Symmetry detection algorithm to detect forwarded spoofing interference signals of BOC modulation receivers

Zhiying Wang, Yucen Liu and Menglan Wang*
Satellite Navigation Center, Beijing, 100094, China
*Corresponding author’s e-mail: 862780529@qq.com

Abstract. In this paper, the symmetry detection algorithm based on the symmetry of binary offset carrier (BOC) modulation signals is proposed to solve the problem of the global navigation satellite system (GNSS) spoofing interference in BOC modulation and acquisition phase which set on the base of the characters of correlation peaks, and achieve the detection of the forwarded spoofing interference signals. The theoretical value and the simulation value of the receiver operating characteristic (ROC) curve of the symmetry detection algorithm can be obtained by the numerical calculation and the experimental simulation. It can be seen from the simulation that with the increase of the accumulation times after the correlation, the signal to noise ratio (SNR) of the spoofing signal compared to the real signal, and the SNR of the real signal, the detection probability of the spoofing signal increases as well. When the power of the spoofing signal is 3 dB greater than that of the real signal, the detection probability can be more than 99% under the condition that the false alarm probability is 0.1%. Given that it only needs to add the module to the software receiver to detect spoofing signals, the algorithm proposed in this paper is of practical significance.

1. Introduction
With the development of the global navigation satellite system (GNSS) and the continuous expansion of its application field, its security has been widely concerned by people from all walks of life[1]. Spoofing as a malicious attack, sends forged or delayed navigation signals to the target receiver to mislead it into wrong position and time information, causing serious consequences[2-3]. Nowadays, the binary offset carrier (BOC) modulation technology is used in many navigation satellite systems, and the existing spoofing detection algorithms are aimed at the binary phase shift keying (BPSK) modulation signals[4]. In this paper, a symmetry detection algorithm of the forwarded spoofing signals is proposed by using the symmetry of correlation peak secondary peak with respect to main peak of the BOC modulated signal under the condition of the small delay.

2. Algorithm principle
BOC modulation symmetry detection algorithm of forwarded spoofing interference works in phase of pseudocode acquisition of navigation receivers. In the condition of small delay, it uses the symmetry of correlation peak secondary peak with respect to main peak of the BOC modulated signal, establishing model by calculating the accumulation of square difference value of correlation peak secondary peaks to achieve the detection of forwarded spoofing interference.

As shown in figure 1, the condition of small delay stands for the procedure of alignment between secondary peaks of the spoofing signal’s and real signal’s correlation peaks when the relative delay between correlation peaks of the spoofing signal and the real signal is less than 2 chips.
Based on the knowledge of statistical signals, the binary assumptions can be constructed.

\( H_0 \): There is no spoofing interference.
\( H_1 \): There is spoofing interference.

Through this binary detection, it can ensure that receiver can move into tracking phase normally after capturing the real signal.

![The real signal](https://example.com/real_signal.png) ![The spoofing signal](https://example.com/spoofing_signal.png)

Figure 1. The schematic diagram of the small delay condition.

The premise of adopting the algorithm is that the real signal’s main peak of correlation is not deformed.

In the process of signal transmission, the baseline complex signal can be expressed as equation (1), the real signal can be expressed as equation (2), and the spoofing signal can be expressed as equation (3).

\[
\text{s}_{IF}(t) = s(t) + j(t) + w(t) \\
s(t) = A d(t - \tau) \chi(t - \tau) c(t - \tau) e^{\left[ j 2 \pi f (t - \tau + \phi) \right]} \\
j(t) = k A d(t - \tau - \tau_0) \chi(t - \tau - \tau_0) c(t - \tau - \tau_0) e^{\left[ j 2 \pi f (t - \tau - \tau_0 + \phi) \right]}
\]

The reference signal of receivers can be expressed as

\[
h(t) = \chi(t) c(t) e^{j(2\pi f + \phi)}
\]

In the process of signal acquisition, the receiver despreads the carrier doppler and searches the field of code phase, and the output of the correlator can be expressed as

\[
x_n = \frac{1}{T_c} \int_{nT_c}^{(n+1)T_c} s_{IF}(t) h(t)^* \, dt = R_n + w_n, t \in [nT_c, (n+1)T_c], n = 1, \ldots, N
\]

In equation (5), \( R_n \) is the correlation peak value of the signal, \( w_n \) is the Gaussian white noise independent from the signal.

Under the binary assumptions, the correlator output is normally distributed.
Under the assumption of $H_0$, the received signal is real. The value of the left secondary peak is $R_1^{(1)}$ and the right one is $R_2^{(1)}$. Then the assumption of $H_0$ can be expressed as
\[
x_n(n) H_0 = x_1(n) - x_2(n) = w_2(n) - w_1(n) - N(0, 2\sigma_n^2)
\]  

Under the assumption of $H_1$, the secondary peak is deformed because of spoofing. The value of the left secondary peak value is $R_1^{(2)}$ and the right one is $R_2^{(2)}$. Then the assumption of $H_1$ can be expressed as
\[
x_n(n) H_1 = x_1(n) - x_2(n) = R_1^{(2)} - R_1^{(1)} + w_2(n) - w_1(n) - N(\Delta R^{(2)}, 2\sigma_n^2)
\]  

In equation (7), $\Delta R^{(2)} = R_2^{(2)} - R_1^{(2)}$.

Then the above two assumptions can be expressed as
\[

H_0 : x_n = \frac{1}{T_e} \int_{-T_e/2}^{T_e/2} w(t) h(t) \, dt = w_n
\]
\[

H_1 : x_n = \frac{1}{T_e} \int_{-T_e/2}^{T_e/2} A(t) \, dt + \frac{1}{T_e} \int_{-T_e/2}^{T_e/2} w(t) h(t) \, dt = R_n + w_n
\]

In equation (8), the normalization condition $\int_{-T_e/2}^{T_e/2} |h(t)|^2 \, dt = 1$. $A(t)$ represents the channel gain of the synthesized signal.

Based on the above analysis, the receiver can construct such binary assumptions by accumulating the value of the square difference between secondary peaks of the signal to determine whether there is a spoofing interference signal.

So the test statistic of the binary hypothesis can be expressed as
\[
T = T(x) = X^T X = \sum_{n=1}^{N} x_n^2
\]

In equation (9), the test statistic $T$ represents the accumulation of square difference value between secondary peaks of correlation of the synthesized signal. Based on the hypothesis of module, the test statistic is central chi-square distribution whose degree of freedom is $N$ in the condition of $H_0$. In the condition of $H_1$, the test statistic $T$ is non-central chi-square distribution whose degree of freedom is $N$.

Under the assumption of $H_0$, the probability density function (PDF) of the test statistic $T$ can be expressed as
\[
f_{T|H_0}(T) = \begin{cases}
\frac{1}{T^{n/2-1}} \exp\left(-\frac{T}{2\sigma_n^2}\right), & T > 0 \\
0, & T < 0
\end{cases}
\]  

In equation (10), the gamma function $\Gamma(u)$ can be expressed as
Γ(u) = \int_0^{\infty} t^{\nu-1} \exp(-t) \, dt \hspace{1cm} (11)

Under the assumption of \( H_1 \), the PDF of the test statistic \( T \) can be expressed as

\[
f_{T|H_1}(T) = \begin{cases} 
\frac{1}{2} \left( \frac{T}{\lambda \sigma_n} \right)^{\frac{N-2}{2}} \exp \left( -\frac{1}{2} \left( \frac{T}{\sigma_n} + \frac{\lambda}{\sigma_n} \right) \right) \frac{\Gamma_{N-1} \left( \frac{\lambda T}{\sigma_n} \right)}{\Gamma_{\frac{N-1}{2}} \left( \frac{\lambda}{\sigma_n} \right)} & , \quad T > 0 \\
0 & , \quad T < 0
\end{cases} \hspace{1cm} (12)
\]

In equation (12), the non-central parameter \( \lambda = \frac{1}{\sigma_n} \sum_{n=1}^{N} |\Delta_n^{(2)}|^2 \). The three-order modified Bessel function \( I_r(u) \) can be expressed as

\[
I_r(u) = \frac{\left( \frac{u}{2} \right)^r}{\sqrt{x\Gamma(x + \frac{1}{2})}} \int_0^\infty \exp(u \cos \theta) \sin^2 \theta d\theta \hspace{1cm} (13)
\]

We can obtain the probability density map of the test statistic \( T \) under the two assumptions, as shown in figure 2.

![Figure 2. The PDF of the test statistic T under the two assumptions.](image)

Proper selection of the detection threshold \( \gamma \) reasonably is essential for good performance of the detector. On the one hand, if the threshold is too low, it may lead to false alarms, which means that the detector treats noise as a real signal. On the other hand, if the threshold is too high, it may lead to missing detection, which means that the detector cannot detect the existing spoofing signals.

So the false alarm probability \( P_{FA} \) should be selected first, and then the detection threshold \( \gamma \) can be obtained.

According to Neyman-Pearson lemma[5], the false alarm probability \( P_{FA} \) can be expressed as

\[
P_{FA} = Pr \{ T > \gamma \mid H_0 \} = \int_{\gamma}^{\infty} f_{T|H_0}(T) \, dT \hspace{1cm} (14)
\]
In equation (14), \( \gamma \) represents the judgement threshold of detection statistics, which can be expressed as

\[
\gamma = F_{T|\mu_0}^{-1}(1 - P_{FA}) \tag{15}
\]

In equation (15), \( F_{T|\mu_0}^{-1} \) represents the cumulative distribution function of the detection statistics \( T \) under the assumption of \( H_0 \), which can be expressed as

\[
F_{T|\mu_0}(T) = \int_0^T \frac{1}{2^{\frac{N}{2}} \Gamma(\frac{N}{2})} T^{\frac{N-1}{2}} \exp(-\frac{T}{2\sigma_n^2})dT \tag{16}
\]

As the detection threshold are selected, the detection probability \( P_D \) of a real spoofing signal being detected can be expressed as

\[
P_D = Pr\{T > \gamma | H_1\} = \int_{\gamma}^{\infty} f_{T|H_1}(T)dT \tag{17}
\]

### 3. Detection method

The detection process is shown in figure 3. If there is a spoofing signal during the acquisition phase of the receiver while the relative delay of the correlation peak of the spoofing signal and the actual signal is less than 2 chips, we can make such a hypothesis statistics by using the deference of secondary peaks of two sides, when these two correlation peaks start contacting and deforming. Comparing detection statistics with threshold fixed, if it is more than threshold receiver will claim there is a spoofing signal, otherwise receiver will switch to the tracking phase according to the normal process.

![Figure 3. The procedure of symmetry detection algorithm.](image_url)

The steps of symmetry detection algorithm are as follows:
• Receivers can obtain the complexed baseband signal \( x(n) = I(n) + jQ(n) \) by multiplying the received signal with the in-phase and quadrature signal produced by local oscillator to get the fast Fourier transform \( X(k) \) of \( x(n) \), \( n = k = 0, 1, 2, \cdots, N \).

• Receivers calculate the fast Fourier transform \( H(k) \) of \( h(n) \) which is the product of local recurrence code and square subcarrier, and we can get the conjugate value \( H^*(k) \).

• Receivers can obtain \( P(k) \) by multiplying \( X(k) \) and \( H^*(k) \), and do the reverse Fourier transform to \( P(k) \) to get \( r(n) \), then modulo \( r(n) \) to get \( |r(n)| \).

• Based on the last step, receivers can obtain main peak of correlation \( R \) and secondary peaks \( R^{(1)} \). And then receivers can get the detection statistics \( T \) by calculating the square of difference between two secondary peaks.

• Comparing detection statistics \( T \) with threshold \( \gamma \), if \( T \) is bigger than \( \gamma \), which means there is a spoofing signal, receivers will issue a warning, otherwise receivers will step into capture phase which means the received signal is real.

The steps of symmetry detection algorithm are as follows:

4. Simulation verification

Based on such an analysis, expressions of false alarm, threshold, deception detection probability and probability density function and cumulative distribution function of detection statistics \( V \) in two hypothesis conditions, now we can obtain the theoretical and simulation value of the receiver operating characteristic (ROC) curve of the symmetry detection algorithm through numerical calculations and stimulation.

According to the literature, the power of the received satellite navigation signals is about the same when signals reach the ground, while the carrier-to-noise ratio is in the range of 35 ~ 55 dB·Hz roughly [6]. Therefore, for a capture process using a coherent integration with an integration step size of 1 ms, the signal-to-noise ratio of the correlator output result is in the range of 5 ~ 25 dB.

Assumed that the BOC modulation receiver was interfered by the forwarded spoofing signal, we would use MATLAB software to verify the effectiveness of algorithm proposed by two simulation experiments. During the simulation, the carrier to noise ratio (CNR) of the received real signal is 35 dB·Hz or 37 dB·Hz, the coherent integration time is 1 ms and the number of accumulated \( N \) (the degree of freedom) after correlation is 1, 3 or 5.

If the CNR of the real signal is 35 dB·Hz, the signal to noise ratio (SNR) of output is 5 dB after the correlation of 1 ms. If the CNR of the real signal is 37 dB·Hz, the SNR of output is 7 dB after 1 ms’ correlation. We will do Monte Carlo simulation for 5000 times, and the parameters is shown in table 1.

| Parameter  | The real signal/dB | The spoofing signal/dB |
|------------|--------------------|------------------------|
| Experiment A | 5                  | 7                      |
|            |                    | 8                      |
| Experiment B | 7                  | 9                      |
|            |                    | 10                     |

In Experiment A, the SNR of the real signal is 5 dB, while the SNR of the spoofing signal is 7 dB and 8 dB respectively.

Under the condition that the SNR of the spoofing signal is 7 dB in Experiment A, the ROC curve of symmetry detection is shown in figure 4. In figure 4, the horizontal axis is the false alarm probability of the spoofing signal, the vertical axis is the detection probability of the spoofing signal. The solid line is theoretical value of numerical calculation, circle is the stimulation value of Monte Carlo simulation. If the SNR of the spoofing signal is 2 dB more than that of the real signal, in the condition of same false alarm probability, with increasing of accumulation times \( N \) after correlation, the
probability of detecting the spoofing signal may get higher. When the degree of freedom is 1 and the false alarm is 2%, the detection probability can only reach over 46%. When the degree of freedom is 3 and the false alarm is 2%, the detection probability will be over 85%. When the degree of freedom is 5 and the false alarm is 2%, the detection probability can will be more than 96%.

Figure 4. The ROC curve of symmetry detection (the SNR of the spoofing signal is 7 dB).

Under the condition that the SNR of the spoofing signal is 8 dB in Experiment A, the ROC curve of symmetry detection is shown in figure 5. In figure 5, it can be seen that when the degree of freedom is 1 and the false alarm is 2%, the detection probability may be more than 57%. When the degree of freedom is 3 and the false alarm is 2%, the detection probability may be more than 93%. When the degree of freedom is 5 and the false alarm is 2%, the detection probability may be more than 99%.

According to figure 4 and figure 5, it can be seen that the simulation results agree with the numerical calculations. When the SNR of the real signal is the same, the detection probability of the spoofing signal increases as the SNR of the spoofing signal increases.

Figure 5. The ROC curve of symmetry detection (the SNR of the spoofing signal is 8 dB).
In Experiment B, the SNR of the real signal is 7 dB, while the SNR of the spoofing signal is 9 dB and 10 dB respectively.

Under the condition that the SNR of the spoofing signal is 9 dB in Experiment B, the ROC curve of symmetry detection is shown in figure 6. When the false alarm probability is the same, the detection probability of the spoofing signal increases as the accumulation times after the correlation increases. When the degree of freedom is 5 and the false alarm is 0.2%, the detection probability is more than 98%.

![Figure 6. The ROC curve of symmetry detection (the SNR of the spoofing signal is 9 dB).](image)

Under the condition that the SNR of the spoofing signal is 10 dB in Experiment B, the ROC curve of symmetry detection is shown in figure 7. It can be seen that the SNR of the spoofing signal is 3 dB more than that of the real signal, when the degree of freedom is 5 and the false alarm is 2%, the detection probability is more than 99%.

![Figure 7. The ROC curve of symmetry detection (the SNR of the spoofing signal is 10 dB).](image)
According to the figure 4 – 7, it can be seen that the detection probability of the spoofing signal increases as the SNR of the real signal increases.

In summary, with the increase of accumulation times after correlation, the SNR of the spoofing signal relative to the real signal, and the improvement of the SNR of the real signal, the detection probability gets higher and the theoretical values of numerical calculation agree with the Monte Carlo simulation. When power of the spoofing signal is 3 dB more than the power of the real signal, the detection probability can achieve 99% under the condition of the false alarm probability is 0.1%.

5. Conclusion
In this paper, the symmetry detection algorithm based on the symmetry of BOC modulation signals is proposed to detect forwarded spoofing interference signals of BOC modulation receivers. The algorithm uses the symmetry of secondary peak of correlation with respect to main peak of correlation of the BOC modulated signal to achieve the detection of forwarded spoofing interference signals. The performance of the algorithm can be seen from the simulation. With the increase of the accumulation times after the correlation, the SNR of the spoofing signal compared to the real signal, and the SNR of the real signal, the detection probability of the spoofing signal increases as well. When the power of the spoofing signal is 3 dB more than the power of the real signal, the detection probability can achieve 99% under the condition that the false alarm probability is 0.1%. Given that there is only need to add the module to the software receivers to detect spoofing signals, the algorithm proposed in this paper is of practical significance.

References
[1] Wullems, C.J. (2012) A spoofing detection method for civilian L1 GPS and the E1-B Galileo safety of life service. IEEE Transactions on Aerospace and Electronic Systems, 48:2849–2864.
[2] Hatch, R., Sharpe, R., Yang, Y. (2004) An innovative algorithm for carrier-phase navigation. Proceedings of ION GNSS, Long Beach, CA, USA.
[3] Kaplan, E.D. (2006) Understanding GPS principles and applications. Artech House, Boston, USA.
[4] Wei, X. (2011) Research on GPS signal interference technology modulated by BOC. Electronic design engineering, 19:139–144.
[5] Luo, P., Zhang, W. (2014) Basics of Statistical Signal Processing: Estimation and Detection Theory. Publishing House of Electronics Industry, Beijing.
[6] Xie, G. (2009) Principles of GPS and Receiver Design. Publishing House of Electronics Industry, Beijing.