Multi-peak and power cooperative detection algorithm to detect forwarded spoofing interference signals of BOC modulation receivers

Zhiying Wang¹, Jiawen Wang¹ and Yidong He²*
1 32021 Troops, Beijing, 100094, China
2 Satellite Navigation Center, Beijing, 100094, China
*Corresponding author’s e-mail: 1012807308@qq.com

Abstract. In this paper, the multi-peak and power cooperative detection algorithm is proposed to detect forwarded spoofing interference signals of satellite navigation BOC modulation receivers without considering suppression interference. The theoretical value and the simulation value of the ROC curve of the multi-peak and power cooperative 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 number of accumulations after the receiver correlation value and the power intensity of the spoofing signal relative to the real signal, the detection probability of the proposed algorithm is higher. When the power of the spoofing signal is 3 dB greater than that of the real signal, the detection probability can be more than 90% under the condition that the false alarm probability is 5%. While when the power of the spoofing signal is 4 dB greater than that of the real signal, the detection probability can be more than 95% under the condition that the false alarm probability is 0.7%. 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
The Global Navigation Satellite System (GNSS) has become indispensable infrastructures for promoting economic development and maintaining national security. With the continuous development of GNSS technology, binary offset carrier (BOC) modulation technology, which has been seen as a new modulation method, has been used in modernization schemes of GNSS. Moreover, the vulnerability and potential risks of BOC modulation technology have attracted widespread attention. In 2011, Iran captured the US military unmanned reconnaissance aircraft RQ-170 successfully [1], which stimulated the US military to accelerate research on anti-spoofing interference technology greatly. In the GNSS conference organized by the Institute of Navigation (ION) in 2011, there were 18 articles on spoofing and anti-spoofing technology of GNSS, which was the sum of the number of similar research articles in the ION conference in the past 10 years [2]. In 2012, the US Naval Research Office and Rockwell Collins reached the Modern Integrated Spoofing Tracking (MIST) contract to research anti-spoofing technology, which was against attempts by the enemy to disrupt military operations by interfering with GPS signals [3]. Therefore, it can be seen that spoofing and anti-spoofing technology have attracted more and more attention.

Spoofing detection technology is the first step and a key step in the research on anti-spoofing technology. At present, the main anti-spoofing methods include signal encryption authentication...
detection [4], signal arrival time detection [5], signal arrival angle detection [6], signal power detection [7], multi-peak detection [8] and so on. Each detection method has its own shortcomings and applicable scenarios. Meanwhile, there are deficiencies in using only one single detection method. In this paper, the multi-peak and power cooperative detection algorithm is proposed to detect forwarded spoofing interference signals of BOC modulation receivers without considering suppression interference. At the same time, the calculation method of the decision threshold and the corresponding ROC curves are given.

2. Algorithm principle
Forwarded spoofing interference is to receive the real satellite signal through its own antenna, delay appropriately, amplify and transmit to the target receiver to interfere with it. Since the pseudo codes and the navigation messages contained in the signal are all from real navigation satellites, there is no need to know the pseudo code sequence and the navigation message structure of the navigation signal received by the target receiver. Forwarded spoofing interference can deceive many satellite navigation receivers effectively, including military receivers. The principle of forwarded spoofing interference is shown in Figure 1.

![Figure 1. The principle of forwarded spoofing interference.](image)

The multi-peak and power cooperative detection algorithm combines the multi-peak detection method and the signal power detection method to detect forwarded spoofing interference of BOC modulation receivers. It works in the capture phase of the pseudo code of the navigation receiver. If there is no spoofing signal, when the capture threshold is set appropriately, there will be only one correlation peak higher than it typically. Conversely, if there is a spoofing signal, there will be multiple correlation peaks higher than the threshold. It can be seen from the difference between the two cases that when several correlation peaks which are larger than the threshold are detected, at least one spoofing signal exists in the currently received signals. At this time, the spoofing signal can be detected for the power of the spoofing signal is greater than that of the real signal.

![Figure 2. The real signal in the capture phase.](image)  ![Figure 3. The spoofing signal in the capture phase.](image)

If only one signal was detected during the two-dimensional search including carrier Doppler and code phase, it indicates that the signal should be a real satellite signal, and the receiver should track the signal subsequently, as shown in figure 2. If multiple correlation peaks were detected, there would be a spoofing interference signal in the current signal, as shown in figure 3.
Therefore, the following ternary detection problem can be constructed.

- \( H_0 \): There is no signal at the current carrier Doppler and code phase search cell.
- \( H_1 \): There is a real signal at the current carrier Doppler and code phase search cell.
- \( H_2 \): There is a spoofing signal at the current carrier Doppler and code phase search cell.

By constructing the ternary detection problem mentioned above, it is ensured that the receiver track the real signal normally, thereby preventing forwarded spoofing interference from influencing the final positioning result of the receiver.

3. Detection method

In the process of capturing the satellite signal by the receiver, the received signal is mixed with the sinusoidal replica carrier on the same branch and the cosine replica carrier on the orthogonal branch of the same receiving channel firstly. Then, the mixing result is correlated with the copied C/A code to obtain correlation results named \( i \) and \( q \). The correlation results \( i \) and \( q \) generate \( I \) and \( Q \) after the coherent integration of time \( T_c \). Finally, \( I \) and \( Q \) are subjected to non-coherent integration calculation to obtain the amplitude \( A \) of the incoherent integration. If there was a forwarded spoofing interference signal, its power would be higher than that of the real one in order to achieve deception. Therefore, the value of \( A^2 \) can be used to determine whether there is a forwarded spoofing interference signal. If \( A^2 \) was less than the threshold \( \rho_1 \), it indicates that the signal would not have been searched yet. If \( A^2 \) was greater than the threshold \( \rho_1 \) and less than the threshold \( \rho_2 \), then the real signal should be in the search cell. If \( A^2 \) was greater than the threshold \( \rho_2 \), then the forwarded spoofing interference signal should be in the search cell. Figure 4 shows the decision process of the forwarded spoofing interference signal.

\[
\begin{align*}
\text{The mixer} & \quad \text{The correlator} \\
\cos 2\pi ft & \quad i \quad \int I \\
-sin 2\pi ft & \quad q \quad \int Q \\
\text{The local carrier} & \quad \text{The subcarrier}
\end{align*}
\]

Figure 4. The decision process of the forwarded spoofing interference signal.

It is assumed that the difference of the code phase of the correlation peak between the spoofing signal and the real signal is significant. During the signal capture phase, the receiver despreads each of the carrier Doppler and code phase search cells, and the correlator output is

\[
x_n = \frac{1}{T_c} \int_{a_{t_n}}^{(a_{t+1})T_c} s_{IF} (t) s_{0} (t) \, dt
\]

In equation (1), \( s_{IF} (t) \) is the received signal, \( s_{0} (t) \) is the reference signal of the receiver, \( t \in \left[ nT_c, (n+1)T_c \right] \).

Then the above three assumptions can be expressed as

\[
\begin{align*}
H_0 : x_n &= \frac{1}{T_c} \int_{a_{t_n}}^{(a_{t+1})T_c} w(t) s_{0} (t) \, dt = w_n \\
H_1 : x_n &= \frac{1}{T_c} \int_{a_{t_n}}^{(a_{t+1})T_c} A^{(1)} (t) \, dt + \frac{1}{T_c} \int_{a_{t_n}}^{(a_{t+1})T_c} w(t) s_{0} (t) \, dt = s_{n}^{(1)} + w_n \\
H_2 : x_n &= \frac{1}{T_c} \int_{a_{t_n}}^{(a_{t+1})T_c} A^{(2)} (t) \, dt + \frac{1}{T_c} \int_{a_{t_n}}^{(a_{t+1})T_c} w(t) s_{0} (t) \, dt = s_{n}^{(2)} + w_n
\end{align*}
\]
In equation (2), the normalization condition \( \int_{a}^{(2)} \left| \delta(t) \right|^2 \, dt = 1 \), \( A^{(1)} \) represents the channel gain of the real signal, \( A^{(2)} \) represents the channel gain of the forwarded spoofing interference signal, and \( w_n \) represents the noise component.

The output of the correlator follows a normal distribution under the above assumptions

\[
x_t \big| H_0 = w_n \sim N(0, \sigma_n^2)
\]

\[
x_t \big| H_1 = s_n^{(1)} + w_n \sim N(s_n^{(1)}, \sigma_n^2)
\]

\[
x_t \big| H_2 = s_n^{(2)} + w_n \sim N(s_n^{(2)}, \sigma_n^2)
\]

The forwarded spoofing interference signal power is higher than the real signal. According to the statistical signal theory, in the additive Gaussian noise environment, the sufficient statistics of the above ternary hypothesis test can be expressed as

\[
V = h(x) = X^t X = \sum_{n=1}^{N} x_n^2
\]

According to the assumption of the model, under the \( H_0 \) condition, the test statistic \( V \) follows the centralized Chi square distribution, while under the conditions of \( H_1 \) and \( H_2 \), the test statistic \( V \) follows the decentralized Chi square distribution.

![Figure 5. The probability distribution function of the test statistic under different assumptions.](image)

By comparing with the detection thresholds \( \rho_1 \) and \( \rho_2 \), the decision is made in the ternary hypothesis in equation (7), as shown in figure 5.

If the energy of the correlation value is lower than \( \rho_1 \), there should be no signal. If the energy of the correlation value is higher than \( \rho_2 \), there should be a forwarded spoofing interference signal. If the energy of the correlation value is between \( \rho_1 \) and \( \rho_2 \), there should be a real signal.

Therefore, two types of false alarm probabilities are defined. The first type of false alarm is that a cell without a signal is detected as a cell containing a real signal or a spoofing signal. The second type of false alarm is that a cell containing a real signal is detected as a cell containing a spoofing signal.

In order not to lose generality, it is assumed that \( \rho_2 > \rho_1 \), then the threshold \( \rho_1 \) determines the first type of false alarm probability \( P_{fa1} \), which can be expressed as

\[
P_{fa1} = P \{ V > \rho_1 | H_0 \} \cup P \{ V > \rho_2 | H_0 \} = \int_{\rho_1}^{\infty} f_{V | H_0} (V) \, dV
\]

So \( \rho_1 \) can be expressed as

\[
\rho_1 = F_{V | H_0}^{-1} (1 - P_{fa1})
\]

The threshold \( \rho_2 \) determines the second type of false alarm probability \( P_{fa2} \), which can be expressed as

\[
P_{fa2} = P \{ V > \rho_2 | H_1 \} = \int_{\rho_2}^{\infty} f_{V | H_1} (V) \, dV
\]
So $\rho_2$ can be expressed as

$$\rho_2 = F_{\hat{v}_i}^{-1}(1 - P_{FA2})$$

(8)

The detection probability of the spoofing signal can be expressed as

$$P_{D2} = \int_{\rho_2}^{\infty} f_{\hat{v}_i}(V)\,dV$$

(9)

In equation (5) ~ (9), the $f_{\hat{v}_i}(.)$ represents the probability density function of the random variable $V$ under the assumption of $H_0$, $F_{\hat{v}_i}(.)$ represents the cumulative distribution function of the random variable $V$ under the assumption of $H_i$.

4. Simulation verification

According to the analysis above, the false alarm, the threshold and the detection probability have been expressed. By integrating the probability density function, the cumulative distribution function can be obtained. Substituting the cumulative distribution function of the random variable $V$ under the assumption of $H_0$ into equation (6) can obtain the threshold $\rho_1$ for signal detection.

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 [10]. 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 to 25 dB. Given that the prior information of the power of the real satellite signals and the second type of false alarm probability $P_{FA2}$, the threshold $\rho_2$ for spoofing signal detection can be obtained.

Through the above analysis, the probability density function and the cumulative distribution function of the test statistic $V$ under each hypothesis are obtained. The theoretical value and simulation value of the ROC curve of the multi-peak and power cooperative detection algorithm can be obtained by numerical calculation and experimental simulation.

Table 1. The simulation parameter settings.

| Parameter                  | Real signal | Spoofing signal |
|----------------------------|-------------|-----------------|
| Pre-detection integration time / ms | 1           | 1               |
| Carrier-to-Noise Ratio / dB·Hz | 40          | 43, 44          |
| Signal to noise ratio / dB  | 10          | 13, 14          |
| Degree of freedom (N)       | 1, 3, 5     | 1, 3, 5        |

In order to verify the effectiveness of the proposed algorithm in this paper, 1000 Monte Carlo simulations were performed using MATLAB software. The simulation parameter settings are shown in table 1. Figure 6 and figure 7 show the ROC curves of different spoofing signal-to-noise ratios and post-accumulation times under the condition that the signal-to-noise ratio of the real signal at the output of the receiver correlator is 10 dB.

Figure 6 shows the relationship between the false alarm probability and the detection probability when the signal-to-noise ratio of the real signal is 10 dB, the signal-to-noise ratio of the spoofing signal is 13 dB, and the degrees of freedom are 1, 3, and 5 respectively. It can be seen from figure 6 that in the case of the same false alarm probability, the detection probability of the spoofing signal increases as the number of accumulations after the receiver correlation value increases. When the false alarm probability is 5%, the detection probability is higher than 90%.

Figure 7 shows the relationship between the false alarm probability and the detection probability when the signal-to-noise ratio of the real signal is 10 dB, the signal-to-noise ratio of the spoofing signal is 14 dB, and the degrees of freedom are 1, 3, and 5 respectively. It can be seen from figure 7 that when the false alarm probability is 0.7%, the detection probability is higher than 95%.
Figure 6. The spoofing detection ROC curve when the spoofing signal-to-noise ratio is 13 dB.

Figure 7. The spoofing detection ROC curve when the spoofing signal-to-noise ratio is 14 dB.

By comparing figure 6 and figure 7, it can be seen that when the number of accumulations after the receiver correlation value and the false alarm probability are the same, the detection probability of the spoofing signal increases as the signal-to-noise ratio of the spoofing signal increases.

In summary, with the increase of the number of accumulations after the receiver correlation value and the power intensity of the spoofing signal relative to the real signal, the detection probability of the forwarded spoofing interference signal detection algorithm proposed in this paper is higher. When the power of the spoofing signal is 3 dB greater than that of the real signal, the detection probability can be more than 90% under the condition that the false alarm probability is 5%. When the power of the spoofing signal is 4 dB greater than that of the real signal, the detection probability can be more than 95% under the condition that the false alarm probability is 0.7%.

5. Conclusion

In this paper, the multi-peak and power cooperative detection algorithm is proposed to detect forwarded spoofing interference signals of BOC modulation receivers without considering suppression interference. When using this algorithm, there is no need to increase the hardware facilities of the receiver. What needs to be done is to add the corresponding module in the signal processing part of the software receiver to detect the spoofing signal, which is of practical significance. However, suppression interference is not considered in this paper. If suppression interference and forwarded spoofing interference were used at the same time, the noise floor of the receiver would be raised and only one peak would appear in the signal capture phase after the RF front-end AGC control. At this time, it is difficult to distinguish whether the peak represents a spoofing signal or a real signal. The above issue needs to be researched in the next step.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Nos. 61601485).

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] Wesson, K., Shepard, D., Humphreys, T. (2012) Straight talk on anti-spoofing: Securing the future of PNT. GPS World, 23: 32–34.

[3] China News Network. (2012) US company will develop technology for detecting GPS interference and deception for the US Navy. http://www.chinanews.com/mil/2012/10-18/4257529.shtml.
[4] Humphreys, T.E., Ledvina, B.M., Psiaki, M.L. (2008) Assessing the Spoofing Threat Development of a Portable GPS Civilian Spoofer. In: ION GNSS Conference. Savannah. pp. 165–176.

[5] Jafarnia, A., Broumandan, A., Nielsen, J. Lachapelle, G. (2012) GPS spooper countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. International Journal of Satellite Communications and Networking, 30: 1002–1012.

[6] Psiaki, M.L., O’Hanlon, B.W., Powell, S.P., Bhatti, J.A., Wesson, K.D., Humphreys, T.E. (2014) GNSS spoofing detection using two-antenna differential carrier phase. Programme & Abstracts the Volcanological Society of Japan, 5: 342–344.

[7] Humphreys, T.E., Ledvina, B.M., Psiaki, M.L. (2015) Research on GNSS Receiver Spoofing Detection Technology. In: China Satellite Navigation Conference. Xi’an. pp. 1–9.

[8] Yuan, D., Li, H., Lu, M. (2014) A method for GNSS spoofing detection based on sequential probability ratio test. In: ION Position. Monterey. pp. 351–358.

[9] Luo, P., Zhang, W. (2014) Basics of Statistical Signal Processing: Estimation and Detection Theory. Publishing House of Electronics Industry, Beijing.

[10] Xie, G. (2009) Principles of GPS and Receiver Design. Publishing House of Electronics Industry, Beijing.