 54th Research Institute of CECT, Shijiazhuang, Hebei, China

[a]fgweihb@163.com

Keywords: Spoofing Interference; detection ; Circular Correlation.

Abstract. Concerning the problem that a single spoofing detection method has poor performance in the receiver capturing phase, this paper presents a joint spoofing detection algorithm that combines the signal arrival time detection with the capturing correlation peak detection. The relationship among detection probability, false alarm probability and detection threshold is derived in addition to an analysis to the performance and the scope of application of the proposed method. It solves the problem of failure to detect repeater spoofing and strong generator spoofing interferences simultaneously in the receiver capturing phase. The algorithm has good application prospects, for it does not require additional equipment to the existing receivers in addition to low computation complexity.

Introduction

Along with the evolution of navigation confrontation technology and microelectronic technology, the threats from spoofing interference [1~3] have become increasingly worse to satellite navigation systems. Spoofing interference is purposed to deviate the positioning results provided by satellite navigation system and thereby to make aircrafts and vessels impossible to position correctly and make precision-guided munitions off targets by means of rebroadcasting or generating similar spoofing signals. Spoofing interference is not easy to be detected or highly undetectable. Therefore, it is of great importance to research the detection and identification technology of spoofing interferences, eliminate the effects, exert the all-weather and high-accuracy strengths of satellite navigation system and promote the development of navigation applications.

However, since spoofing interference signals are relatively weak and generally much lower than noises, it is very difficult to detect spoofing interference with traditional interference detection techniques; therefore, full use must be made of the prior knowledge in the detection of spoofing interferences. Researchers in China or abroad ever proposed some detection methods of spoofing interferences, e.g., Nielsen J [4] proposed a detection method for spoofing interferences using a handheld single-antenna receiver; Mark L.Psiaki [5] proposed a detection method for spoofing interferences using two receivers from different systems; Logan Scott [6] summarized and analyzed the popular spoofing techniques; Geng Zhenglin [7] summed up both spoofing techniques and spoofing detection techniques; Huang Long [8~9] summarized and analyzed the spoofing detection methods in several his papers.

Concerning the spoofing interference detection requirements in the acquisition phase, this paper proposed a code-frequency 2D technique to obtain the arrival time of the received signal and acquire the correlation peaks based on circular correlation. A simulation test was given afterwards to validate the algorithm performance.

Acquisition Technique Based on Circular Correlation

Acquisition refers to the process of demodulating a signal to find out the carrier frequency and code phase. Since the time-domain convolution is equivalent to Fourier transform in the frequency domain; therefore, it is acceptable to convert the convolution search process to the frequency domain

in the course of acquisition. It is possible to obtain the frequency of a received signal by means of Fourier transform. For the civil signal at Beidou B1 frequency point, the spectral resolution is 1kHz after Fourier transform if the length of the input signal is 1 pseudo-code period. Therefore, it is allowed to set an acquisition threshold in a frequency domain. The highest frequency component above the threshold is the frequency corresponding to the received signal.

In the frequency searching process, let the native code be multiplied by a RF carrier signal within a search scope and make the search successively by certain steps. The generated native code q_{si} is expressed as follows:

$$q_{si} = C_s e^{j2\pi f_i t} \tag{1}$$

Where, C_s represents the native code of the s th channel and f_i represents the i th frequency component.

The code phase search process in the course of receiver acquisition may be considered as the process that a signal goes through a linear system, which is expressed as follows:

$$y(t) = \int_{-\infty}^{\infty} x(\tau) q_{si}(t-\tau) d\tau \tag{2}$$

Where, $q_i(t)$ represents the native code of the i th channel, of which the Fourier transform is expressed as follows:

$$\begin{aligned} Y(f) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x(\tau) q_{si}(t-\tau) d\tau e^{-j2\pi ft} dt \\ &= \int_{-\infty}^{\infty} x(\tau)\left(\int_{-\infty}^{\infty} q_{si}(t-\tau) e^{-j2\pi ft} dt\right) d\tau \end{aligned} \tag{3}$$

Let the variable $u = t - \tau$, then,

$$\begin{aligned} Y(f) &= \int_{-\infty}^{\infty} x(\tau)\left(\int_{-\infty}^{\infty} q_{si}(u) e^{-j2\pi fu} du\right) e^{-j2\pi f\tau} d\tau \\ &= Q_i(f)\int_{-\infty}^{\infty} x(\tau) e^{-j2\pi f\tau} d\tau = Q_i(f) X(f) \end{aligned} \tag{4}$$

After inverse Fourier transform, we get:

$$y(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} Y(f) e^{j2\pi ft} df \tag{5}$$

The detection statistical quantity $V = \sqrt{Y_I^2 + Y_Q^2}$, because the signals in both Branch I and Branch Q are subject to normal distribution. And it is derived that V is subject to Rice distribution, then its probability density function is expressed as follows:

$$f(v,\lambda) = \frac{v}{\sigma_n^2} e^{-\frac{v^2+\lambda^2}{2\sigma_n^2}} I_0\left(\frac{\lambda v}{\sigma_n^2}\right) \tag{6}$$

Where, I_0 represents the first sort of modified Bessel function at zeroth order, σ_n^2 represents noise variance, $\lambda = \left|aR(\tau)\mathrm{sinc}(f_e T_{coh})\right|$ represents signal amplitude, τ represents the time delay of received signal relative to native code, f_e represents the frequency difference between the replicate carrier and the received signal and T_{coh} represents coherent integration time.

It is possible to work out the mean value of V with reference to the density function (6) of Rice distribution, as expressed below:

$$E(V) = \sqrt{\frac{\pi}{2}}\sigma_n L_{1/2}\left(-\frac{\lambda^2}{2\sigma_n^2}\right) \tag{7}$$

Where, Lagrange polynomial $L_{1/2}(\bullet)$ is expressed as $L_{1/2}(x) = e^{\frac{x}{2}}\left((1-x)I_0\left(-\frac{x}{2}\right) - xI_1\left(-\frac{x}{2}\right)\right)$.

Let's assume the variance constant of noise power is σ_n^2. When no signal or the signal is rather weak, $\lambda \ll \sigma_n^2$, then the probability density function of statistical quantity V is approximately subject to Rayleigh distribution, as expressed below:

$$f(v,\lambda)=\frac{v}{\sigma_n^2}e^{-\frac{v^2}{2\sigma_n^2}} \tag{8}$$

The mean value of Rayleigh distribution can be expressed as $E(v)=\sqrt{\frac{\pi}{2}}\sigma_n^2$.

When no satellite signal is present, H_0 is subject to Rayleigh distribution. Then, the false alarm probability P_{fa1} corresponding to threshold value η_1 is:

$$P_{fa}=\int_{\eta_1}^{\infty}\frac{v}{\sigma_n^2}e^{-\frac{v^2}{2\sigma_n^2}}dv=e^{-\frac{\eta_1}{2\sigma_n^2}} \tag{9}$$

It means,

$$\eta_1=\sigma_n\sqrt{-2\ln P_{fa}} \tag{10}$$

If the noise power σ_n^2 and the false alarm probability P_{fa} are given, then it is possible to figure out the acquisition threshold η_1. Therefore, it is acceptable to convert the correlation search process in time domain for code phase acquisition to the frequency domain.

Improvement Repeater Spoofing Detection Based on Circular Correlation

The value of non-coherent accumulation in the acquisition phase is also a response to signal energy. And the spoofing signal energy is generally 5~10dB higher than that of the real navigation signal to achieve good spoofing performance. Therefore, it is feasible to detect the presence of spoofing interference using the non-coherent accumulation peak value in the process of acquisition, i.e., the presence of spoofing interference is considered if the peak value is greater than a threshold.

Let's assume the power of spoofing signal is higher than that of the true navigation signal and they are of the same signal format but from different sources. Therefore, it is acceptable to express their probability density functions with Equation (6) though they have different mean values. In this case, the probability distribution of the detection statistical quantity V after non-coherent integration may be illustrated with the graph below.

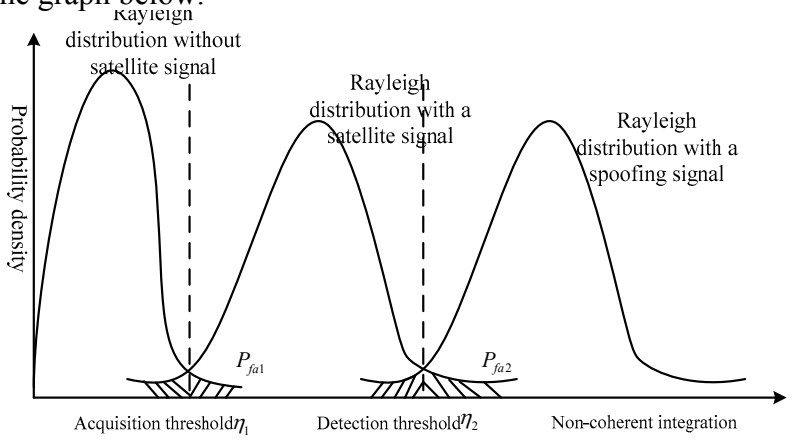


Figure 1 Probability distribution of non-coherent integration values

As shown in the graph, the detection for spoofing interference based on non-coherent integration statistical quantity may be regarded as a trivariate detection issue, i.e., to make a valid selection among H_0, H_1 and H_2 under the conditions of the probability density function depending on an unknown parameter.

The trivariate hypothesis model may be expressed as $\begin{cases} H_0: x(t)=n(t) \\ H_1: x(t)=s(t)+n(t) \\ H_2: x(t)=j(t)+n(t) \end{cases}$

The detection relation determined as per figures 6-11 is

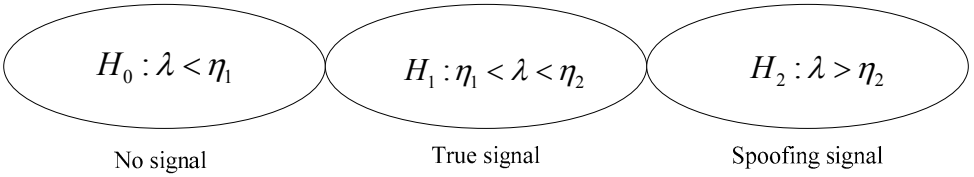


Figure 2 Relations with detection threshold

The key to correctly acquiring navigation signal and detecting spoofing interference is how to set the two thresholds η_1 and η_2 rationally. False alarm will be incurred if the threshold values are too small; missed alarm will be incurred if the threshold values are too large. The value of the detection threshold η_1 can be worked out with the Equation (10) given in the previous section.

In the presence of a navigation signal or a spoofing signal, $\lambda \gg \sigma_n^2$, then the mean value of the statistical quantity V can be approximately expressed as:

$$E(V) = \sqrt{\frac{\pi}{2}}\sigma_n L_{1/2}\left(-\frac{\lambda^2}{2\sigma_n^2}\right) \approx \lambda \tag{11}$$

It is already known that the navigation signal and the spoofing signal have the same distribution separately but different distribution mean values. Let's assume their mean values are λ_1 and λ_2 respectively, and their relation is as shown in figure 6, then, it is possible to derive their probability density functions from Equation(8) and Equation(11), which are expressed as follows respectively:

$$f(v,\lambda_1) = \frac{v}{\sigma_n^2} e^{-\frac{v^2+\lambda_1^2}{2\sigma_n^2}} I_0\left(\frac{\lambda_1 v}{\sigma_n^2}\right) \tag{12}$$

$$f(v,\lambda_2) = \frac{v}{\sigma_n^2} e^{-\frac{v^2+\lambda_2^2}{2\sigma_n^2}} I_0\left(\frac{\lambda_2 v}{\sigma_n^2}\right) \tag{13}$$

Where, λ_1 represents the non-coherent integration mean value of navigation signal and λ_2 represents the non-coherent integration mean value of the spoofing signal, $\lambda_2 > \lambda_1$.

The false alarm probability P_{fa2} of spoofing interference detection is expressed as:

$$P_{fa2} = \int_{\eta_2}^{\infty} f(v,\lambda_1)dv = \int_{\eta_2}^{\infty} \frac{v}{\sigma_n^2} e^{-\frac{v^2+\lambda_1^2}{2\sigma_n^2}} I_0\left(\frac{\lambda_1 v}{\sigma_n^2}\right)dv \tag{14}$$

If $v/\sigma_n = x$, then

$$P_{fa2} = \int_{\eta_2\sigma_n}^{\infty} x e^{-\frac{x^2+\frac{\lambda_1}{\sigma_n}}{2}} I_0\left(\frac{\lambda_1}{\sigma_n}x\right)dx = Q\left(\frac{\lambda_1}{\sigma_n}, \eta_2\sigma_n\right) \tag{15}$$

Where, η_2 represents the preset spoofing detection threshold and $Q_K(a,b)$ represents the generalized Marcum 's Q function.

$$Q_K(a,b) = \int_b^{\infty} x\left(\frac{x}{a}\right)^{K-1} e^{-(x^2+a^2)/2} I_{K-1}(ax)dx \tag{16}$$

Conclusively, the modified spoofing interference detection algorithm in the acquisition phase can be divided into the following steps:

1) Carry out fast Fourier transform to the received navigation signal of one pseudo-code period, and convert the output to the frequency domain to obtain $X(k)$, where,. $n = k = 0,1,\cdots,N$.

2) Take the complex conjugate of $X(k)$ to get $X(k)^*$.

3) Generate a number of native-code signals $q_{si}(n)$ corresponding to the frequency steps within the frequency scope of search using Equation (6), where, $i = 1,2,\cdots,M$ represents the corresponding number of search channel and $s = 1,2,\cdots,S$ represents the searching frequency step.

4) Carry out FFT conversion to convert $q_{si}(n)$ to frequency domain and get $q_{si}(k)$.

5) Complete a point-to-point multiplication between $X(k)^*$ and $q_{si}(k)$ to get $R_{si}(k)$.

6) Perform inverse Fourier transform to convert $R_{si}(k)$ to the time domain and get its absolute value $|r_{si}(n)|$. There are a total of $S \times N$ values for every channel.

7) Conduct a frequency-phase 2D search among $S \times N$ $|r_{si}(n)|$ values and compare each of them with the preset detection threshold. Consider the presence of a signal when a value is higher than the threshold. If there are two separate peaks higher than the threshold, it is believed the presence of repeater spoofing interference. Determine it is a navigation signal or a repeater spoofing signal with reference to the arrival time at the corresponding position.

8) If only one peak is detected, perform L times of non-coherent accumulation to the searched data.

9) Compare the acquired correlation peak values with the preset threshold η_2. Consider the presence of spoofing interference if the peak value is greater than the threshold η_2; take it as a true navigation signal if the peak value is less than the threshold η_2.

The flow chart of the entire detection process is as shown in the figure below.

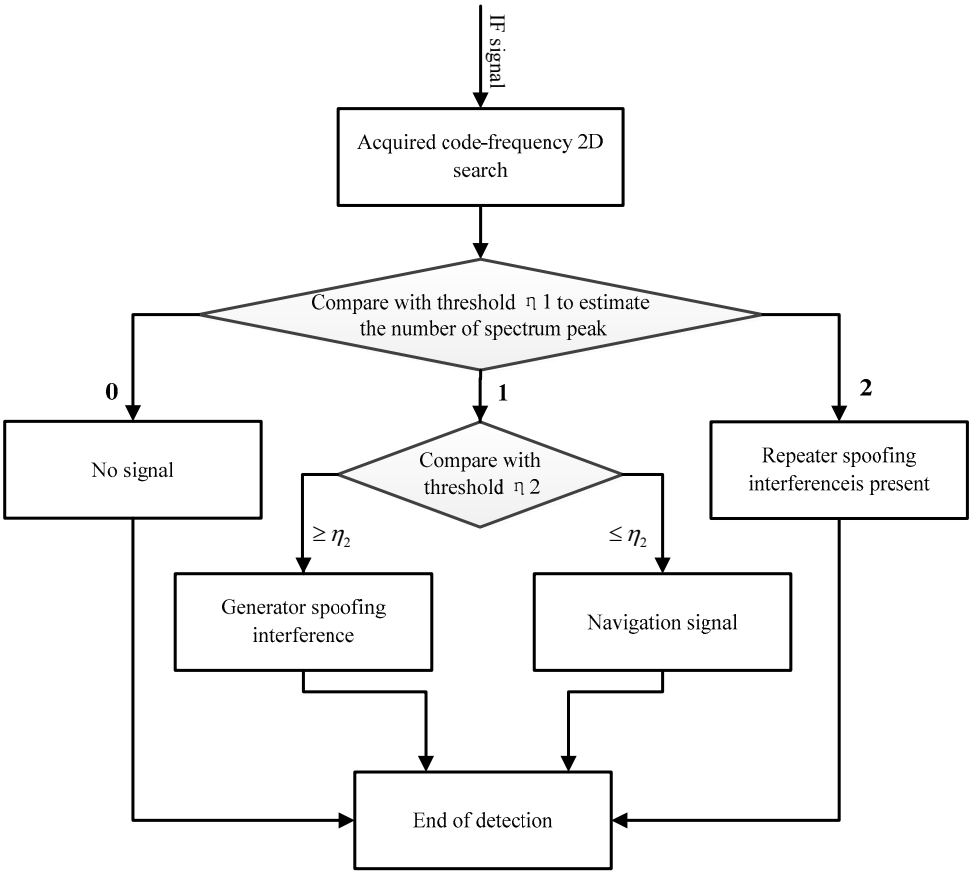
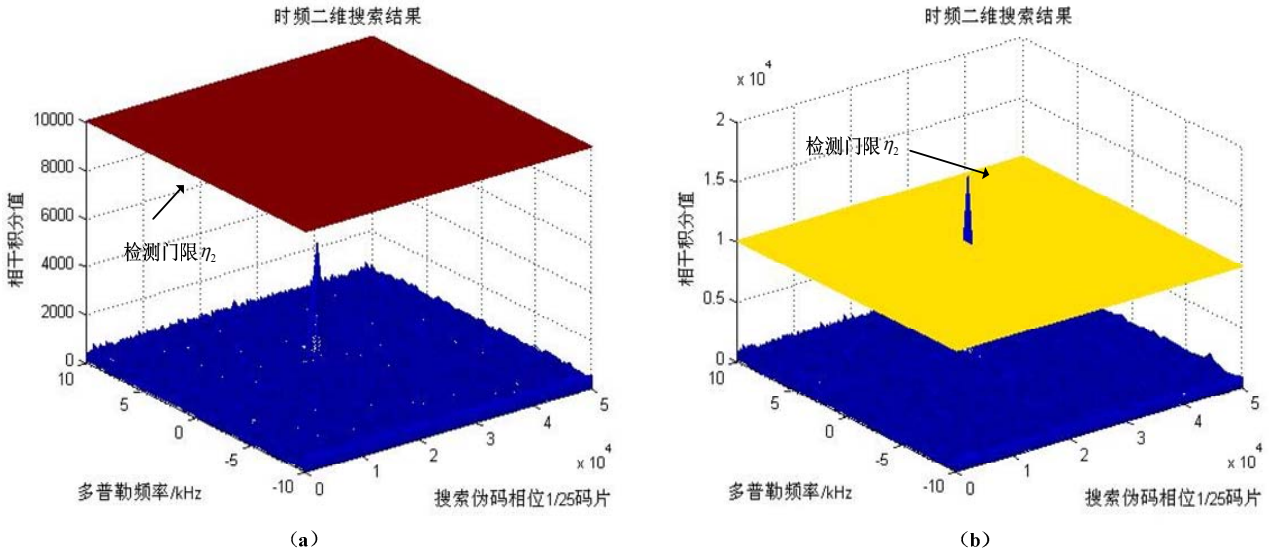


Figure3 Flow chart of detection process

The detection performance of the algorithm is simulated below. Taking the civil signal at B1 frequency point as example, let's assume the length of the received signal after coherent integration is 1ms, the sampling frequency is 50MHz, the carrier frequency is 20mhz, the SNR is -20dB and the Doppler frequency shift is 1KHz for the received signal in one channel, the SNR is -10dB and the Doppler frequency shift is 2KHz for the received signal in the other channel. The graph after code-frequency 2D research with the proposed algorithm is as shown in 错误!未找到引用源。8.



（a） （b）

Figure 4 Energy detection in the acquisition phase错误!未找到引用源。8 shows the energy detection results to the correlation peak after the 2D acquisition search, where (a) represents the peak detection to navigation signal and (b) represents the peak detection to spoofing signal. It is clear that the energy of navigation signal is less than the detection threshold η_2 in (a) and the energy of spoofing signal is greater than the detection threshold η_2 in (b). It demonstrates that this algorithm has good performance in detection of spoofing signal of power higher than navigation signal.

Of simple structure, this detection method does not require additional equipment for the original receiver to complete detection for spoofing interference, which adds it a certain value of promotion. However, this technique has its limitation because spoofing signal and navigation signal share the same signal format and the same probability distribution, and they are identified from each other only by different power levels. When a navigation signal is of high power, it is very likely to identify it as a spoofing signal; when a spoofing signal is of low power, it is very likely to identify it as a navigation signal. Besides, the search precision is relatively low in the acquisition phase. If the time difference between a repeater spoofing signal and a true navigation signal arriving at the receiver is within one chip, the detection and identification will fail.

Conclusion

Concerning the detection vulnerability of spoofing interferences in the acquisition phase, this paper proposes a detection and identification technique that combines the arrival time of received signal with the acquisition of correlation peaks. After deriving the probability density function distributions of noise, received spoofing signal and navigation signal, it suggests two detection thresholds as well as the relation between detection probability and false alarm probability. Finally, the algorithm performance is analyzed by means of simulation. This algorithm is expected to have good application prospects because it is simple in structure and easy to implement in addition to no additional equipment required for the existing receiver..

References

[1] Basker S. Jamming:A Clear and Present Danger[J].GPS World.2010.21(4):8-9.

[2] Anonymous. Global Positioning System Impact to Critical Civil Infrastructure (GICCI)[R].Naval Surface Warfare Center,2009.

[3] He Sihua, Li Tianwei, Han Yundong: A Research of GPS Jamming Technology in Navigation Wars [J]. Shipboard Electronic Countermeasure, 2004, 27(1): 24-27.

[4] NielsenJ，Broumandan A, Lachapelle G.. Gnss spoofing detection for single antenna handheld.

[5] Psiaki, Mark L.;O'Hanlon, Brady W.;Bhatti, Jahshan A.;Shepard, Daniel P.，GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals[J]，Aerospace and Electronic Systems, IEEE Transactions on,pp:2250-2267.

[6] Logan Scott LS Consulting Anti-Spoofing & Authenticate Signal Architectures for Civil Navigation Systems.

[7] Geng Zhenglin, Nie Junwei and Wang Feixue: a research on GNSS anti-spoofing technology [J]. Global Positioning System, 2013, 38(4): 65-70.

[8] Huang Long, Gong Hang, Zhu Xiangwei and Wang Feixue: A Research on Repeater Spoofing Techniques against GNSS Time Service Receiver [J]. Journal of National University of Defence Technology, 2013, 35(4): 93-96.

[9] Huang Long, Lv Zhicheng and Wang Feixue: A Research on Spoofing Interference against GNSS Receiver [J]. Acta Astronautica, 2012, 33(7): 884-890.