Carrier phase double-difference GNSS spoofing detection technology based on generalized likelihood ratio

Jidong Yin¹, Le He¹ and Xuyang Lai¹
¹Aerospace Science & Industry Academy of Communication Technology Co., Ltd, Chengdu, China
E-mail: yinjidongx@126.com

Abstract: In recent years, with the wide application of Global Navigation Satellite System (GNSS), the security problem of GNSS has attracted wide attention. Spoofing interference will become an important threat to the security of satellite navigation information because of its concealment. In this paper, we propose a new double antenna structure spoofing interference detection method according to the spatial characteristics of GNSS signal. The test statistics are constructed by the generalized likelihood ratio (GLR) theory, and the GNSS spoofing interference detection methods under the same direction spoofing interference and different direction spoofing interference are obtained respectively. The feasibility of this method is verified by simulation.

1 Introduction
With the development of information technology, satellite navigation and positioning technology has been widely used in finance, civil aviation, urban transportation, weapon precision guidance and other important fields. However, the GNSS signal is extremely weak when it reaches the ground, and the ground receiving equipment is vulnerable to interference. The spoofing interference has attracted much attention because of its strong concealment and harmfulness. Effective detection technology of spoofing interference is the premise of GNSS anti-spoofing interference, and it is also an effective measure to ensure the information security of GNSS.

At present, there are a lot of research results on GNSS spoofing interference detection technology at home and abroad. The detection technology of spoofing interference based on signal characteristics mainly includes signal amplitude detection, signal arrival angle detection, signal correlation peak detection, antenna array technology and other assistant technologies [1]. Usually, the traditional spoofing interference detection method uses multiple antenna arrays, and assumes that the spoofing interference signal comes from the same direction [2-3], or an additional inertial measurement unit is needed to obtain the multi-antenna attitude information [4-5]. By analyzing the spatial characteristics of GNSS signal, when the spoofing interference signal comes from the same spoofing interference source antenna, the detection of spoofing interference can be realized by using the double difference measurement value of carrier phase with two antennas to construct a test statistic. A spoofing detection method based on dual antenna structure is introduced, which uses the fractional part of double difference carrier phase observation value to detect, and uses the normalization of double difference carrier phase observation value to carry out spoofing detection hypothesis test [6]. However, it is difficult to detect spoofing signals when they come from different antennas. The spoofing interference can be detected by using the pseudo range double difference measurement of two receivers and the
spoofing signal can be identified by analyzing the difference between the pseudo range double difference measurement value and the expected estimation value [7]. The spoofing detection method based on maximum likelihood sliding window checks the input of spoofing signal by using sliding window to compare the anomalies before and after spoofing [8]. We can estimate the baseline vector by the double difference measurement of the carrier phase with two antennas and the baseline length, construct the test statistics, and use the sum of squares of baseline vectors to judge whether there is spoofing interference [9]. In addition, based on the idea of statistical test, the consistency between the observed pseudo range measurements and the known information of satellite topology and receiver geometry can be used to check whether there is spoofing [10].

In this paper, based on the GLR theory, a new GNSS spoofing interference detection method is proposed. Using the carrier phase measurement value of two receiving antennas, the spoofing interference hypothesis test model is established for spoofing scenarios where spoofing interference comes from the same direction and spoofing interference comes from different directions. Without adding additional monitoring equipment, the spoofing interference detection method is obtained, and the feasibility of the proposed method is analyzed through simulation.

2 Detection model of double antenna GNSS spoofing interference

Let the two antennas of the receiver be in the horizontal plane. The connecting line between the two antennas is in the direction of zero azimuths. The signal incidence is shown in the figure below.

![Figure 1. GNSS signal incidence diagram.](image)

In figure 1, A and B refers to two receiving antennas, b is the baseline vector, the unit is the carrier period, S is the unit direction vector of the incident signal, and the receiver points to the direction of the signal arrival, θ and ϕ represent the angle of pitch and azimuth angle of the incident signal respectively. The position of antenna A is the coordinate origin, the straight line where AB is located is the X axis, and the horizontal plane is XOY to establish a plane rectangular coordinate system.

At the same time, the carrier phase single difference observation equation of two antennas receiving the same satellite signal is as follows [11-12]:

\[
\Delta \phi_i = b \cdot s + \Delta t + \epsilon_i
\]

\[
= |b| \cos(\psi) + \Delta t + \epsilon_i
\]

\[
= |b| \cos(\theta) \cos(\phi) + \Delta t + \epsilon_i
\]

(1)

Where \( \Delta t \) represents the delay difference between the two antennas, which is fixed for all signals. \( \epsilon_i \) is the sum of the carrier phase measurement errors of the received satellite signal \( i \), which is the Gauss white noise of variance \( 2\sigma^2 \). \( \psi_i \) is the incident angle of the signal arriving at the receiving antenna plane.

The double difference observation equation of carrier phase of two satellite signals received by two antennas is as follows:

\[
\Delta \phi_{ij} = |b| \left[ \cos(\theta_i) \cos(\phi_i) - \cos(\theta_j) \cos(\phi_j) \right] + \epsilon_{ij}
\]

(2)
Where $\epsilon_{ij} = \epsilon_i - \epsilon_j$.

It can be seen that the carrier phase difference of the same signal on the two element antennas can be expressed by the antenna baseline length and the angle of arrival. When the antenna baseline length is known, the carrier phase difference is completely determined by the angle of arrival.

3 Carrier phase double-difference test for spoofing interference

Usually, in order to induce the target receiver to obtain the wrong timing and positioning information, the spoofing interference source needs to transmit at least four or more spoofing signals. Considering the spatial characteristics of GNSS signal, when the multi-channel spoofing signal comes from the same incident direction, the carrier phase double difference measurement value of two receiving antennas at the same time is basically zero. Therefore, the hypothesis test model can be constructed by detecting whether the carrier phase double difference measurement values of any two signals at the same time are the same, and the spoofing interference identification can be carried out. When the multi-channel spoofing signals come from different incident directions, it is difficult to detect whether there is spoofing interference through the spatial characteristics of the signals because the direction of spoofing signals is unknown and the real satellite signals are also variable. However, it is not difficult to find that when there is spoofing interference, the measured value of carrier phase double difference with two antennas has an offset \cite{9}. Therefore, a hypothesis test model can be constructed by detecting the difference of carrier phase double difference of any two signals by two antennas to further determine whether there is spoofing.

3.1 Carrier phase double-difference test for same direction spoofing based on GLR

It is generally considered that the same direction spoofing interference is transmitted by a single spoofing interference source antenna, and the interference signal has the same incident direction, that is, $\theta_i = \theta_j, \phi_i = \phi_j$. The detection model of spoofing interference is established based on the fact that the spoofing interference signal reaches the receiving antenna plane in the same direction. Let the double difference of carrier phase with two antennas be $\Delta \phi$, and $\Delta \phi$ be a random variable obeying normal distribution. Construct hypothesis test: the original hypothesis $H_0$ indicates that at least one of the two signals is real signal, alternative hypothesis $H_1$ means that both signals are spoofing signals.

$$H_0 : \Delta \phi_i = \mu \left( \cos(\theta_i) \cos(\phi_i) - \cos(\theta_j) \cos(\phi_j) \right) + \epsilon_{ij}$$

$$H_1 : \Delta \phi_i = \epsilon_{ij}$$

Then, in the case of $H_0$ and $H_1$, the probability density function of the double difference measurement value $\Delta \phi$ of carrier phase with two antennas are as follows:

$$f(\Delta \phi, H_0) = \frac{1}{2\sqrt{2\pi}\sigma} \exp \left( -\frac{(\Delta \phi - \mu)^2}{8\sigma^2} \right)$$

$$f(\Delta \phi, H_1) = \frac{1}{2\sqrt{2\pi}\sigma} \exp \left( -\frac{(\Delta \phi)^2}{8\sigma^2} \right)$$

Where $\mu$ is the mean value of $\Delta \phi$ when at least one signal is true.

For a set of sample data $\Delta \phi_k (k = 1, 2, \cdots, N)$ of $\Delta \phi$, the GLR of double difference measurements of carrier phase with two antennas can be expressed as follows:

$$\lambda(\Delta \phi) = \frac{f(\Delta \phi; \hat{\mu}, \hat{\sigma}^2; H_0)}{f(\Delta \phi; \sigma^2_1; H_1)} = \prod_{k=1}^{N} \frac{f(\Delta \phi_k; H_0)}{f(\Delta \phi_k; \sigma^2_1; H_1)} = \left( \frac{\sigma^2_1}{\hat{\sigma}^2_0} \right)^{N/2}$$
\[ 2 \ln \lambda(\Delta \phi) = N \ln \left( \frac{\hat{\sigma}_0^2 + \hat{\mu}^2}{\sigma_0^2} \right) = N \ln \left( 1 + \frac{\hat{\mu}^2}{\sigma_0^2} \right) \]

The equivalent test statistics is as follows:

\[ T(\Delta \phi) = \frac{\hat{\mu}^2}{\sigma_0^2} \]  

(8)  

Where \( \hat{\mu}, \hat{\sigma}_0^2 \) are the maximum likelihood estimates of parameters \( \mu, \sigma^2 \) under the condition of \( H_0 \), and \( \hat{\sigma}_1^2 \) is the maximum likelihood estimation of parameter \( \sigma^2 \) under the condition of \( H_1 \). The estimated values are as follows:

\[ \hat{\mu} = \frac{1}{N} \sum_{k=1}^{N} \Delta \phi_k, \quad \hat{\sigma}_0^2 = \frac{1}{N} \sum_{k=1}^{N} (\Delta \phi_k - \hat{\mu})^2, \quad \hat{\sigma}_1^2 = \sum_{k=1}^{N} \Delta \phi_k^2. \]

At this time, when \( T(\Delta \phi) \geq \rho_{th}, H_0 \) is true, when \( T(\Delta \phi) < \rho_{th}, H_1 \) is true for the detection threshold \( \rho_{th} \).

The false alarm probability \( p_f \) can be expression as:

\[ p_f = \int_{-\rho_{th}}^{\rho_{th}} f(\Delta \phi, H_0) d\Delta \phi = \frac{1}{2} \text{erf} \left( \frac{\mu + \rho_{th}}{2\sqrt{2}\sigma} \right) - \frac{1}{2} \text{erf} \left( \frac{\mu - \rho_{th}}{2\sqrt{2}\sigma} \right) \]  

(9)  

Then the detection probability is

\[ p_D = \int_{-\rho_{th}}^{\rho_{th}} f(\Delta \phi, H_1) d\Delta \phi = 2\int_{0}^{\rho_{th}} f(\Delta \phi, H_1) d\Delta \phi = \text{erf} \left( \frac{\rho_{th}}{2\sqrt{2}\sigma} \right) \]  

(10)  

This method can detect GNSS same direction spoofing interference to some extent, but it has some limitations. There is still the possibility of spoofing signal in \( H_0 \) hypothesis, and it cannot be detected when the spoofing interference comes from different directions. In view of this problem, next, we will explore the test of the different directions spoofing.

3.2 Carrier phase double-difference test for different direction spoofing based on GLR

The different direction spoofing interference means that the spoofing interference signal is transmitted by multiple spoofing interference source antennas, and the interference signal has different incident direction, that is \( \theta_i \neq \theta_j, \phi_i \neq \phi_j \). At this time, the detection method of arrival angle using same direction spoofing interference will be invalid. When there is spoofing, the double difference observation equation of carrier phase with two antennas can be expressed as follows:

\[ \Delta \phi_{ij} = |b| \left[ \cos(\theta_i) \cos(\phi_i) - \cos(\theta_j) \cos(\phi_j) \right] + \Delta \phi_{ij}^{\text{spoof}} + \epsilon_{ij} \]  

(11)  

Where \( \Delta \phi_{ij}^{\text{spoof}} \) is the carrier phase double difference offset caused by spoofing interference signal.

Usually, spoofing interference will force the position of the target receiver to change slowly. We set the double differential carrier offset \( \Delta \phi_{ij}^{\text{spoof}} \) obey a uniform distribution ranging from -0.5 cycle to 0.5 cycles. Construct hypothesis test: \( H_0 \) indicates no spoofing interference, \( H_1 \) indicates existence of spoofing interference.

\[ H_0 : \Delta \phi_{ij} = |b| \left[ \cos(\theta_i) \cos(\phi_i) - \cos(\theta_j) \cos(\phi_j) \right] + \epsilon_{ij} \]  

(12)  

\[ H_1 : \Delta \phi_{ij} = |b| \left[ \cos(\theta_i) \cos(\phi_i) - \cos(\theta_j) \cos(\phi_j) \right] + \Delta \phi_{ij}^{\text{spoof}} + \epsilon_{ij} \]  

(13)  

In the presence of spoofing interference, the density function of the double difference measurement value \( \Delta \phi \) of the carrier phase with two antennas is the mixed density function after increasing the
carrier offset, that is, the mixed density function of normal distribution \( N(\mu, 4\sigma^2) \) and uniform distribution \( U(-0.5, 0.5) \). The mixed density function can be obtained by using convolution formula.

\[
f_H(\Delta \phi, H_i) = \int_{-0.5}^{0.5} \frac{1}{2\sqrt{2\pi\sigma}} \exp\left(-\frac{(\Delta \phi - x - \mu)^2}{8\sigma^2}\right) dx
\]

Let \( \Delta \phi - x = t \), then

\[
f_H(\Delta \phi, H_i) = \int_{\Delta \phi - 0.5}^{\Delta \phi + 0.5} \frac{1}{2\sqrt{2\pi\sigma}} \exp\left(-\frac{(t - \mu)^2}{8\sigma^2}\right) dt
\]

\[
= \Phi\left(\frac{\Delta \phi + 0.5 - \mu}{2\sigma}\right) - \Phi\left(\frac{\Delta \phi - 0.5 - \mu}{2\sigma}\right)
\]

(14)

Where \( \Phi(\cdot) \) is the cumulative distribution function of the standard normal distribution.

For a set of test sample data \( \Delta \phi_k (k = 1, 2, \cdots, N) \) of \( \Delta \phi \), the GLR of double difference measurement of carrier phase with two antennas is:

\[
\lambda(\Delta \phi) = \frac{f(\Delta \phi; \hat{\mu}_i, \hat{\sigma}_h^2; H_i)}{f_H(\Delta \phi; \hat{\mu}_0, \hat{\sigma}_0^2; H_0)} = \frac{\prod_{k=1}^{N} f(\Delta \phi_k; H_0)}{\prod_{k=1}^{N} f(\Delta \phi_k; H_i)}
\]

\[
= \left(\frac{1}{2\sqrt{2\pi\sigma}}\right)^N \exp\left(-\frac{N}{8}\right) \prod_{k=1}^{N} \left[ \Phi\left(\frac{\Delta \phi_k + 0.5 - \hat{\mu}_i}{2\hat{\sigma}_h}\right) - \Phi\left(\frac{\Delta \phi_k - 0.5 - \hat{\mu}_i}{2\hat{\sigma}_h}\right) \right]
\]

(15)

Where \( \hat{\mu}_0, \hat{\sigma}_0^2 \) is the maximum likelihood estimation value of \( \mu, \sigma^2 \) when \( H_0 \) is true, and the estimation result is the same as that of same direction spoofing interference test. When \( H_i \) is true, \( \left(\hat{\mu}_i, \hat{\sigma}_h^2\right) = \arg \max f_H(\Delta \phi, H_i) \).

Next, calculate the value of \( \hat{\mu}_i, \hat{\sigma}_h^2 \).

According to formula (14), the maximum likelihood estimation is used. The likelihood function is as follows:

\[
L(\mu, \sigma^2) = \left(\frac{1}{2\sqrt{2\pi\sigma}}\right)^N \prod_{k=1}^{N} f(\Delta \phi_k; H_0) ^{\Delta \phi_k + 0.5} \exp\left(-\frac{(t - \mu)^2}{8\sigma^2}\right) dt
\]

(16)

The log likelihood function is as follows:

\[
\ln\left(L(\mu, \sigma^2)\right) = -N \ln\left(2\sqrt{2\pi\sigma}\right) - \frac{1}{8\sigma^2} \sum_{k=1}^{N} (\Delta \phi_k - \mu)^2 + \frac{1}{12}
\]

The results are as follows:

\[
\hat{\mu}_i = \frac{1}{N} \sum_{k=1}^{N} \Delta \phi_k
\]

\[
\hat{\sigma}_h^2 = \frac{1}{4} \hat{\sigma}_0^2 + 48.
\]

The estimated value is brought into equation (15), when \( T(\Delta \phi) \geq \rho_{\rho_h}, H_0 \) is true, when \( T(\Delta \phi) < \rho_{\rho_h}, H_i \) is true for the detection threshold \( \rho_{\rho_h} \). When the sample size \( N \) is large,
–2\ln \lambda(\Delta \phi) approximately obeys the chi square distribution.

Similarly, the function expressions of detection probability and false alarm probability can be obtained.

4 Simulation analysis
Due to the lack of test sample data, the rationality and feasibility of the test method are analyzed by simulation. Under the hypothesis of \( H_0 \) and \( H_1 \), the statistical information of carrier phase double difference measurement can be obtained directly from the measurement of two receiving antennas, and can also be calculated by measuring the azimuth angle and elevation angle with angle data. Using GPS L1C/A code as the real signal, the length of baseline vector of two receiving antennas is 0.5, the mean value of carrier phase double difference measurement is 0.5, and the measurement accuracy is 0.01 cycle that is \( \sigma^2 = 0.01 \).

Figure 2 and Figure 4 show the density functions of \( \Delta \phi \) in the case of same direction spoofing interference and different direction spoofing interference respectively. It can be found that \( \Delta \phi \) has different density functions under the hypothesis of \( H_0 \) and \( H_1 \) in Figure 2, which is easy to distinguish. In Figure 4, the \( \Delta \phi \) has great fluctuation under \( H_1 \) assumption. The essence of the GLR test is to compare the probability of the test samples occurrence under the hypothesis of \( H_0 \) and \( H_1 \). Therefore, the detection method using likelihood ratio test statistics is feasible. Figure 3 and Figure 5 show the change curves of detection probability and false alarm probability under two scenarios of same direction spoofing interference and different direction spoofing interference. It can be found that the detection probability and false alarm probability increase correspondingly with the increase of threshold. In practical application, the threshold range can be set on the receiving equipment according to the actual situation.

![Figure 2. Density function of \( \Delta \phi \).](image1)

![Figure 3. Detection probability and false alarm probability.](image2)
5 Conclusion

In this paper, a new detection method of GNSS spoofing interference using two receiving antennas is proposed, based on the idea of statistical hypothesis test. This method collects the data samples of carrier phase double difference measurements of two receiving antennas, establishes the hypothesis test model of spoofing interference, and constructs the test statistics through the GLR, and gives the test methods under two spoofing scenarios: spoofing interference from the same direction and spoofing interference from different directions. Finally, the feasibility of this method is verified by simulation. At the same time, this method has a certain reference value for the protection of GNSS information security.

Reference

[1] Junzhi L, Wanqing L, Qixiang F, et al 2019 Research Progress of GNSS Spoofing and Spoofing Detection Technology (2019 IEEE 19th International Conference on Communication Technology, Xi’an, China, IEEE) PP 1360-1369
[2] Borio D, Gioia C 2015 A Dual-antenna Spoofing Detection System Using GNSS Commercial Receivers (ION GNSS 28th Int.Tech.Meeting Satellite Division, Tampa, FL,USA) PP 325-330
[3] Jahromi A J, BROUMANDAN A, GÉRARD LACHAPELLE 2016 GNSS Signal Authenticity Verification Using Carrier Phase Measurements with Multiple Receivers(NAVITEC 2016,IEEE) PP 1-11
[4] Swaszek P F, Pratz S A, Arocho B N, et al 2014 GNSS Spoof Detection Using Shipboard IMU Measurements Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation.2014 745-758
[5] Konovaltsev A, Cuntz M, Christian Hättich, et al 2013 Performance Analysis of Joint Multi-Antenna Spoofing Detection and Attitude Estimation (2013 Ion Int. Technical Meeting) PP 864-872
[6] Hu Y,Bian S, Ji B, et al 2018 GNSS Spoofing Detection Technique Using Fraction Parts of Double-difference Carrier Phases J.of Navigation.71 1111-1129
[7] Xiao L, Li X, Wang G 2019 GNSS Spoofing Detection Using Pseudo-range Double Differences between Two Receivers (2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China) PP 498-502
[8] Jeong S 2020 GNSS spoofing detection using a maximum likelihood-based sliding window method PLoS ONE.15 e0237164
[9] Chen J,Xu Y,Yuan H,et al 2020 A new GNSS spoofing detection method using two antenna IEEE Access.2020 1-10
[10] Kalantari A,Larsson E G 2020 Statistical test for GNSS spoofing attack detection by using...
multiple receivers on a rigid body. *J. on Advances in Signal Processing* **2020** 1-16

[11] Zhenglin G, Junwei N, Baiyu L, et al. 2016 Carrier phase double difference GNSS spoofing detection technique based on multi-direction measurements. *J. of national university of defense Technol.* **38** 32-38 (in china)

[12] Xin Z, Jing P, Yingxue S, et al. 2014 Spoofing detection technique on antenna array carrier phase double difference. *J. of national university of defense Technol.* **36** 55-60 (in china)