

Satellite Navigation Spoofing Interference Detection and Direction Finding Based on Array Antenna

Huiyun Yang ^{1,2}, Ruimin Jin ^{1,2,3,*}, Wenpu Xu ¹, Lei Che ^{1,3} and Weimin Zhen ¹¹ China Research Institute of Radiowave Propagation, Qingdao 266107, China² National Key Laboratory of Electromagnetic Environment, Qingdao 266107, China³ School of Electronic Engineering, Xidian University, Xi'an 710071, China

* Correspondence: jinrm@crip.ac.cn

Abstract: Satellite navigation signals are feeble when they reach the ground, so they are vulnerable to attacks from outside interference signals. By emitting spoofing interference signals similar to real satellite signals, spoofing interference can make receivers give wrong navigation, position, and time information, and it is challenging to detect. This seriously affects the safe use of GNSS; therefore, it is essential to identify spoofing interference signals quickly and accurately. In our study, we proposed a novel six-array spoofing-interference-monitoring array antenna, which achieved the detection and identification of spoofing interference sources by monitoring the relevant peaks and combining an airspace-trapping algorithm. Moreover, we quickly accomplished our search for the whole circumferential ambiguity by using long- and short-baseline algorithms, which can realize the high-precision detection of spoofing interference sources. To verify this method's accuracy, we conducted outdoor real experiments using a special spoofing interference source, and our experimental results show that our proposed array antenna's directional accuracy for spoofing interference signals is kept within 2°, showing high spoofing interference direction-finding capability.

Keywords: GNSS; array antenna; spoofing interference; detection; direction finding



Citation: Yang, H.; Jin, R.; Xu, W.; Che, L.; Zhen, W. Satellite Navigation Spoofing Interference Detection and Direction Finding Based on Array Antenna. *Sensors* **2023**, *23*, 1604. <https://doi.org/10.3390/s23031604>

Academic Editor: Shuai Zhang

Received: 21 December 2022

Revised: 27 January 2023

Accepted: 27 January 2023

Published: 1 February 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Global navigation satellite systems (GNSS) provide users with all-weather, high-precision position, velocity, and time (PVT) services, which are widely used in national economic and military fields, i.e., transportation, electricity, finance, telecommunications, military aviation, precision-guided weapons, etc. Because of the importance of satellite navigation systems to the security and economic development of each country, all major powers in the world are actively striving to develop their satellite navigation systems, which mainly include the GPS, Galileo, GLONASS, and Beidou systems of the United States, Europe, Russia, and China, respectively [1–4].

As GNSS is widely used in various fields, its radio magnetic environment is becoming increasingly complex, making the satellite signal in the transmission process extremely vulnerable to intentional or unintentional interference, which can seriously affect the satellite navigation system's ground monitoring, as well as the normal use of GNSS by users, posing a severe threat to the accuracy, availability, and integrity of satellite navigation. Unintentional interference is usually the result of electronic equipment signal leakage or natural phenomena, including radio frequency interference, ionospheric scintillation, the multipath effect, and non-line of sight (NLOS) propagation [5], etc. Intentional interference, including suppression and spoofing interference, usually disrupts normal satellite communications, forges spoofing interference signals, and generates suppression signals to block and deceive ground receivers so that the receiver obtains incorrect information [6]. Suppression jamming is performed by high-power-emitting signals so that the real satellite signal is drowned in the interference signal in terms of power or frequency band, meaning the navigation receiver cannot work normally. Spoofing interference techniques are

relatively complex and are divided into transponder and generative spoofing interference categories. Among them, transponder spoofing interference through the spoofing interference source to receive the real signal modifies the real signal and then sends it out, while generative spoofing interference requires understanding the satellite structure to forge the satellite signal. Both ways deceive the navigation user so that they cannot be correctly positioned. Due to its particularity, the military signals in satellite navigation usually have confidentiality in the signal generation method and signal format, meaning the outside world cannot know the satellite signal parameters in advance; therefore, there are certain technical difficulties when attempting satellite military signal interference [7]. However, considering the extensiveness and convenience of civil satellite signals, the modulation mode and signal format of satellite signals are usually in an open state, making civil satellite signals extremely susceptible to various forms of interference [8,9].

Although the technology involved in spoofing interference is relatively complex, its harm is apparent. Currently, GNSS civil navigation signals are more susceptible to interference by GNSS navigation spoofing signal generators because they are not encrypted like military signals. This causes the navigation receiver to acquire misplaced position information under normal working conditions; therefore, spoofing interference must be detected, weakened, or eliminated.

In 2016, Lee et al. used the signal quality monitor (SQM) algorithm for spoofing interference detection based on the characteristics of spoofing signals that distort the correlation peaks [10]; in 2017, Margarita et al. studied the characteristics related to spoofing interference and improved the receiver of the Galileo system to achieve the function of anti-spoofing interference [11], but the method is only theoretically applicable to some civil systems, and there is no special equipment; in 2018, Geng proposed that the receiver could estimate the signal power before despreading its received signal [12] to realize the detection of the spoofing signal, which can significantly reduce the amount of target-receiver computation—its implementation is simple but the applicability of the spoofing scenario is not high. In 2019, Zhang et al. exploited the fact that transposed spoofing interference is a delay to the real satellite signal by combining the observation of the number of correlation peaks with measuring the half-height width size to achieve the detection of spoofing interference with large and small time delays [13]. In 2020, Li et al. proposed a convolutional neural network-based method to effectively detect the presence of small-delay spoofing interference signals, with the method achieving high detection accuracy for small-delay spoofing interference signals [14]. In 2022, Wang et al. used the power combined with the SQM (PCS) method to detect spoofing interference signals and improve detection timeliness [15].

Aiming at the problem that the traditional spoofing interference detection method cannot locate the direction of the spoofing interference source, many scholars proposed the use of an array antenna to locate the direction of the spoofing interference source, drawing on the relevant interferometer direction measurement principle; using the same signal received by different array elements of the carrier phase difference to build the observation, it can realize the direction of the signal captured by the receiver. Spoof interference detection and identification can be achieved by comparing the satellite direction with the ephemeris solution. However, their methods remain in the experimental simulation stage and are not verified in the real outdoor environment. In the real environment, there will be interference from the external environment such as multipath, which has some influence on the detection of spoofing interference signals.

In our study, an L-shaped six-array antenna was specially designed for spoofing interference. In the real environment, the method we designed can realize the simultaneous capture and tracking of the normal and interference signals of the same satellite through multimodal monitoring and effectively separate the real satellite and spoofing interference signals by using the airspace identification method, followed by the long- and short-baseline interferometric-direction-finding method of the spoofing interference source to locate the direction of the interference source through the designed antenna array.

2. Materials and Methods

2.1. Spoofing Interference Sources

Spoofing interference, including transponder and generation interference, uses signal acquisition equipment to capture and amplify spoofing interference signals for directly broadcasting. Generative interference, on the other hand, simulates the generation of pseudosatellite signals and broadcasts them according to the institutional requirements of the navigation signal, which is more difficult to achieve compared with transponder interference.

Transponder spoofing interference is the direct transponder of the real navigation signals by the spoofing interference sources. Figure 1 shows that after delay and power amplification, S1, S2, S3, and S4 denote satellites, J denotes the position of the spoofing interference sources, R denotes the position of the normal receiver, and F denotes the position to which the receiver is spoofed to locate. The spoofing interference source generates a spoofing signal by forwarding the real signal without generating a high-fidelity interference signal; the spoofing interference signal is captured by receivers within a certain range, which is relatively easy to implement technically. Furthermore, its power is stronger than the real signal, meaning there is a high probability of being captured. Theoretically, successful spoofing is a probabilistic event.

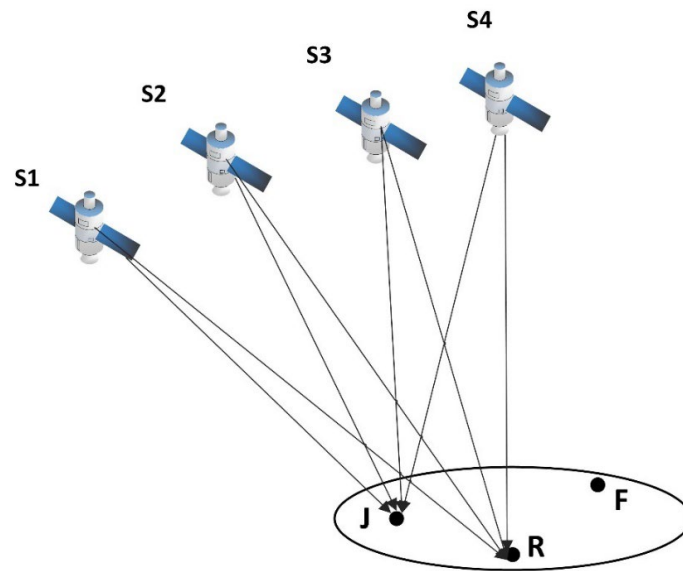


Figure 1. Transponder spoofing interference schematic.

A spoofing interference source is placed at J . In the interference effective region, the spoofed receiver is assumed to be located at R . If the spoofing destination is F , then:

$$\begin{aligned}\rho_1 &= S_1F + ct_R \\ \rho_2 &= S_2F + ct_R \\ \rho_3 &= S_3F + ct_R \\ \rho_4 &= S_4F + ct_R\end{aligned}\quad (1)$$

If ρ_i ($i = 1, 2, 3, 4$) is the observation pseudorange, $S_i f$ ($i = 1, 2, 3, 4$) is the distance from the satellite to the spoofing point, and c is the speed of light, t_R is the receiver clock difference (atmospheric delay is neglected in the equation), and the equation when the receiver at the R is subjected to the transponder spoofing interference signal is:

$$\begin{aligned}\rho'_1 &= S_1J + JR + ct_1 + ct_R \\ \rho'_2 &= S_2J + JR + ct_2 + ct_R \\ \rho'_3 &= S_3J + JR + ct_3 + ct_R \\ \rho'_4 &= S_4J + JR + ct_4 + ct_R\end{aligned}\quad (2)$$

If ρ'_i ($i = 1, 2, 3, 4$) is the observation pseudorange of the transponder, $S_i J$ ($i = 1, 2, 3, 4$) is the distance from the satellite to the spoofing interference source, JR is the distance from the spoofing interference source to receiver, c is the speed of light, t_i is the delay time to the signal of the satellite, t_R is the receiver clock difference (atmospheric delay is neglected in the equation), let $\rho_i = \rho'_i$, according to the pseudorange positioning principle of the GNSS, Equations (1) and (2) will solve the same position, and $S_i F = S_i J + JR + ct_i$. Because the physical delay needs to be positive, it is required that $JR < S_i F - S_i J$, and when the timing is accurate and does not affect the receiver clock difference, assuming that the condition is not satisfied, then

$$\tau = \frac{\min(S_i F - S_i J - JR)}{c} \quad (3)$$

The delay correction is $t'_i = t_i + |\tau|$, and the receiver clock difference resulting from the substitution in Equation (3) is $t'_R = t_R + |\tau|$. The receiver clock difference has a jump, which is not what the spoofers would like to see. This is the disadvantage of transponder spoofing interference, which puts a high demand on the real-time performance of the spoofing interference sources.

Generative spoofing interference is the premise that the interferer does not rely on the real signal and independently emits a spoofing signal similar to the real signal. Through the relative motion of the peaks associated with the two, the spoofing peak gradually strips the real peak from the tracking loop by virtue of its power advantage, and then controls the tracking loop [16,17]. Figure 2 shows the generative spoofing interference flow.

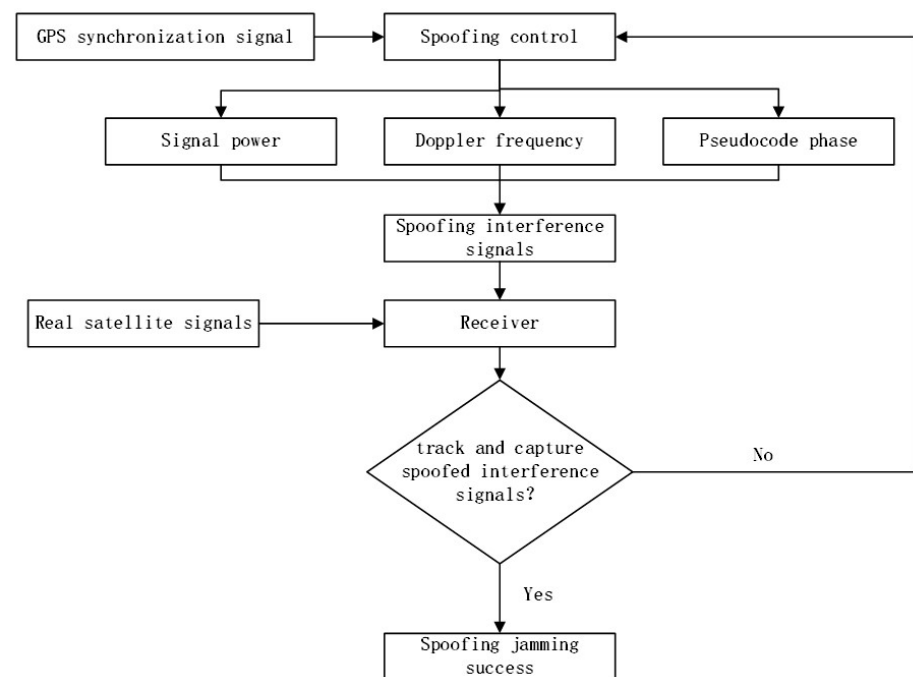


Figure 2. Generative spoofing interference process.

GNSS spoofing interference signals typically include the following characteristics:

- (1) The frequency/pseudocode sequence of the interference signal is the same as the normal GNSS signal;
- (2) There is a difference between the phase of the interference signal pseudocode and the normal GNSS signal, usually greater than 1.5 code chips;
- (3) A single spoofing interference source usually broadcasts more than 4 GNSS satellite spoofing interference signals simultaneously.

When there is a GNSS spoofing interference source around the GNSS receiver, the GNSS receiver will directly capture the peak position related to the spoofing interference

signal in the satellite capture stage under the condition that the relevant peak's maximum determination criterion is adopted, and the spoofing interference signal will be stably tracked through the tracking loop. When each channel of the GNSS receiver is stably tracked to the spoofing interference signal, the receiver positioning solution result is completely controlled by the GNSS spoofing interferer. To realize the monitoring and effective identification of GNSS interference signals, the GNSS receiver can monitor according to the relevant peak morphology of each satellite and deceive the interference and identification of real satellite signals through the airspace characteristics of real satellite and interference signals [18,19].

To facilitate the experiment, this paper uses a self-researched spoofing interference source. The spoofing interference source can simultaneously send the spoofing navigation signal of the three GPS L1/BDS B1I/BDS B1C frequency points, while the navigation signal power and pseudocode can be set as needed, and the power of the spoofing interference signal is continuously adjustable within $-135\sim-60$ dBm. Furthermore, our methods are verified according to the test requirements.

Figure 3 shows the flow of spoofing interference detection.

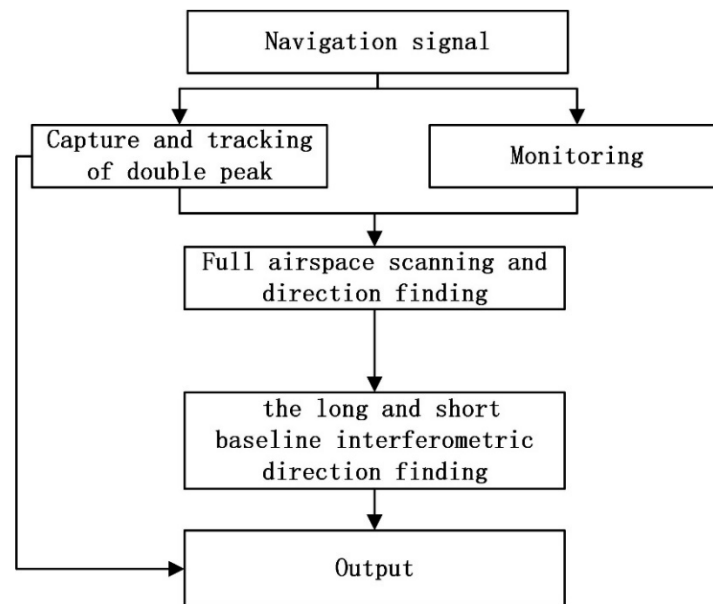


Figure 3. Spoofing interference detection process.

2.2. Spoofing Interference Detection

In the absence of interference, taking the GPS L1 navigation signal as an example, the satellite signal received by the receiver is

$$s(t) = c_i(t) \times d_i(t) \cos(2\pi(f_i + \Delta f_i)t + \theta) \quad (4)$$

where $c_i(t)$ is the spread spectrum code sequence of the i -th satellite, $d_i(t)$ is the navigation message information of the i -th satellite, f_i is the center frequency of the i -th satellite, Δf_i is the Doppler shift of the i -th satellite, and θ is the initial phase of the i -th satellite. After the receiver is synchronized through the captured trace, the receiver can ideally obtain a navigation signal correlation function, which is:

$$R(\tau) = 1 - |\tau|/T_c \quad (5)$$

where $R(\tau)$ is the baseband correlation function after the accurate stripping of carrier Doppler, τ is the delay of the initial phase of the local spread spectrum code and the phase

difference between the received navigation signals, and T_c is the spread spectrum code period of the navigation signal.

In the presence of spoofing interference, the satellite signal received by the receiver is:

$$s_m(t) = A_i(t)c_i(t) \times d_i(t)\cos(2\pi(f_i + \Delta f)t + \theta) + \sum_{k=1}^n B_k(t)c_i(t + t_k) \times d_i(t + t_k)\cos(2\pi(f_i + \Delta f_k)t + \theta_k) \quad (6)$$

where $s_m(t)$ is the navigation signal received by the receiver containing spoofing interference, $c_i(t)$ represents the spread spectrum code of the i th satellite, $d_i(t)$ represents the navigation message data of the i th satellite, t_k represents the time difference between the initial pseudocode phase between the spoofing interference signal and the real signal, Δf_k represents the Doppler frequency offset of the spoofing interference signal, $A_i(t)$ represents the amplitude of the real navigation signal, $B_k(t)$ represents the amplitude of the spoofing interference signal, and k represents the existence of k spoofing interference source signals for the i -th navigation satellite. The receiver navigation signal correlation peak function can be expressed as:

$$R_m(\tau) = A_i^2(1 - |\tau|/T_c) + \sum_{k=1}^n B_k^2(1 - |\tau - t_k|/T_c)\cos(\theta_k - \theta) \quad (7)$$

The detection of multi-correlated peaks can be expressed as the following ternary hypothesis problem: satellite signal correlated peaks and spoofing signal correlation peaks and no navigation signal.

$$\begin{cases} H_0 : x_n = W_n \\ H_1 : x_n = S_n + W_n \\ H_2 : x_n = S_n^{(sp)} + W_n \end{cases} \quad (8)$$

where W_n is additive white noise, S_n is the real satellite signal, $S_n^{(sp)}$ is the spoofing interference signal, and x_n is the detection amount. H_0 , H_1 , and H_2 indicate that the navigation signal does not exist, the navigation signal exists, and the spoofing signal exists, respectively. Based on the real satellite signal detection threshold V_t , a threshold V_s is introduced when the number of relevant peaks exceeding the detection threshold V_t is more than two and the relevant peak exceeds the threshold V_s , while the signal corresponding to the relevant peak is considered to be a spoofing signal. The relationship between the detection statistic V and thresholds V_t and V_s can be expressed as:

$$\begin{cases} H_0 : V < V_t \\ H_1 : V_t \leq V < V_s \\ H_2 : V \geq V_s \end{cases} \quad (9)$$

Assuming H_1 and H_2 , the signal strength is $\lambda \gg \sigma_n^2$, in which case the mean of the detection statistic V is approximately expressed as:

$$E(V) = \sqrt{\frac{\pi}{2}}\sigma_n L_{\frac{1}{2}}\left(-\frac{\lambda^2}{2\sigma_n^2}\right) \approx \lambda \quad (10)$$

where σ_n is the noise intensity, and the Lagrangian polynomial $L_{\frac{1}{2}}$ is:

$$L_{\frac{1}{2}}(x) = e^{\frac{x}{2}} \left[(1-x)I_0\left(-\frac{x}{2}\right) - xI_1\left(-\frac{x}{2}\right) \right] \quad (11)$$

where I_0 and I_1 are zero- and first-order modified Bessel functions, respectively.

Because navigation and spoofing signals are independently distributed, their probability density functions are:

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

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

where v is the detection statistic, λ_1 is the mean of the incoherent integration of the navigation signal, λ_2 is the mean of the incoherent integration of the spoofing interference signal, and $\lambda_2 > \lambda_1$.

The spoofing signal detection false-alarm probability can be expressed as:

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

where v is the detection statistic, and V_s is the set spoofing interference detection threshold.

Therefore, given the noise power σ_n^2 , false-alarm probability P_{fa} , and mean λ_1 of the non-coherent integral of the navigation signal, the spoofing signal power detection threshold V_s can be calculated, and the spoofing interference signal can be detected by the multimodal detection of the capture module.

2.3. Spoofing Interference Identification

Considering that the multipath of a single satellite of the receiver will also introduce a multimodal environment, which will lead the receiver to recognize false alarms for fraudulent interference [20], based on multimodal detection, we used the multi-antenna array to zero the notch to identify the wave arrival angle of all satellites [21–25].

The navigation signal received by the GNSS array antenna enters the system through the antenna array composed of M antennas, as shown in Figure 4, and the data are converted into an MN channel after delay processing, which is represented by the symbol X . W represents the processor weight vector ($MN \times 1$ dimension), and $R = E[XX^H]$ represents the covariance matrix ($MN \times MN$ dimension) of the received data.

Zeroing weights for a certain direction is equivalent to a constrained optimization problem:

$$w_s^{opt} = \arg \min w^H R w, \quad w^H S = 1 \quad (15)$$

where S is the space-time two-dimensional guide vector, $S = S_S \otimes S_T$, where $\otimes$ is the Krocker product, $S_S = [1, e^{jw_s}, \dots, e^{j(M-1)w_s}]^T$, and $S_T = [1, e^{jw_t}, \dots, e^{j(N-1)w_t}]^T$. $w_s = \frac{2\pi d \sin \theta}{\lambda}$ and $w_t = 2\pi f T_s$, where d is the distance between two adjacent antennas in the antenna array, θ is the angle of incidence, that is, the angle between the direction of incidence and the normal direction of the array, and λ is the wavelength. The solution of the optimal space-time processor is:

$$w_s^{opt} = [S^H R^{-1} S]^{-1} R^{-1} S (MN \times 1) \quad (16)$$

Figure 5 shows the schematic of airspace trap. If the receiver finds that some satellites have multimodal characteristics, it can complete the zero-trapping direction of the received signal by zero-trap scanning in the whole airspace, and when more than four satellites lose signals or the carrier-to-noise ratio is greatly reduced in a certain direction, the existence of a spoofing interference signal is determined and the direction of the incoming wave of the spoofing interference signal is obtained.

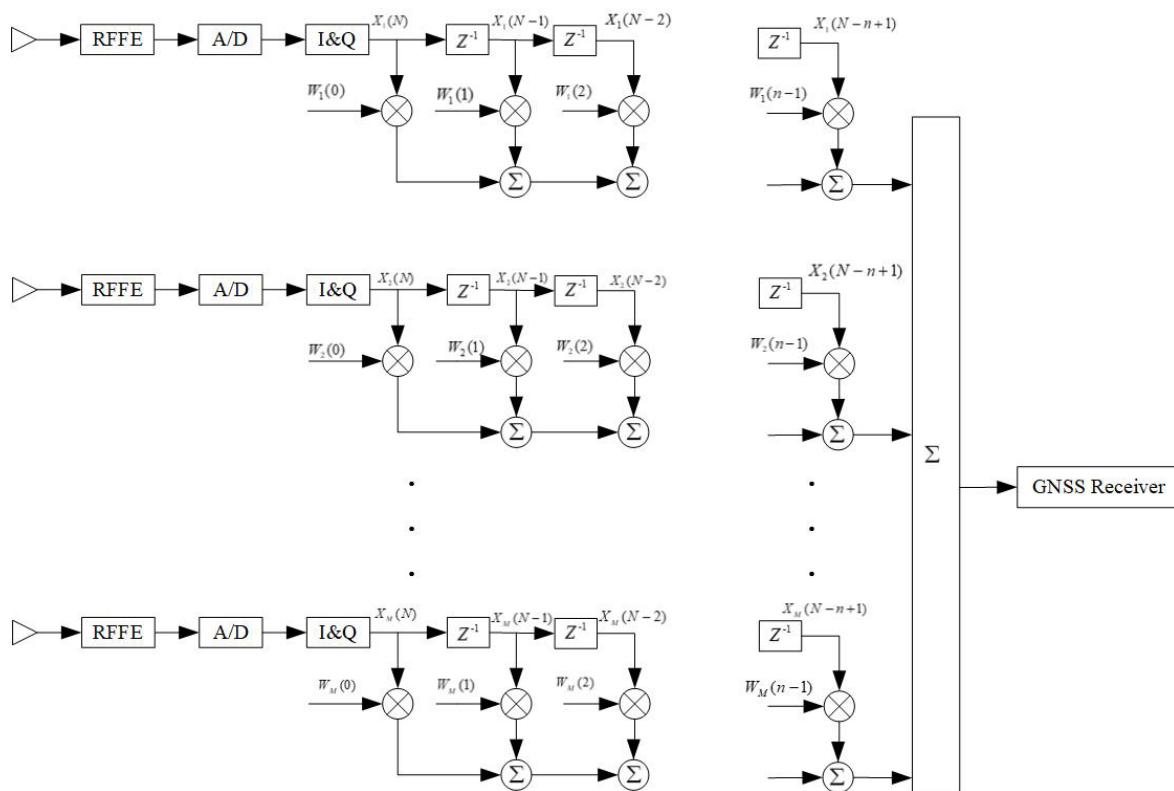


Figure 4. Space-time two-dimensional filtering algorithm.

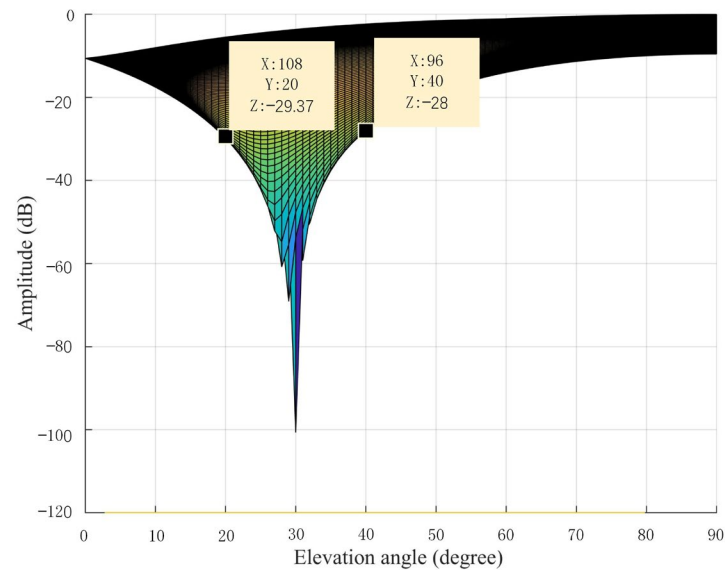


Figure 5. Zero airspace scanning beamwidth.

2.4. Spoofing Interference Source Direction Finding

In this study, we adopted the long- and short-baseline interferometric-direction-finding method for the direction finding of the deceptive interference source, and the direction-finding accuracy is related to the array antenna array [26,27], while the designed array antenna configuration is as follows in Figure 6:

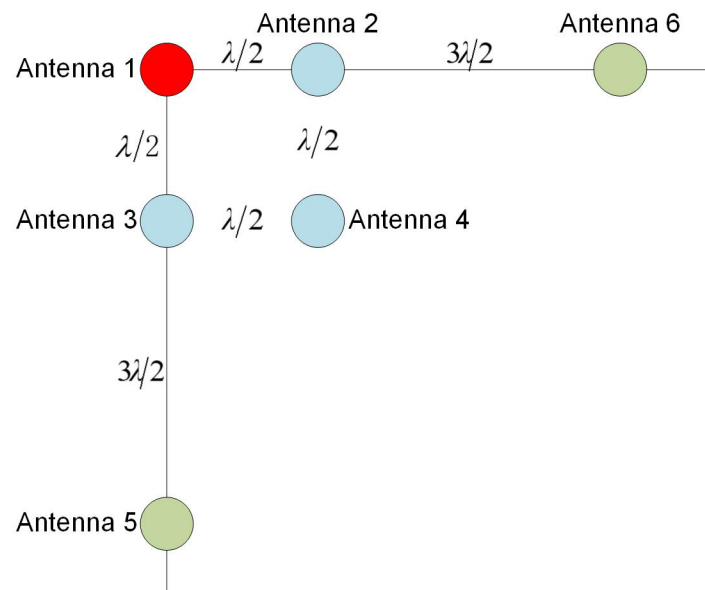


Figure 6. Array antenna configuration.

The direction-finding accuracy of the spoofing interferer can be obtained by referring to the interferometric goniometric formula, and the specific calculation steps are as follows:

(1) The baseline lengths of antennas 1 and 2 are the half wavelength, and we used the long- and short-baseline algorithm to remove the integer ambiguity of the carrier phase spoofing interference source.

(2) The angular accuracy is directly related to the incidence angle and carrier phase tracking accuracy, which can be calculated by index decomposition through the engineering experience formula.

$$\Delta\theta = \frac{\lambda\Delta\varphi}{2\pi d\cos\theta} + \frac{\Delta\lambda}{\lambda}\tan\theta \quad (17)$$

where λ is the GNSS signal wavelength, d is the antenna baseline length, $\Delta\varphi$ is the carrier phase tracking error, θ is the incidence angle of the spoofing interference source, and $\Delta\lambda$ is the wavelength measurement error introduced by Doppler.

In the above equation, interferometric goniometry adopts a third-order PLL carrier tracking loop, and the wavelength measurement error introduced by the carrier Doppler is negligible when the receiver is working stably; therefore, the angle measurement error formula can be simplified to

$$\Delta\theta = \frac{\lambda\Delta\varphi}{2\pi d\cos\theta} \quad (18)$$

where $\Delta\varphi$ is the amount of PLL carrier phase measurement error after the stable tracking of the receiver carrier tracking loop, which is directly related to the signal-to-noise ratio of the spoofing interferer signal and the receiver phase noise; and after receiving the stable tracking spoofing interferer signal, the carrier phase measurement accuracy can be expressed as:

$$\sigma_{PLL} = \frac{180^\circ}{\pi} \sqrt{\frac{B_L}{C/N_0} \left(1 + \frac{1}{2T_{coh}C/N_0} \right)} \quad (19)$$

where B_L is the loop noise bandwidth, C/N_0 is the carrier-to-noise ratio, and T_{coh} is the pre-detection integral time.

(3) Using a right-angle interference array, after simulation analysis, under the condition that the carrier phase measurement error is fixed, the single-baseline angle measurement accuracy is approximately 11.5° when the incidence angle is 50° , and the angular measurement accuracy is 8° at the incidence angle of 22° . Considering that the system adopts a vertical double baseline for direction finding, the baseline angle is 90° , and when the

incidence angle is $>45^\circ$, the vertical baseline can be used to complete the direction finding of the interference source, while the short-baseline direction-finding accuracy is 13° (RF-channel zero value and antenna installation error factors).

(4) To ensure the accuracy of direction finding of deceptive interference sources, our use of antennas 1, 2, 3, 5, and 6 involved vertical double baselines to achieve the accurate direction finding of deceptive interference sources, while the lengths of the long and short baselines were $\lambda/2$ and 2λ , respectively. The long baseline in this mode can quickly complete the whole week fuzzy search through short-baseline assistance, realizing the high-precision direction-finding function.

After simulation analysis, under the condition that the carrier phase measurement error is fixed, the single-baseline angle measurement accuracy is about 6° at 75° , and 2.2° at 45° . Considering that the system adopts vertical double-baseline direction finding, the baseline angle is 90° , and when the incidence angle is 45° , the vertical baseline can be used to complete the direction finding of the interference source, and the accuracy of the long baseline angle measurement is 1.3° .

3. Results and Discussion

For a single spoofing interference source, we used our direction-finding method to establish an outfield test environment. The test equipment included a spoofing interference source, transmitting antenna, set of high-precision directional receiver computers, power supply, set of RF cables, and spoofing interference detection and direction-finding device.

On a circumference with a deceptive interference detection and direction-finding antenna as the center and a radius of 30 m, a high-precision GNSS receiver was used to calibrate a point every 60 degrees, and 0 degrees represented the true north direction. The transmitting antenna of the interference source was placed on each calibration point in turn, the direction of the deceptive interference source was determined, and when the deceptive interference source transmitting antenna is erected, the incidence angle should be greater than 15 degrees by as much as possible.

Table 1 shows that, when the power of the spoofing signal is -124 dBm, the spoofing interference source simultaneously broadcasts the synchronous spoofing signal of satellites 6/8/13/9/16 and regenerates the spoofing signal of satellite 19. The two types of interference signals are simultaneously transmitted in one channel to realize spoofing interference to the regional receiver.

Table 1. Result of spoofing interference detection.

Channel	Satellite Number	Pseudorange (m)	C/N0	Track Status	Detection Result
1	6	36,273,924.8	40.9	Tracking	True
2	36	22,249,771.6	46.6	Tracking	True
3	13	36,668,067.6	42.3	Tracking	True
4	16	36,508,379.1	44.9	Tracking	True
5	2	37,236,339.6	41.2	Tracking	True
6	3	36,890,554.3	38.5	Tracking	True
7	26	26,477,344.4	44.2	Tracking	True
8	6	36,159,106.3	41.9	Tracking	Spoofing
9	9	36,766,094.4	39.7	Tracking	True
10	21	24,020,616.0	41.9	Tracking	True
11	22	21,789,099.7	45.5	Tracking	True
12	8	37,401,729.9	38.9	Tracking	True
13	8	36,992,831.9	41.3	Tracking	Spoofing
14	13	36,637,555.0	40.6	Tracking	Spoofing
15	19	23,981,686.4	35.9	Tracking	True
16	9	37,031,246.4	41.4	Tracking	Spoofing
17	19	24,176,708.4	40.6	Tracking	Spoofing
18	16	36,473,256.8	41.8	Tracking	Spoofing
19	5	38,484,892.8	36.4	Tracking	True

Figure 7 shows the correlation peaks in spoofing interference environment. This method can simultaneously capture and track the normal and interference signals of the same satellite through multi-peak monitoring and realize the multi-channel concurrent tracking of satellites 6/8/13/9/16 to complete the spoof interference monitoring. Therefore, the spatial identification method can be used to effectively separate real satellite signals from spoofing interference signals. Our test results show that channels 1–7, 9–13, 16, and 20 are tracking normal GPS signals, and channels 6, 14, 15, 17, 18, and 19 are spoofing interference signals, which is consistent with the signals sent by spoofing interference sources.

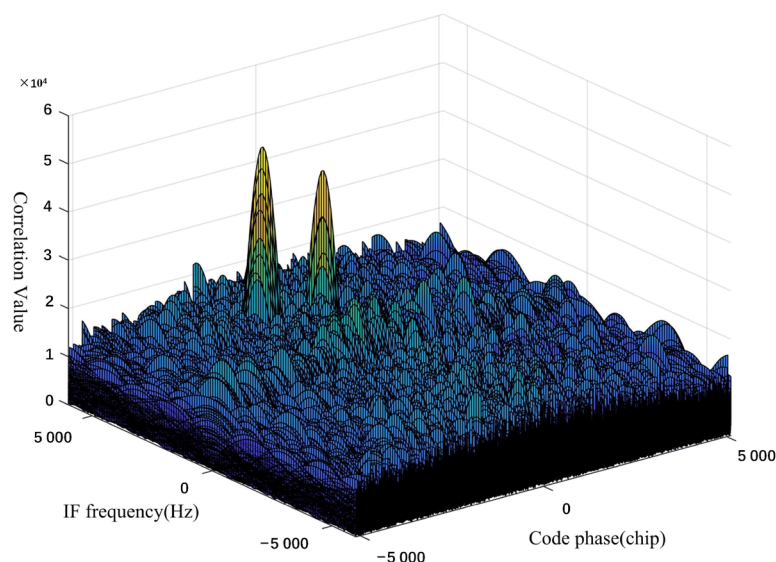


Figure 7. Schematic diagram of frequency-code two-dimensional correlation peaks in spoofing interference environment.

At the same time, we calculated the detection time of the spoofing interference. The average time from the signal source to the detection of spoofing interference is about 7.7 s, showing good real-time detection. Table 2 shows the detection-time statistics:

Table 2. Time of spoofing interference detection.

Number	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	Average
Time(s)	5.59	6.72	4.60	5.19	3.53	6.53	4.62	7.43	3.09	4.94	5.22

We used our novel vertical dual-baseline antenna array to achieve accurate direction findings of spoofing interference sources. In this mode, the long baseline can be assisted by the short baseline to quickly complete the whole-circle fuzzy search and realize the high-precision direction-finding function. The mean error accuracy is kept within 2° at approximately 1.4° . Table 3 shows the test's direction-finding results.

Table 3. Angle of direction finding.

Number	Ideal Angle	Actual Measurement Angle	Direction Angle	Relevance
1	0°	0.07°	0.60°	0.53°
2	60°	59.96°	58.10°	1.86°
3	120°	119.97°	121.45°	1.48°
4	180°	181.01°	183.44°	2.43°
5	240°	240.31°	241.10°	0.79°
6	300°	300.14°	301.53°	1.39°

Due to the existence of the antenna installation and RF-channel zero-calibration errors in the actual tests, there will also be complex multipath interference and other problems; therefore, the calibration of the electronic compass and cable will also have some impact on accuracy. The angle measurement accuracy error of this method is slightly lower than the simulation results. However, it can still achieve high direction-finding accuracy.

4. Conclusions

In our study, we detected the spoofing interference source by monitoring the correlation peaks and zeroing the spatial notch, which effectively reduces the false alarm caused by the multipath environment. At the same time, we designed an antenna array with vertical double baselines, which uses its long and short baselines to quickly complete the whole-circle ambiguity search and realize the high-precision direction finding of spoofing interference sources, with a directional accuracy within 2° and detection time of about 5 s. The designed method has high precision and strong feasibility, can be used as a reference for other navigation-frequency-band spoof detection and direction-finding methods, and has high theoretical and practical value. At present, this method has been applied to the equipment developed and verified in the test.

At present, there are still some problems to be solved, and future research can be carried out in the following aspects:

- (1) Although we verified the reliance on array antennas for spoofing interference detection and direction finding using a relatively simple electromagnetic environment through experiments, in a complex electromagnetic environment, the receiver will be affected by a variety of interference types, such as ionospheric scintillation, solar radio burst, suppression, and spoofing interference. At present, research on interference detection mostly focuses on one of the interferences alone, meaning that methods of unified identification and the classification of different interferences need to be urgently studied;
- (2) The traditional spoofing interference detection methods are limited by the model or need additional equipment, and the detection parameters are single, making it difficult to reflect the characteristics of spoofing interference signals comprehensively. In the future, deep-learning-based methods could be considered for studies of spoofing interference detection methods based on the existing receivers.

Author Contributions: Conceptualization, W.Z. and R.J.; methodology, H.Y.; software, L.C.; validation, W.X.; formal analysis, H.Y.; investigation, R.J.; writing—original draft preparation, H.Y.; writing—review and editing, L.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program, grant number 2018YFB0505100.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge the technical and administrative support from individuals throughout the data collection and calibration process. In addition, we thank the editor and four anonymous reviewers for providing helpful comments and suggestions, which substantially improved the manuscript.

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

References

- Chang, C.L.; Juang, J.C. Effect of Array Configurations on the Performance of GNSS Interference Suppression. *Int. J. Control Autom. Syst.* **2008**, *6*, 884–893.
- Gao, Y.J.; Li, G.Y.; Lv, Z.W. Current Situation and Prospect of Satellite Navigation Interference Technology. *Geomat. Spat. Inf. Technol.* **2022**, *45*, 13–18.
- Pang, J.; Ni, S.J.; Nei, J.W.; Ou, G. An Overview to GNSS Spoofing Technologies. *Fire Control Command Control* **2016**, *41*, 1–4+9.
- Zhang, Y.; Qiu, J.Y. Recognition Technology of GNSS Spoofing with Wavelet Singular Value and SVM. *Commun. Technol.* **2022**, *55*, 468–472.
- Dovis, F. *GNSS Interference Threats and Countermeasures*; Radar Receivers; Artech House: Boston, MA, USA, 2015.
- Fan, G.W.; Deng, J.N.; Wang, Z.H.; Lei, C. Study of GNSS Interference Detection Technology Based on Energy Detection. *Radio Eng.* **2013**, *43*, 33–35+39.
- Gao, G.X.; Heng, L.; Hornbostel, A.; Denks, H.; Meurer, M.; Walter, T.; Enge, P. DME/TACAN interference mitigation for GNSS: Algorithms and flight test results. *GPS Solut.* **2013**, *17*, 561–573. [\[CrossRef\]](#)
- Lindström, J.; Akos, D.M.; Isoz, O.; Junered, M. *GNSS Interference Detection and Localization Using a Network of Low Cost Front-End Modules*; Institute of Navigation: Manassas, VA, USA, 2007.
- 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. [\[CrossRef\]](#)
- Lee, J.-H.; Kwon, K.-C.; An, D.-S.; Shim, D.-S. GPS spoofing detection using accelerometers and performance analysis with probability of detection. *Int. J. Control Autom. Syst.* **2015**, *13*, 951–959. [\[CrossRef\]](#)
- Margaria, D.; Motella, B.; Anghileri, M.; Floch, J.-J.; Fernandez-Hernandez, I.; Paonni, M. Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives. *IEEE Signal Process. Mag.* **2017**, *34*, 27–37. [\[CrossRef\]](#)
- Geng, Z.L.; Li, Z.R.; Nei, J.W.; Wang, F.X. Spoofing detection technique before despreading for GNSS antenna-array receivers. *J. Natl. Univ. Def. Technol.* **2018**, *40*, 91–96.
- Zhang, G.L.; Ding, J.C.; Zhang, Y. Research on Repeater Deception Jamming Detection Algorithm Based on GNSS Signal Delay Characteristics. *Radio Eng.* **2019**, *49*, 626–630.
- Li, J.; Zhu, X.; Ouyang, M.; Li, W.; Chen, Z.; Dai, Z. Research on Multi-Peak Detection of Small Delay Spoofing Signal. *IEEE Access* **2020**, *8*, 151777–151787. [\[CrossRef\]](#)
- Wang, L.; Zhang, L.J.; Wu, R.B. GNSS spoofing detection based on power monitoring combined with SQM. *J. Signal. Process.* **2022**, 1–12. Available online: <https://kns.cnki.net/kcms/detail/11.2406.TN.20221021.1127.002.html> (accessed on 20 December 2022).
- Wang, J.Q.; Sun, G.F.; Tang, X.M.; Ma, C.J.; Ma, P.C. GNSS Spoofing Signal Parameters Estimation Using NELDER-MEAD Simplex Algorithm. *J. Signal Process* **2022**, *38*, 2606–2616.
- Zhang, X.R.; Li, H.; Yang, C.; Lu, M.Q. Influence of spoofing interference on GNSS vector tracking loops. *J. Tsinghua Univ. Sci. Technol.* **2022**, *62*, 163–171. [\[CrossRef\]](#)
- Wang, W.Y.; Wang, P.H. GNSS Spoofing Interference Detection Based on Acquisition Results. *J. Signal Process.* **2021**, *37*, 1460–1469. [\[CrossRef\]](#)
- Gao, G.X.; Sgammini, M.; Lu, M.; Kubo, N. Protecting GNSS Receivers from Jamming and Interference. *Proc. IEEE* **2016**, *104*, 1327–1338. [\[CrossRef\]](#)
- Wildemeersch, M.; Slump, C.H.; Rabbachin, A. Acquisition of GNSS signals in urban interference environment. *IEEE Trans. Aerosp. Electron. Syst.* **2014**, *50*, 1078–1091. [\[CrossRef\]](#)
- Daneshmand, S.; Jafarnia-Jahromi, A.; Broumandan, A.; Lachapelle, G. A GNSS structural interference mitigation technique using antenna array processing. In Proceedings of the 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), A Coruna, Spain, 22–25 June 2014.
- Borio, D.; Camoriano, L.; Presti, L.L. Two-Pole and Multi-Pole Notch Filters: A Computationally Effective Solution for GNSS Interference Detection and Mitigation. In Proceedings of the International Conference on Telecommunications, St. Petersburg, Russia, 16–19 June 2008.
- Arribas, J.; Fernandez-Prades, C.; Closas, P. Antenna Array Based GNSS Signal Acquisition for Interference Mitigation. *Aerosp. Electron. Syst. IEEE Trans.* **2013**, *49*, 223–243. [\[CrossRef\]](#)
- Arribas, J.; Closas, P.; Fernandez-Prades, C. Interference mitigation in GNSS receivers by array signal processing: A software radio approach. In Proceedings of the Sensor Array & Multichannel Signal Processing Workshop, A Coruna, Spain, 22–25 June 2014.
- Tang, H.J.; Huang, Q.L.; Zeng, H. Anti-spoofing methodology using nulling antenna in GNSS. *J. Nanjing Univ. Inf. Sci. Technol Nat. Sci. Ed.* **2022**, 1–9. Available online: <https://kns.cnki.net/kcms/detail/32.1801.N.20220922.1609.004.html> (accessed on 20 December 2022).
- Sun, F.L.; Yin, J.L.; Li, F.; Zeng, H. Space-time Joint Detection Algorithm for GNSS Spoofing Interference GNSS. *Comput. Simul.* **2022**, *39*, 60–65.
- Nie, J.W.; Rui, G.E.; Min, L.I.; Wang, F.X. The Influence Analysis of Narrowband Hypothesis to GNSS Array Anti-jamming Performance Evaluation. *J. Natl. Univ. Def. Technol.* **2011**, *35*, 128–133.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.