electronics

MDPI

Article

A Real-Time Spoofing Detection Method Using Three Low-Cost Antennas in Satellite Navigation

Jiajia Chen [1,2], Xueying Wang [1], Zhibo Fang [2,3], Cheng Jiang [4], Ming Gao [2,3] and Ying Xu [2,3,*]

[1] School of Information Engineering, Suqian University, Suqian 223800, China; chenjiajia19@mails.ucas.ac.cn (J.C.); wangxueying@squ.edu.cn (X.W.)
[2] Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China; fangzb@aircas.ac.cn (Z.F.); gaoming@aircas.ac.cn (M.G.)
[3] School of Navigation and Internet of Things, Aerospace Information Technology University, Jinan 250200, China
[4] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100094, China; jiangcheng@bupt.edu.cn
* Correspondence: nadinexy@aoe.ac.cn; Tel.: +86-13691383176

Abstract: The vulnerability of civil receivers of the Global Satellite Navigation System (GNSS) to spoofing jamming has raised significant concerns in recent times. Traditional multi-antenna spoofing detection methods are limited in application scenarios and come with high hardware costs. To address this issue, this paper proposes a novel GNSS spoofing detection method utilizing three low-cost collinear antennas. By leveraging the collinearity information of the antennas, this method effectively constrains the observation equation, leading to improved estimation accuracy of the pointing vector. Furthermore, by employing a binary statistical detection model based on the sum of squares (*SSE*) between the observed value and the estimated value of the pointing vector, real-time spoofing signal detection is enabled. Simulation results confirm the efficacy of the proposed statistical model, with the error of the skewness coefficient not exceeding 0.026. Experimental results further demonstrate that the collinear antenna-based method reduces the standard deviation of the angle deviation of the pointing vector by over 55.62% in the presence of spoofing signals. Moreover, the experiments indicate that with a 1 m baseline, this method achieves 100% spoofing detection.

Keywords: collinearity; Global Navigation Satellite System (GNSS); low cost; multi-antenna; spoofing detection

Citation: Chen, J.; Wang, X.; Fang, Z.; Jiang, C.; Gao, M.; Xu, Y. A Real-Time Spoofing Detection Method Using Three Low-Cost Antennas in Satellite Navigation. *Electronics* **2024**, *13*, 1134. https://doi.org/10.3390/electronics13061134

Academic Editor: Massimiliano Pieraccini

Received: 25 February 2024
Revised: 13 March 2024
Accepted: 14 March 2024
Published: 20 March 2024

1. Introduction

GNSS is widely recognized as an accurate and effective means for users to obtain spatiotemporal reference information [1]. However, it is susceptible to various vulnerabilities, such as intentional or unintentional spoofing signals in the environment, which can lead to a decrease in positioning accuracy or even provide false Positioning, Navigation, and Timing (PNT) information. These issues can result in serious security threats in applications like unmanned aerial vehicles and autopilot systems [2,3]. One of the current hotspots in the field of GNSS anti-spoofing is the multi-antenna GNSS spoofing detection method, which utilizes the geometric differences between spoofing signals and real signals to detect spoofing attempts [4–6]. Since it is nearly impossible to replicate the geometric space information of GNSS satellites, the multi-antenna spoofing detection method has become one of the most effective spoofing detection techniques [7,8].

The simplest form of the multi-antenna technique is the two-antennas spoofing detection method. These methods are typically predicated on the notion that multiple spoofing signals emanate from a single direction (e.g., a GNSS signal repeater broadcasting all received GNSS signals). In this scenario, the double difference between the code pseudorange and carrier phase observations received by the two antennas serves as the deciding

factor for spoofing detection [9]. Assuming that two or more spoofing signals are coming from the same direction, the single difference of pseudo-range or carrier phase for distinct antennas is nearly identical, and the double difference of pseudo-range or carrier phase between two or more spoofing signals will approach zero. In contrast, the difference for real signals varies significantly, as the directions of different satellites differ greatly at any given time, resulting in a relatively large double difference observation value. Generally speaking, the observation value of pseudo-range does not suffer from any ambiguity resolution issues, making it easier to implement. However, the observation error of pseudo-range is relatively significant and may significantly impact the algorithm's spoofing performance [10,11]. The carrier phase's precision is two orders of magnitude greater than the code pseudo-range, so the carrier phase is the preferred choice for constructing the detection statistical model in the two-antennas spoofing detection method [12,13]. Nonetheless, this approach is contingent on the assumption that the spoofing signal originates from the same direction. If the spoofing source emitted only one spoofing signal, this technique might fail [14,15].

The utilization of multiple antennas through the array anti-spoofing method has been proposed as a more advanced approach [16–18]. This technique samples the GNSS signal in the space domain through the array antenna and detects the spoofing signal based on the direction of the incident signal. A null is formed in the antenna pattern employing adaptive filtering, which leads to the complete suppression of the spoofing signal towards the direction of the interference source [19]. However, this method can only detect a limited number of spoofing signals. When there are multiple spoofing signals, this method may also fail, and forming a null for the spoofing signal will also cause a certain degree of attenuation of the real signal power [20,21]. Additionally, the cost of large-scale dedicated antenna arrays is high, limiting its practical applications [22–24].

There exists a comparatively intricate multi-antenna spoofing detection technique that can identify a single spoofing signal and spoofing signals from varying directions [25]. When the attitude information of several antennas is obtainable, the real signal's incident direction can be deduced from the satellite's broadcast ephemeris information, in conjunction with the antenna's crude position. The method deems that there is spoofing signal jamming when the difference between the estimated signal incident direction and the actual incident direction of the multi-antenna is greater than a stipulated threshold [26]. In principle, this method can identify the presence of spoofing signals as long as the incident direction of the actual and spoofing signals are inconsistent. Due to the absence of additional assumptions, this method has a vast range of practical applications. Since ephemeris information is challenging to forge, this approach has a strong likelihood of detecting spoofing in a variety of circumstances. Nevertheless, using this method typically necessitates more intricate multi-antenna calibration technology to ensure the accuracy of estimation of the signal direction [27]. Furthermore, obtaining accurate carrier attitude information requires auxiliary equipment such as an inertial navigation system (INS) or inertial measurement unit (IMU) [28–30]. Therefore, the entire equipment incurs relatively high hardware and system complexity costs, making it challenging to implement [31].

This paper proposes a method to detect spoofing using three low-cost antennas, addressing the current issues with multi-antenna spoofing detection methods. The proposed method leverages the collinear arrangement of the antennas to effectively constrain the observation equation, aiding in the accurate estimation of the pointing vector. Statistical models are constructed for both real and spoofing signals, measuring the *SSE* statistics between the observed values and the estimated values of the pointing vector and employing a reasonable threshold value to enable effective spoofing detection. This method does not require the use of additional hardware equipment, resulting in a reduction in hardware costs while achieving real-time detection of spoofing signals. To further detail the proposed method, Section 2 outlines the statistical model of spoofing signals and the principle of spoofing detection. The spoofing signal model is then verified by Monte Carlo simulation in Section 3. Experimental verification scenarios are created in Section 4, with one scenario containing spoofing signals and another without. Finally, Section 5 summarizes the paper.

2. Principle of Spoofing Detection Method Using Three Collinear Antennas

The paper proposes a spoofing detection method that utilizes three collinear antennas, as illustrated in Figure 1. The antennas are aligned in a linear formation and labeled as Antenna 1, Antenna 2, and Antenna 3. The direction of the vector is represented by the pointing vector, which is the unit direction vector between any two points in space. As the three antennas are in the same line, the pointing vector calculated from any of the baselines is entirely consistent. To avoid potential clock errors, the three antennas are operated by a common oscillator, and their placement on the carrier is fixed, allowing for accurate measurement of the baseline length between them. In this paper, the baseline length between antennas is labeled as d_{12}, d_{23}, and d_{13}, where $d_{23} = d_{13} - d_{12}$. To maintain consistency in the integer ambiguity of the carrier phase, the length difference between antennas is set to be less than half a wavelength, expressed as $d_{23} - d_{12} < 0.5\lambda$, where λ refers to the wavelength of the received signal [32–34]. Assuming m is the number of satellites, the carrier phase single difference observation equation between Antenna 1 and Antenna 2 can be formulated as follows:

$$\breve{\boldsymbol{\Phi}}_{12} = \boldsymbol{\Phi}_{12} + \boldsymbol{e} = d_{12}\boldsymbol{H}\boldsymbol{a} + \boldsymbol{e} \tag{1}$$

where $\boldsymbol{\Phi}_{12}$ is the carrier phase single-difference true matrix between Antenna 1 and Antenna 2. The observation noise, denoted by $\boldsymbol{e}$, is Gaussian white noise with zero mean value and a standard deviation of σ and satisfies $\boldsymbol{e} \sim \boldsymbol{N}(0, \sigma^2 \boldsymbol{I}_{\mathrm{m}})$, where $\boldsymbol{I}_{\mathrm{m}}$ is the m-order identity matrix. The $m \times 3$ satellite line-of-sight vector matrix, represented by $\boldsymbol{H}$, can be obtained from the ephemeris information. The pointing vector between antennas is denoted by $\boldsymbol{a}$. Additionally, based on the geometric relationship depicted in Figure 1, the true value of the carrier phase single difference may also be expressed as follows:

$$\boldsymbol{\Phi}_{12} = d_{12}\boldsymbol{H}\boldsymbol{a} = d_{12}\cos\boldsymbol{\theta} \tag{2}$$

where $\boldsymbol{\theta}$ is direction of arrival (DOA) of the satellite signals. According to Equation (2), we can get the following:

$$\boldsymbol{a} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{\Phi}_{12}/d_{12} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\cos\boldsymbol{\theta} \tag{3}$$

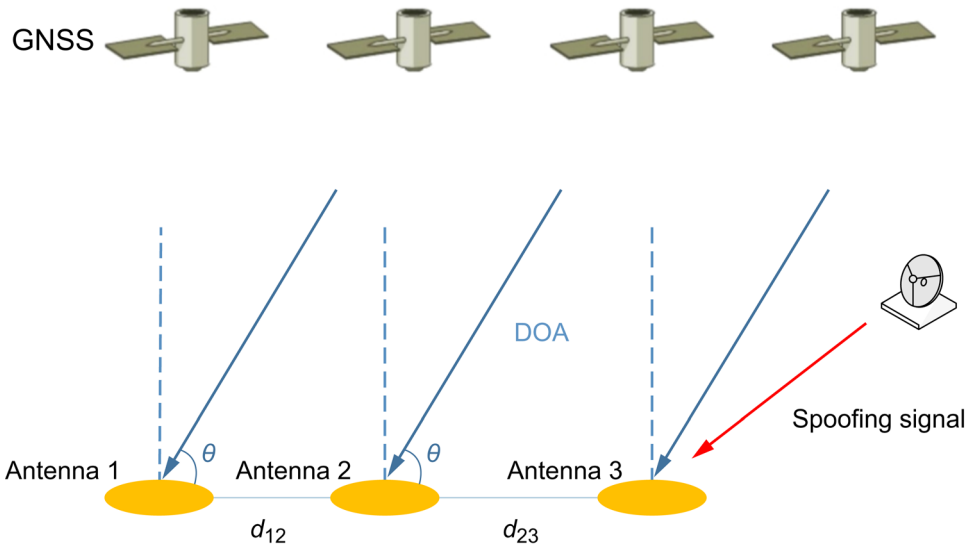


Figure 1. Configuration diagram of three collinear antennas.

From Equation (3), it is evident that the pointing vector $\boldsymbol{a}$ exhibits a positive correlation with the cosine matrix of the signals' DOA. The pointing vector represents the signals' geometry matrix, projected onto the navigation coordinate system, and it reflects the spatial distribution of the GNSS signals. Should a spoofing signal be present, a substantial

deviation will arise between the DOA of the spoofing signal and that of the real signal, thereby causing the pointing vector to change. Consequently, detecting the spoofing signal can be achieved by computing the observation error of the pointing vector.

We can obtain the observed value $\breve{\boldsymbol{a}}$ of the pointing vector by solving the least squares of Equation (1):

$$\breve{\boldsymbol{a}} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\breve{\boldsymbol{\Phi}}_{12}/d_{12} \tag{4}$$

As evidenced by Equation (4), the accuracy of $\breve{\boldsymbol{a}}$ is typically compromised by the prevailing observation noise, leading to a non-negligible deviation from optimal performance. In tandem with this, $\breve{\boldsymbol{a}}$ conforms to the Gaussian distribution. Furthermore, the variance-covariance matrix of $\breve{\boldsymbol{a}}$ can be delineated as follows:

$$\boldsymbol{\Sigma} = \sigma^2(\boldsymbol{H}^T\boldsymbol{H})^{-1}/d_{12}^2 \tag{5}$$

It is established that $\breve{\boldsymbol{a}}$ can be represented as $\breve{\boldsymbol{a}} \sim \boldsymbol{N}(\boldsymbol{a}, \boldsymbol{\Sigma})$. The evaluation of the pointing vector's observation error requires an estimation of its true value $\boldsymbol{a}$. It can be inferred from Equation (5) that $\boldsymbol{\Sigma}$ is inversely proportional to the square of d_{12}, which implies that the accuracy of $\breve{\boldsymbol{a}}$ is positively correlated with the baseline length of Antenna 1 and Antenna 2. To enhance the precision of the pointing vector, additional restrictions can be placed on it by leveraging the unit characteristics and Antenna 3′s information.

The more accurate pointing vector $\breve{\boldsymbol{a}}'$ can be calculated according to the following formula:

$$\breve{\boldsymbol{a}}' = argmin_{\|\boldsymbol{a}\|_2^2=1}\|\breve{\boldsymbol{a}} - \boldsymbol{a}\|_2^2 \tag{6}$$

where $\|\cdot\|_2^2$ represents the two-norm of the vector. Given that the three antennas are aligned in a collinear fashion, the pointing vector for Antenna 1 and Antenna 2 is the same as that for Antenna 1 and Antenna 3. Consequently, the measured carrier phase difference between Antenna 1 and Antenna 3 can be mathematically expressed as:

$$\breve{\boldsymbol{\Phi}}_{13} = d_{13}\boldsymbol{H}\breve{\boldsymbol{a}}' + \boldsymbol{e} \tag{7}$$

In order to re-estimate the pointing vector, the following minimization formula using $\breve{\boldsymbol{\Phi}}_{13}$ can be employed:

$$min_{\|\boldsymbol{a}\|_2^2=1}\breve{\boldsymbol{\Phi}}_{13}\left\|\breve{\boldsymbol{\Phi}}_{13} - d_{13}\boldsymbol{H}\boldsymbol{a}\right\|_2^2 \tag{8}$$

Equation (8) pertains to the solution via least squares with quadratic constraints. This solution may be obtained through the use of the Lagrange multiplier method.

$$d_{13}(\boldsymbol{H}^T\boldsymbol{H} + k\boldsymbol{I})\boldsymbol{a} = \boldsymbol{H}^T\breve{\boldsymbol{\Phi}}_{13} \tag{9}$$

The value of k in Equation (9) can be determined iteratively using the Newton method, starting from an initial value of 0 and converging to a stable final value. Subsequently, this value of k can be used in Equation (9) to obtain an estimate of the pointing vector $\hat{\boldsymbol{a}}$.

$$\hat{\boldsymbol{a}} = (\boldsymbol{H}^T\boldsymbol{H} + k\boldsymbol{I})^{-1}\boldsymbol{H}^T\breve{\boldsymbol{\Phi}}_{13}/d_{13} \tag{10}$$

Based on the calculation process of $\hat{\boldsymbol{a}}$, it is evident that the accuracy of the estimated value $\hat{\boldsymbol{a}}$ is notably higher than that of the observed value $\breve{\boldsymbol{a}}$. This is primarily attributable to a sequence of constrained optimization techniques, whereby additional data from Antenna 3 are incorporated. Consequently, $\hat{\boldsymbol{a}}$ is deemed as a reliable estimate of the true value a. To evaluate the error between $\hat{\boldsymbol{a}}$ and $\breve{\boldsymbol{a}}$, we employ the *SSE* statistics, which can be defined as follows:

$$SSE = (\breve{\boldsymbol{a}} - \hat{\boldsymbol{a}})^T\boldsymbol{\Sigma}^{-1}(\breve{\boldsymbol{a}} - \hat{\boldsymbol{a}}) \tag{11}$$

The utilization of the normalization factor $\boldsymbol{\Sigma}^{-1}$ is essential for the normalization of the residual pointing vector. Equation (11) clearly indicates that in the absence of any spoofing

signals, the *SSE* metrics must conform to the chi-square distribution with three degrees of freedom, which is represented as $\chi^2(3)$.

In the case of the spoofing signal, it is assumed that the satellite signal i is in fact being interfered with. In particular, we record the DOA of the true satellite signal as $\boldsymbol{\theta}_i$. We can denote the DOA with the spoofing signal as $\boldsymbol{\theta}_{sp}$ and express the carrier phase difference of baseline 12 accordingly.

$$\breve{\boldsymbol{\Phi}}'_{12} = \breve{\boldsymbol{\Phi}}_{12} + \Delta\boldsymbol{\Phi} = \breve{\boldsymbol{\Phi}}_{12} + d_{12}\left(cos\boldsymbol{\theta}_{sp} - cos\boldsymbol{\theta}\right) \tag{12}$$

At this time, the observed value of the pointing vector can be recorded as $\breve{\boldsymbol{a}}'$:

$$\begin{aligned} \breve{\boldsymbol{a}}' = \; & (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\breve{\boldsymbol{\Phi}}'_{12}/d_{12} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T(\breve{\boldsymbol{\Phi}}_{12} + \Delta\boldsymbol{\Phi})/d_{12} \\ & = \breve{\boldsymbol{\alpha}} + (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\Delta\boldsymbol{\Phi}/d_{12} \end{aligned} \tag{13}$$

We set $\boldsymbol{R} = \left(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\mathrm{T}}$, and then, Equation (13) can be rewritten as:

$$\breve{\boldsymbol{a}}' = \breve{\boldsymbol{a}} + \boldsymbol{R}\left(cos\boldsymbol{\theta}_{sp} - cos\boldsymbol{\theta}\right) \tag{14}$$

In the presence of the spoofing signal, the *SSE* between the observed value $\breve{\boldsymbol{a}}'$ and estimated value $\hat{\boldsymbol{a}}$ of the pointing vector can be mathematically expressed as follows:

$$SSE = (\breve{\boldsymbol{a}}' - \hat{\boldsymbol{a}})^T\boldsymbol{\Sigma}^{-1}(\breve{\boldsymbol{a}}' - \hat{\boldsymbol{a}}) \tag{15}$$

At present, it is expected that the *SSE* should meet a non-central chi-square distribution with 3 degrees of freedom, denoted as $\chi^2(3, \gamma)$. Based on this, the identification of binary hypotheses for both real signals and spoofing signals can be formulated as follows:

$$\begin{aligned} H_0(\text{no spoofing}): SSE \sim \chi^2(3) \\ H_1(\text{spoofing}): SSE \sim \chi^2(3, \gamma) \end{aligned} \tag{16}$$

where the eccentricity γ of chi-square distribution can be expressed as follows:

$$\begin{aligned} \gamma = \Delta\boldsymbol{\Phi}^T\boldsymbol{R}^T\boldsymbol{\Sigma}^{-1}\boldsymbol{R}\Delta\boldsymbol{\Phi}/d_{12}^2 \\ = (cos\boldsymbol{\theta}_{sp} - cos\boldsymbol{\theta})^T\boldsymbol{R}^T\boldsymbol{\Sigma}^{-1}\boldsymbol{R}(cos\boldsymbol{\theta}_{sp} - cos\boldsymbol{\theta}) \end{aligned} \tag{17}$$

The findings of this research demonstrate that the value of γ is positively related to the cosine difference of the DOA between the real and spoofing signals, as depicted in Equation (17). Conversely, the correlation is negative with the covariance matrix $\boldsymbol{\Sigma}$ of the pointing vector. As for Equation (5), it shows that the *SSE* statistic is inversely proportional to the square of d_{12}. Therefore, γ should be proportional to the square of d_{12}. In simpler terms, increasing the baseline can result in larger *SSE* statistics for the same spoofing scenario.

According to the Neyman–Pearson criterion, an appropriate threshold value SSE_{th} can be determined. The null hypothesis H_0 is rejected when *SSE* exceeds SSE_{th}, and it is not rejected when *SSE* is less than or equal to SSE_{th}. The detection probability P_D and the false alarm rate P_{fa} can be calculated using the following equations:

$$\begin{cases} P_{fa} = P\{SSE > SSE_{\text{th}}|H_0\} = 1 - \int_0^{SSE\text{th}} p_{\chi^2(3)}(x)dx \\ P_D = P\{SSE > SSE_{\text{th}}|H_1\} = \int_{SSE\text{th}}^{\infty} p_{\chi^2(3,\gamma)}(x)dx \end{cases} \tag{18}$$

where and are probability density functions (PDF) of $\chi^2(3)$ and $\chi^2(3, \gamma)$, respectively.

According to Equation (18), it can be observed that the false alarm rate P_{fa} is directly related to the threshold value SSE_{th}. In practical applications, the threshold value SSE_{th} is typically determined based on a predetermined false alarm rate P_{fa} (e.g., $P_{fa} = 10^{-4}$). The relationship between the threshold value and the false alarm rate is illustrated in Figure 2.

The appropriate threshold value can be selected based on the performance requirements of the specific application scenario.

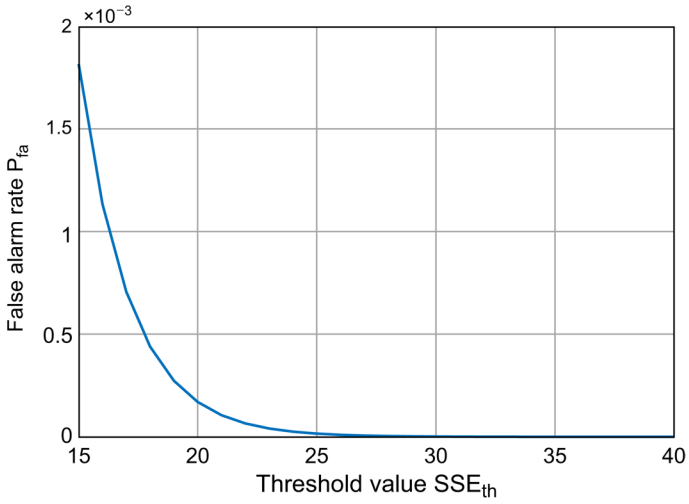


Figure 2. Distribution graph of false alarm rate P_{fa}.

Under current technical conditions, achieving accurate phase synchronization in real time between the spoofing signal and the real signal is not possible. Typically, there is a considerable angle deviation between the two signals, leading to the identification of the presence of the spoofing signal through changes in the *SSE* statistics.

3. Simulation Verification Results

This section presents the simulation-based verification of the proposed method. Specifically, we created two sets of antenna configurations, each with three antennas arranged in a straight line but with differing baseline lengths. The first set had baseline lengths of d_{12} = 0.20 m, d_{13} = 0.48 m, while the second set had a baseline length of d_{12} = 0.30 m, d_{13} = 0.68 m. The simulated scene included seven stationary GPS satellites and utilized L1 frequency signals with a wavelength of approximately 19 cm. The observed noise standard deviation σ of carrier phase was set to 2 mm. The simulation was conducted under two conditions: the H_0 hypothesis without the spoofing signal and the H_1 hypothesis with the spoofing signal. Each case underwent 10,000 simulations.

The H_0 hypothesis posits that the antennas are capable of receiving all real signals, while the H_1 hypothesis suggests that the spoofing signals with higher power can capture the receiver's tracking loop, leading to deviations in the carrier phase [35]. To model the occurrence of two spoofing signals, we artificially introduced errors for the carrier phase of the SV13 and SV21 satellites. Specifically, the elevation and azimuth deviations for both the real and spoofing signals were -10° in the body frame coordinate system. However, all other parameters remained consistent with the scenario of the absent spoofing signal. Figure 3 presents the constellation distribution of both the real and spoofing signals in the body frame coordinate system, with blue and yellow dots representing each signal, respectively.

The *SSE* statistics for the H_0 and H_1 hypotheses, as well as the theoretical eccentricity γ of the H_1 hypothesis, can be calculated using Equations (11), (15) and (17). The PDFs and corresponding theoretical distributions of two sets are shown in Figure 4a,b, respectively. The green and gray histograms represent the *SSE* statistics of H_0 and H_1 hypotheses, respectively, and the red and black curves represent the theoretical distribution of H_0 and H_1 hypotheses, respectively.

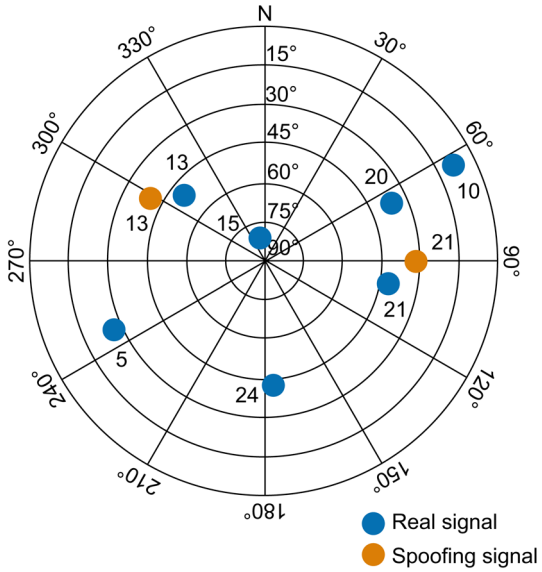
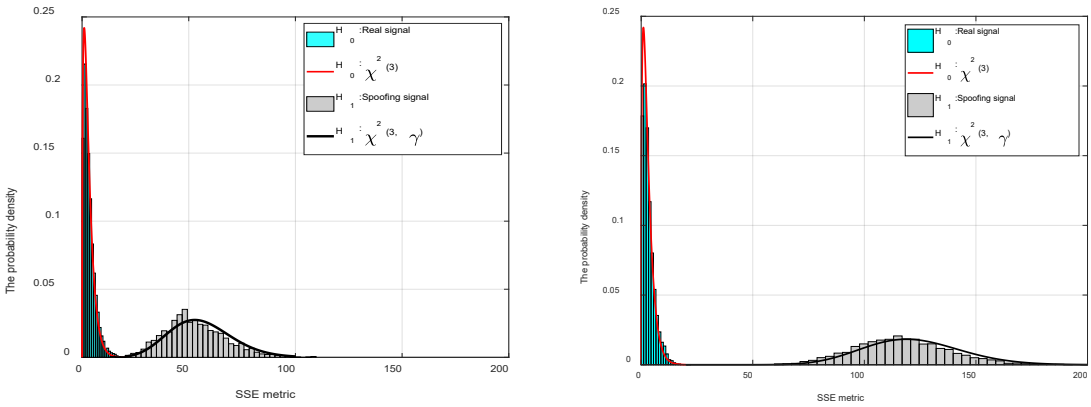


Figure 3. Satellite distribution sky map under the body frame coordinate system.



(**a**) (**b**)

Figure 4. Probability density distribution of *SSE* statistics of simulated data: (**a**) Set1: d_{12} = 0.20 m; (**b**) Set2: d_{12} = 0.30 m.

Upon comparison of Figure 4a,b, a significant disparity in the *SSE* statistics becomes evident between the H_0 and H_1 hypotheses. Consequently, it is feasible to ascertain the presence of the spoofing signal by determining an appropriate threshold. Furthermore, the maximum and mean values of *SSE* for H_1 in Figure 4b are significantly greater than the data in Figure 4a, indicating a correlation between the *SSE* statistics of the spoofing scenario and the length of the baseline, which aligns with Equation (17). As a result, enhancing the detection probability of this technique is theoretically possible by using a longer baseline.

The results indicate that the *SSE* statistics of the H_0 hypothesis are generally in alignment with the $\chi^2(3)$ theoretical distribution. However, a slight divergence is observed between the *SSE* statistics of the H_1 hypothesis and the $\chi^2(3, \gamma)$ theoretical distribution, which can be attributed to errors between the estimated and true values of the pointing vector that arise due to spoofing signals. The χ^2 distribution is inherently a skewed normal distribution, and therefore, the degree of variation between the simulated and theoretical distributions can be evaluated using the skewness coefficient.

The skewness coefficient serves as a crucial statistical metric delineating the asymmetry level of a probability density function concerning the standard normal distribution. Data symmetry is characterized by a skewness coefficient of 0, where a positive coefficient signifies right skewness or positive skew, and a negative coefficient indicates left skewness

or negative skew [36,37]. The magnitude of the skewness coefficient exhibits an inverse relationship with the data bias intensity, with decreased values indicating data proximity to a normal distribution. If the skewness coefficient of simulated data matches the theoretical distribution, it is considered that the constructed model possesses higher usability; otherwise, it is regarded that the model has significant errors.

The skewness coefficient h is calculated by the following formula:

$$h = \frac{K_3}{K_2\sqrt{K_2}} \tag{19}$$

where $K_3 = m\sum\left(SSE - \overline{SSE}\right)^3/(p-1)/(p-2)$, $K_2 = \sum\left(SSE - \overline{SSE}\right)^2/(p-1)$, p is the number of simulation data, and $\overline{SSE}$ is the mean of SSE statistics.

Table 1 presents the skewness coefficient h of both the SSE statistics and theoretical distribution. The skewness coefficients of SSE statistics for H_0 hypothesis are 1.678 and 1.681, respectively, with errors of 0.004 and 0.002 from the theoretical values. For the H_1 hypothesis, the skewness coefficients are 0.420 and 0.288, respectively, with an error of 0.037 and 0.026, respectively. Although the error between the H_1 hypothesis and the theoretical distribution has slightly increased in comparison to the H_0 hypothesis, it remains consistent. Therefore, we can utilize $\chi^2(3, \gamma)$ for the approximation of the H_1 hypothesis distribution fitting. Moreover, it is evident that the skewness coefficient of the second set draws closer to the theoretical value as the baseline length increases. Simultaneously, the skewness coefficient for the H_1 hypothesis gradually decreases as the baseline length increases, approaching normal distribution. Significantly, this outcome aligns entirely with theoretical analysis.

Table 1. Simulated skewness coefficient and kurtosis of the SSE statistics and theoretical distribution.

Scheme	Set	$\chi^2(3)$	H_0 Hypothesis	$\chi^2(3,\gamma)$	H_1 Hypothesis
Skewness	Set 1	1.674	1.678	0.383	0.420
	Set 2	1.679	1.681	0.262	0.288
Kurtosis	Set 1	6.002	6.016	3.506	3.533
	Set 2	6.011	6.012	3.124	3.140

Table 1 also presents the kurtosis of the SSE statistics and the theoretical distribution. It can be observed from the table that the kurtosis under the H_0 hypothesis is very close to that of the theoretical distribution. The kurtosis under the H_1 hypothesis is related to the length of the baseline. The kurtosis of the Set 2, which utilizes a longer baseline, is closer to the kurtosis of the normal distribution (theoretical value of 3). This conclusion is entirely consistent with the preceding discussion.

To further assess the effectiveness of the proposed method, a threshold value of $SSE_{\text{th}} = 20$ was set, and the corresponding detection probability P_{D} was plotted for various DOA of spoofing signals, as depicted in Figure 5. It is evident from Figure 5 that a pronounced drop in detection probability was observed when the DOA of the spoofing signal closely aligns with the true signal, indicating a potential method failure. Nevertheless, it can be observed that when the angular deviation between the spoofing signal and the true signal exceeds 10°, the detection probability of the method can reach nearly 100%. Given the current technological capabilities, achieving real-time phase synchronization between the spoofing and true signals is challenging, resulting in a significant angular deviation. Hence, in the majority of cases, this method exhibits robust detection performance.

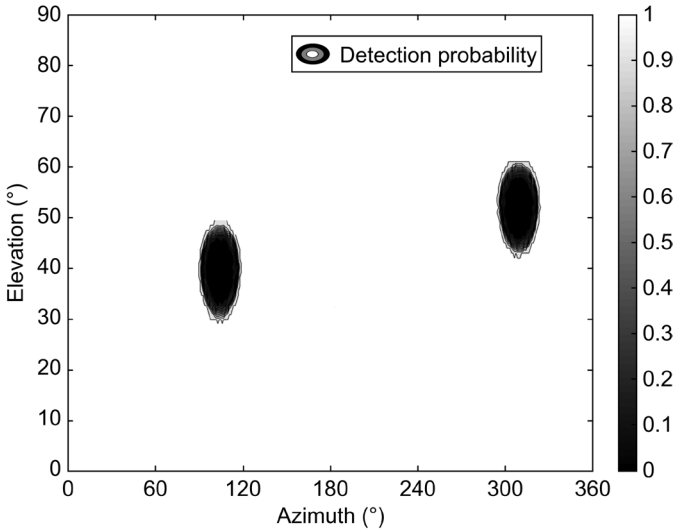
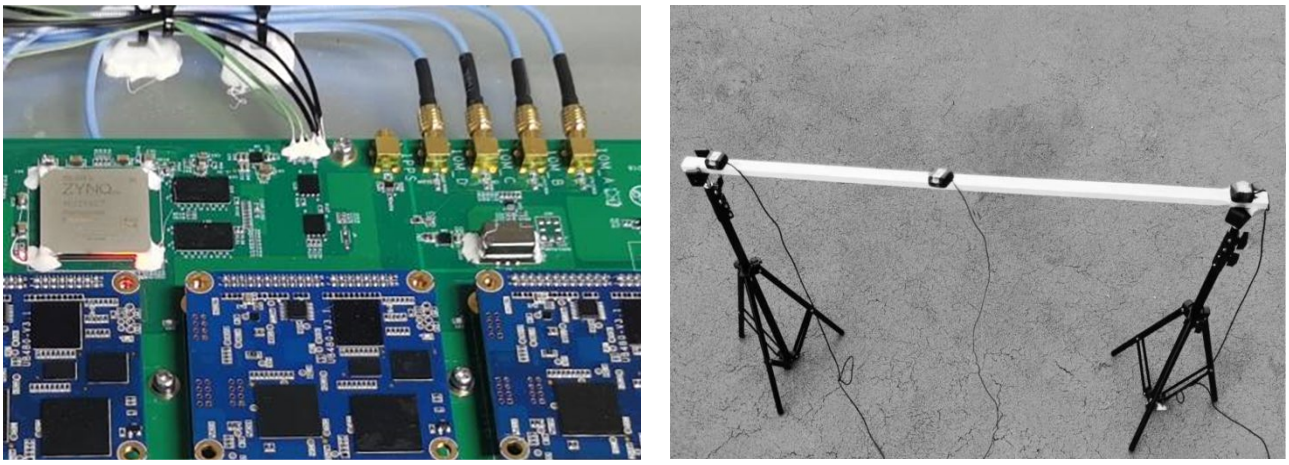


Figure 5. Detection probability corresponding to different spoofing signal directions.

4. Experimental Performance Verification

4.1. Performance Verification of Scenarios without Spoofing Signal

To validate the accuracy of the pointing vector estimation and false alarm rate of the spoofing detection method proposed in this paper, experimental testing was conducted at the Aerospace Information Research Institute, Chinese Academy of Sciences. The chosen experimental site was an open outdoor area with no potential electromagnetic interference. Using the UNICORECO UB480 receiver board and three cost-effective GNSS antennas, we constructed a spoofing detection system. These antennas were powered by a shared resonant oscillator, and their clocks were synchronized to eliminate any potential clock differences. Additionally, we performed ample calibration to eliminate any initial errors that may have arisen from the receiver. We fixed the three antennas onto a strip of wood to ensure they were aligned in a straight line and then used tripods as carriers. Physical representations of the receiver board and collinear antennas are displayed in Figure 6a,b, respectively.



(**a**) (**b**)

Figure 6. Physical image of experimental equipment: (**a**) Physical diagram of the receiver hardware; (**b**) Physical picture of three collinear antennas.

In this experimental setup, the antennas received direct real signals. Both the tripod and wooden structure remained stationary throughout the data collection process, while we gathered two data sets by adjusting the antenna positions. Each set was observed for

a duration of 1 h, at an output frequency of 1 Hz. The number of GPS satellites during the observation period ranged from 6 to 8, with an average Position Dilution of Precision (PDOD) of 1.8 to 2.7. The baseline lengths corresponding to the two sets were d_{12} = 0.26 m, d_{13} = 0.60 m and d_{12} = 0.46 m, d_{13} = 1.00 m, respectively. The true value of the pointing vector $\boldsymbol{a}$ = [0.626, 0.425, 0.653]$^{\mathrm{T}}$ was obtained by averaging the observation values over an extended period in advance. Using Equation (4), we can estimate the observed values $\breve{\boldsymbol{a}}$ of the pointing vector for each epoch, and using Equation (10), we can calculate the estimated values $\hat{\boldsymbol{a}}$ of the pointing vector. Figure 7 shows the box diagrams containing the distribution of observed values $\breve{\boldsymbol{a}}$ and estimated values $\hat{\boldsymbol{a}}$ of the two data sets.

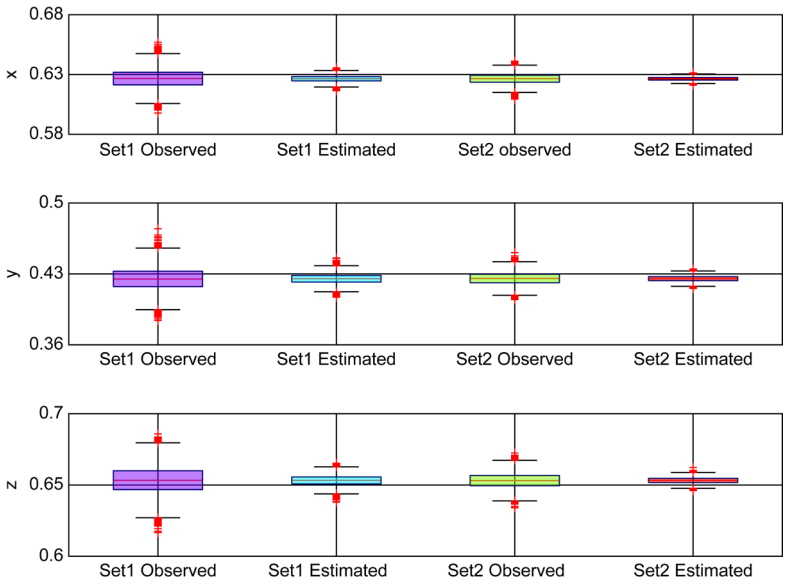


Figure 7. Box diagram of observed and estimated values of pointing vector without spoofing signal.

Figure 7 demonstrates that, without the presence of spoofing signal jamming, the observed values generally conform to a normal distribution. The upper and lower quartiles display a symmetrical distribution. The median of the estimated value in the figure is closer to the true value in comparison to the observed value, with the distribution of the estimated values being more concentrated. The maximum and minimum estimated values are significantly less than the observed values, with fewer observed outliers. These findings effectively establish that the accuracy of pointing vector estimation subsequent to collinearity constraint imposition is greater than the observed values. Furthermore, the second set's use of a longer baseline length produced more accurate values as compared to the first set. This outcome corroborates the outcomes discussed in Section 2.

As the pointing vector is a unit vector, the precision of the observed values $\breve{\boldsymbol{a}}$ and estimated values $\hat{\boldsymbol{a}}$ can be assessed using the subsequent formula:

$$\begin{aligned} \Delta \mathrm{g} &= arccos(\breve{\boldsymbol{a}}^{\mathrm{T}} \cdot \boldsymbol{a} / |\breve{\boldsymbol{a}}|) \\ \Delta \mathrm{g}' &= arccos(\hat{\boldsymbol{a}}^{\mathrm{T}} \cdot \boldsymbol{a} / |\hat{\boldsymbol{a}}|) \end{aligned} \tag{20}$$

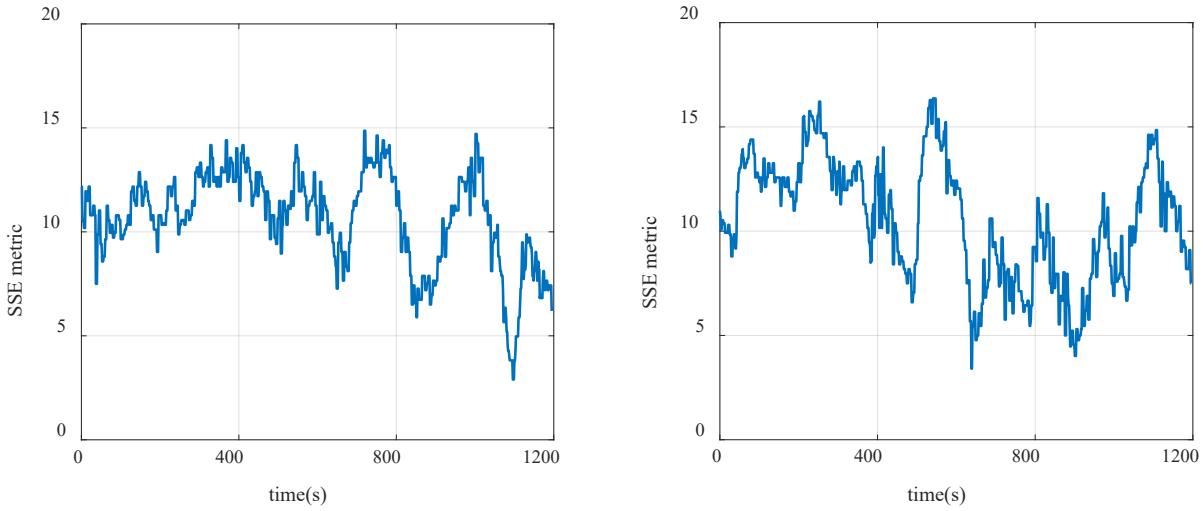
where $|.|$ is the modular operation. The variables Δg and Δg$'$, measured in degrees ($^\circ$) represent the discrepancies between the observed value $\breve{\boldsymbol{a}}$, estimated value $\hat{\boldsymbol{a}}$, and the true value $\boldsymbol{a}$. To analyze these discrepancies, we determined the maximum, minimum, mean, and standard deviation of both Δg and Δg$'$. The results of our statistical analysis are presented in Table 2.

Table 2. Statistics of Δg and $\Delta g'$ in different scenarios.

Scenario	Set	Scheme	Mean (°)	Std (°)
H_0	Set1	Δg $\Delta g'$	0.5923 0.2576 (57%)	5.0593 3.7250 (26%)
	Set2	Δg $\Delta g'$	0.3268 0.1484 (55%)	3.8727 1.5452 (60%)
H_1	Set1	Δg_s $\Delta g_s'$	1.1628 0.4717 (59%)	7.4731 4.6178 (38%)
	Set2	Δg_s $\Delta g_s'$	0.5165 0.2292 (56%)	4.2869 2.1197 (51%)

From the statistical values presented in Table 2, it is evident that the parameter $\Delta g'$ is significantly reduced when compared to Δg. The mean of $\Delta g'$ is less than 1°, which is indicative of the effectiveness of the estimated value in approximating the true value a. The mean of $\Delta g'$ in the two sets exhibits a 60% and 55% reduction in comparison to that of Δg, while the standard deviation shows a 57% and 55% reduction, thus highlighting the greater accuracy of the estimated value compared to the observed value. The utilization of a longer baseline is attributed to the smaller statistical values in Set2 when compared to Set1, a finding that is consistent with the simulation results.

The *SSE* statistics for each set are depicted in Figure 8. It is noteworthy that the received signals are real signals, and as a result, no substantial discrepancy can be observed in the *SSE* statistics distribution between the two sets. By applying the $\chi^2(3)$ theoretical distribution of H_0, an appropriate threshold (such as $SSE_{th} = 20$) can be established. Given that the *SSE* statistics for both sets are smaller than the set threshold, the false alarm rate is considered to be 0.



(**a**) (**b**)

Figure 8. *SSE* statistics of real signals: (**a**) Set 1; (**b**) Set 2.

4.2. Performance Verification with Spoofing Signal

A spoofing test experiment scene was established near the experimental building of the Chinese Academy of Sciences. The GNSS signal generator NavX®-NCS was utilized to simulate the GPS signal in the scenario. The signal generator is depicted in physical form in Figure 9a, while the transmitting antenna of the spoofing signal, shown in Figure 9b, was employed. The NavX®-NCS signal generator can produce accurately defined analog GNSS signals via the pre-defined ephemeris file. Specifically, the GPS signal of PRN 20 was generated by this generator and broadcasted via the transmitting antenna to carry out

spoofing jamming alongside the real signal. To eliminate the near–far-effect, we endeavored to diminish the amplification gain of the antenna while ensuring that the power of the spoofing signal exceeds slightly that of the real signal.

(**a**) (**b**)

Figure 9. Physical picture of broadcasting equipment: (**a**) NavX®-NCS signal generator; (**b**) Spoofing signal transmitting antenna.

In accordance with the previous section, we employed the same antenna configuration for the sake of comparison. The corresponding baseline lengths for this scenario were $d_{12} = 0.26$ m, $d_{13} = 0.60$ m, as well as $d_{12} = 0.46$ m, $d_{13} = 1.00$ m. The experiment's observation time for this spoofing scenario was 16 min and 40 s, involving 1000 sampling points. Prior to the experiment, we obtained the true value of the antenna pointing vector by averaging an extended observation time in advance, which was recorded as $\boldsymbol{a} = [0.420, 0.723, 0.549]^{\mathrm{T}}$. Throughout the entirety of the sampling period, the number of satellites fluctuated between 8 and 11. To facilitate analysis, we included data only from 8 common satellites during all observation periods. The spoofing signal has significant power and must be present in each observation data for the period.

Figure 10 displays the distribution box diagram of the pointing vector's observed $\check{\boldsymbol{a}}'$ and estimated values $\hat{\boldsymbol{a}}$ in the current scenario. The figure illustrates that the existence of the spoofing signal produces a significant deviation between the two values. Furthermore, both values are no longer unbiased; nevertheless, the error between the estimated value and true value is considerably reduced compared to the observed value. Additionally, the estimated value's distribution is concentrated, and its width is smaller than that of the observed values in both sets.

Figure 10 illustrates the significant improvement in the accuracy of the estimated value of the pointing vector resulting from the incorporation of constraint information from collinear antennas. Furthermore, this approach demonstrates a notable resilience to spoofing and jamming.

Figure 7 illustrates the distribution of estimated and observed values in the absence of the spoofing signal. In the absence of the spoofing signal, both the estimated and observed values serve as unbiased estimates of the true values, albeit with some improved precision. Figure 10 showcases the distribution of estimated and observed values under the presence of a spoofing signal. When the spoofing signal interferes, the observed values no longer provide unbiased estimates of the true values, resulting in significant errors. Nonetheless, the distribution of estimated values closely aligns with the unbiased estimates, thereby enhancing both accuracy and precision. A comparison between Figures 7 and 10 reveals

that the proposed method, through the incorporation of additional constraints, fortifies the model and demonstrates a certain resilience against spoofing interference.

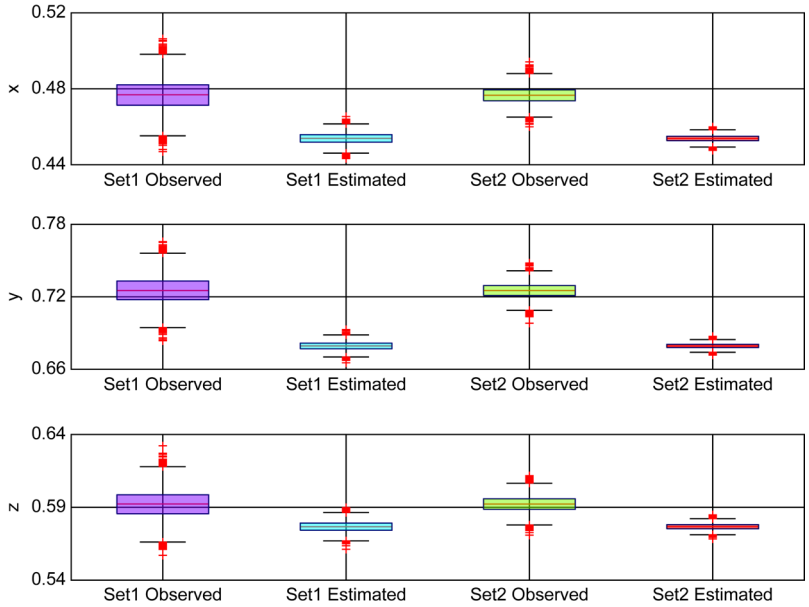


Figure 10. Box diagram of observed and estimated values of pointing vector with spoofing signal.

Utilizing Equation (20), we computed the deviation between the observed value $\breve{\boldsymbol{a}}'$, estimated value $\hat{\boldsymbol{a}}$, and the true value $\boldsymbol{a}$, recorded as Δg_s and $\Delta g_s{}'$, the statistical results of which are also displayed in Table 2. When there were spoofing signals, the statistics of Δg_s in Table 2 exhibited significant differences from that of Δg. Take, for instance, the first set, where the mean of Δg_s increased by 1.66°. This implies that the existence of the spoofing signal has a considerable impact on the observed value of the pointing vector. Furthermore, the statistics of $\Delta g_s{}'$ also increased in comparison with Δg_s. In the first set, the mean increased by 1.11°. However, the error of $\Delta g_s{}'$ was substantially reduced when compared with Δg_s, where the mean and standard deviation of the two sets are reduced by 47%, 59%, and 57%, 56%, respectively. This indicates that the accuracy of the estimated value $\hat{\boldsymbol{a}}$ is still considerably higher than the observed value $\breve{\boldsymbol{a}}'$ when the spoofing signal is present.

Upon examination of Table 2, it is apparent that the standard deviation of the second set is lower than that of the first, regardless of whether it pertains to Δg_s or $\Delta g_s{}'$. This observation suggests that the precision of the pointing vector is positively correlated with the length of the baseline, a result that is in congruence with findings in the absence of spoofing signals.

Equation (15) enables calculation of the *SSE* statistics for both sets, as depicted in Figure 11. Set1 and Set2 correspond to the blue and red curves on the graph, respectively, with the threshold for spoofing detection represented by a dotted line. When compared to Figure 8, Figure 11 reveals the *SSE* statistic to be higher in the presence of spoofing signals. Real-time detection of these signals can therefore be achieved by applying a reasonable *SSE* threshold. Additionally, due to the utilization of a longer baseline, the mean of the *SSE* statistic for Set2 exceeds that of Set1, consistent with Equation (17). It is observed that longer baselines can enhance detection probability, producing detection rates of 99.53% and 100% for Set1 and Set2, respectively. The experimental results underscore the efficacy of longer baselines in increasing detection probabilities.

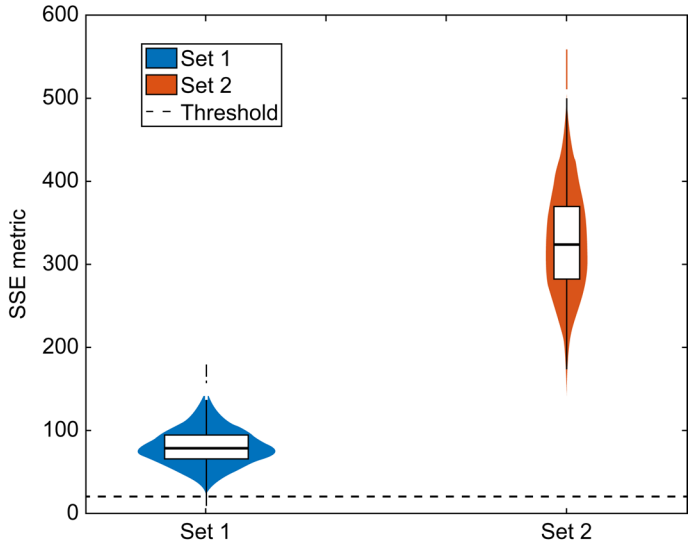


Figure 11. *SSE* statistics with one spoofing signal.

Comparing Figures 8 and 11 shows that when there is no spoofing signal, the *SSE* values remain below the predefined threshold, and the *SSE* values across both data sets are closely aligned. However, in the presence of the spoofing signal, there is a substantial increase in *SSE* values, surpassing the threshold significantly and indicating a positive correlation between *SSE* values and baseline length. Consequently, by monitoring *SSE* value fluctuations, we can effectively detect spoofing signals, with the potential for an increased success rate by utilizing a longer baseline in the methodology.

In order to verify the performance of the method in the presence of multiple spoofing signals, we further used the NavX®-NCS signal generator to generate two spoofing signals and calculated the *SSE* metric for this scenario, as shown in Figure 12. Comparing Figure 12 with Figure 11, it can be observed that due to the presence of multiple spoofing signals, the means of the *SSE* metric in Figure 12 are significantly larger than those in Figure 11, while the detection probability in both cases is 100%. As the number of spoofing signals increases, the detection performance of the method tends to improve.

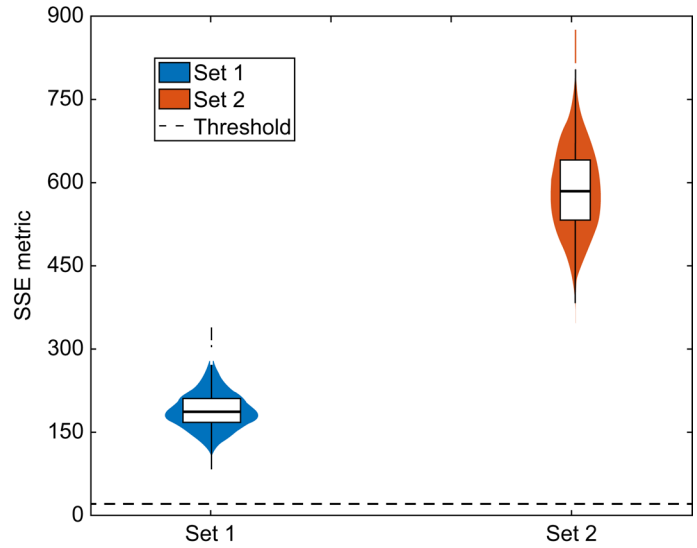


Figure 12. *SSE* statistics with two spoofing signals.

5. Discussion and Conclusions

Spoofing detection based on multi-antenna technology represents a growing field within anti-spoofing research. Traditional methods using multiple antennas face challenges related to limited applicability and high costs. In response to these challenges, our study introduces a real-time spoofing detection approach utilizing three low-cost collinear antennas and establishes a binary hypothesis statistical model for spoofing detection. By exploiting the consistency of the pointing vectors from the three antennas, our method achieves effective spoofing signal detection. Simulation results illustrate a notable enhancement in the accuracy of pointing vector estimation when spoofing signals are absent. Two sets of simulated data show reductions in mean angle deviation of the pointing vector by 59.6% and 54.9%, and decreases in standard deviation by 56.5% and 54.6%, respectively. Additionally, experimental findings reveal that the false alarm rate of our method approaches 0.

In the presence of spoofing signals, the estimation of the pointing vector becomes biased. However, our proposed method effectively enhances the accuracy of pointing vector estimation. Experimentally, we observe reductions of 47.12% and 59.43% in mean angle error and 56.5% and 55.62% in standard deviation of the angle error of the pointing vector. Moreover, our approach demonstrates proficient spoofing signal detection, with detection probability increasing with the baseline length as predicted by our theoretical analysis. Specifically, for a baseline length of 1 m, our method achieves a detection probability of 100%.

Comparing the approach outlined in this study with the four-antenna array spoofing detection method detailed in reference [31], it is evident that both techniques attain close to 100% detection probability in static experimental assessments under spoofing signal conditions. Nonetheless, the receiver employed in reference [31] is a specialized array receiver characterized by substantial hardware dimensions and expenses. In contrast, the three-antenna spoofing detection methodology introduced in this paper can be integrated utilizing readily available low-cost receivers, offering substantial cost-effectiveness and scalability benefits.

Author Contributions: Conceptualization, J.C. and Y.X.; methodology, X.W.; software, Z.F.; validation, C.J. and M.G.; writing—original draft preparation, J.C.; writing—review and editing, Y.X.; supervision, Y.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The State Key Laboratory of Air Traffic Management System and Technology, grant number YJKYYQ20200069 and SKLATM202108; Design and development of a visualized Internet of Things (IoT) intelligent operation and maintenance platform, grant number H2024027; Development of a Quantum Dot-based Light Emitting Device and its Manufacturing Process, grant number H2023294.

Data Availability Statement: Data are contained within the article.

Acknowledgments: We are grateful to the referee for their constructive suggestions to improve the manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Wu, Z.; Zhang, Y.; Yang, Y.; Liang, C.; Liu, R. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access* **2020**, *8*, 165444–165496. [CrossRef]
2. Broumandan, A.; Kennedy, S.; Schleppe, J. Demonstration of a Multi-Layer Spoofing Detection Implemented in a High Precision GNSS Receiver. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020.
3. Kujur, B.; Khanafseh, S.; Pervan, B. Detecting GNSS spoofing of ADS-B equipped aircraft using INS. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020.
4. Chen, J.; Xu, Y.; Yuan, H.; Yuan, Y. A New GNSS Spoofing Detection Method Using Two Antennas. *IEEE Access* **2020**, *8*, 110738–110747. [CrossRef]
5. Xiao, L.; Li, X.; Liao, Z. GNSS Spoofing Detection with Using Linear Array. In Proceedings of the 2020 IEEE 8th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 20–22 November 2020.

6. Chen, J.; Yuan, H.; Xu, Y.; Yu, F. Joint attitude determination and spoofing detection method using three antennas. *J. Beijing Univ. Aeronaut. Astronaut.* **2023**, *49*, 127–136.
7. Chen, J.; Wang, J.; Yuan, H.; Xu, Y.; Chen, X.; Chen, X.; Yang, G. Performance analysis of a GNSS multipath detection and mitigation method with two low-cost antennas in RTK positioning. *IEEE Sens. J.* **2022**, *22*, 4827–4835. [CrossRef]
8. Jahromi, A.J.; Broumandan, A.; Lachapelle, G. GNSS signal authenticity verification using carrier phase measurements with multiple receivers. In Proceedings of the 8th ESA Workshop Satellite Navigation Technologies and European Workshop GNSS Signals Signal Processing (NAVITEC), Noordwijk, The Netherlands, 1–13 December 2016.
9. Falletti, E.; Falco, G.; Nguyen, V.H.; Nicola, M. Performance Analysis of the Dispersion of Double Differences Algorithm to Detect Single-Source GNSS Spoofing. *IEEE Trans. Aerosp. Electron. Syst.* **2021**, *57*, 2674–2688. [CrossRef]
10. Xiao, L.; Li, X.; Wang, G. GNSS Spoofing Detection Using Pseudo-range Double Differences between Two Receivers. In Proceedings of the 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 19–20 October 2019.
11. Enge, P. The Global Positioning System Signals, Measurements, and Performance. *Int. J. Wirel. Inf. Netw.* **1994**, *1*, 83–105. [CrossRef]
12. Hoffmann-Wellenhof, B.; Lichtenegger, H.; Walse, E. *GNSS-Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and More*; Springer: Vienna, Austria; New York, NY, USA, 2008.
13. Closas, P.; Fernandez-Prades, C. A statistical multipath detector for antenna array based GNSS receivers. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 916–929. [CrossRef]
14. Huang, L.; Yong, L.; Xu, B.; Wang, F. Analysis of carry phase difference detection for satellite navigation receivers anti-spoofing. *J. Natl. Univ. Def. Technol.* **2016**, *38*, 103–106.
15. Borio, D.; Gioia, C. A dual-antenna spoofing detection system using GNSS commercial receivers. In Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Tampa, FL, USA, 14–18 September 2015.
16. Xu, H.; Cui, X.; Shen, J.; Lu, M. A two-step beam-forming method based on carrier phases for GNSS adaptive array anti-jamming. In Proceedings of the 2016 International Technical Meeting of the Institute of Navigation, Monterey, CA, USA, 25–28 January 2016.
17. Wang, L.; Wu, R.; Wang, W.; Lu, D.; Jia, Q. Joint GNSS interference mitigation approach for jamming and spoofing based on multi-antenna array. *J. Electron. Inf. Technol.* **2017**, *38*, 2344–2350.
18. Daneshmand, S.; Jafarnia-Jahromi, A.; Broumandan, A.; Lachapelle, G. A GNSS structural interference mitigation technique using antenna array processing. In Proceedings of the IEEE 8th Sensor Array Multichannel Signal Processing Workshop (SAM), A Coruna, Spain, 22–25 June 2014.
19. Ge, D.; Zhou, G.; Xu, D.; Mao, R. GPS receiver anti-deceptive jamming method based on space-time multi-antenna null. *J. Sichuan Ordnance* **2015**, *36*, 41–45.
20. Bao, L.; Wu, R.; Wang, W.; Lu, D. Spoofing mitigation in Global Positioning System based on C/A code self-coherence with array signal processing. *J. Commun. Technol. Electron.* **2017**, *62*, 66–73. [CrossRef]
21. Zhang, J.; Cui, X.; Xu, H.; Zhao, S.; Lu, M. Efficient Signal Separation Method Based on Antenna Arrays for GNSS Meaconing. *Tsinghua Sci. Technol.* **2019**, *24*, 216–225. [CrossRef]
22. Zhang, R.; Qin, H.; Zhou, Z.; Li, B. GNSS Multipath Mitigation Algorithm with Antenna Arrays Based on Matrix Reconstruction. In Proceedings of the IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020.
23. Wang, J.; Xiao, Y.; Li, T.; Chen, C.L.P. Impacts of GPS Spoofing on Path Planning of Unmanned Surface Ships. *Electronics* **2022**, *11*, 801. [CrossRef]
24. Zhu, X.; Lu, Z.; Hua, T.; Yang, F.; Tu, G.; Chen, X. A Novel GPS Meaconing Spoofing Detection Technique Based on Improved Ratio Combined with Carrier-to-Noise Moving Variance. *Electronics* **2022**, *11*, 738. [CrossRef]
25. Xu, G.; Shen, F.; Amin, M.; Wang, C. DOA classification and CCPM-PC based GNSS spoofing detection technique. In Proceedings of the 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 23–26 April 2018.
26. Meue, M.; Konovaltse, A.; Cuntz, M.; Hättich, C. Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM. In Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012.
27. Ceccato, M.; Formaggio, F.; Laurenti, N.; Tomasin, S. Generalized Likelihood Ratio Test for GNSS Spoofing Detection in Devices with IMU. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3496–3509. [CrossRef]
28. Swaszek, P.F.; Pratz, S.A.; Arocho, B.N.; Seals, K.C.; Hartnett, R.J. GNSS spoof detection using shipboard IMU measurements. In Proceedings of the ION GNSS 27th International Technical Meeting Satellite Division, Tampa, FL, USA, 8–12 September 2014.
29. Lemieszewski, Ł.; Radomska-Zalas, A.; Perec, A.; Dobryakova, L.; Ochin, E. The Spoofing Detection of Dynamic Underwater Positioning Systems (DUPS) Based on Vehicles Retrofitted with Acoustic Speakers. *Electronics* **2021**, *10*, 2089. [CrossRef]
30. Lemieszewski, Ł.; Radomska-Zalas, A.; Perec, A.; Dobryakova, L.; Ochin, E. GNSS and LNSS Positioning of Unmanned Transport Systems: The Brief Classification of Terrorist Attacks on USVs and UUVs. *Electronics* **2021**, *10*, 401. [CrossRef]
31. Konovaltsev, A.; Cuntz, M.; Haettich, C.; Meurer, M. Performance Analysis of Joint Multi-Antenna Spoofing Detection and Attitude Estimation. In Proceedings of the 2013 International Technical Meeting of the Institute of Navigation, San Diego, CA, USA, 28–30 January 2013.

32. Ballal, T.; Bleakley, C.J. Phase-difference ambiguity resolution for a single-frequency signal in the near-field using a receiver triplet. *IEEE Trans. Signal Process.* **2010**, *58*, 5920–5926. [CrossRef]
33. Ballal, T.; Bleakley, C.J. GNSS instantaneous ambiguity resolution and attitude determination exploiting the receiver antenna configuration. *IEEE. Trans. Aerosp. Electron. Sys.* **2014**, *50*, 2061–2069. [CrossRef]
34. Chen, J.; Shi, H.; Fang, Z.; Yuan, C.; Xu, Y. Performance Analysis of the GNSS Instantaneous Ambiguity Resolution Method Using Three Collinear Antennas. *IEEE Sens. J.* **2023**, *23*, 11936–11945. [CrossRef]
35. Li, J.; Zhu, X.; Ouyang, M.; Li, W.; Chen, Z.; Fu, Q. GNSS Spoofing Jamming Detection Based on Generative Adversarial Network. *IEEE Sens. J.* **2021**, *21*, 22823–22832. [CrossRef]
36. Goldma, A.; Devore, J.L. Probability and Statistics for Engineering and the Sciences. *Technometrics* **1988**, *30*, 235. [CrossRef]
37. Jareankam, W. A detection of outliers in random sample from normally distributed population using coefficient of skewness. *Burapha Sci. J.* **2020**, *25*, 236–245.