ORIGINAL RESEARCH
published: 15 June 2022
doi: 10.3389/fphy.2022.905918

GNSS Spoofing Suppression Based on Multi-Satellite and Multi-Channel Array Processing

Shaojie Ni, Binbin Ren, Feiqiang Chen, Zukun Lu, Jie Wang, Pengcheng Ma and Yifan Sun*

Department of Electronic Science and Technology, National University of Defence Technology, Changsha, China

The endless spoofing interference affects the credibility of the navigation system seriously. In order to suppress the forward spoofing which is more threatening to military signals in GNSS, this paper proposes a spoofing suppression algorithm based on angle of arrival estimation and multi-satellite fusion. On the basis of successfully suppressing the spoofing signal, the algorithm improves the estimation accuracy of the angle of arrival of the forwarded spoofing and reduces the attenuation of the carrier to noise ratio of the real satellite signal. Finally, the effectiveness of the algorithm is verified by simulation, which has guiding significance for the anti-spoofing research of GNSS.

Keywords: GNSS, the forwarding spoofing, array multi-channel processing, spoofing suppression, multi-satellite signal processing, antenna array

OPEN ACCESS

Edited by:
Jaroslav Chum,
Institute of Atmospheric Physics (ASCR), Czechia

Reviewed by:
Ilya Edemskiy,
Institute of Solar-Terrestrial Physics (RAS), Russia
Jaroslav Urbář,
Istituto Nazionale di Geofisica e Vulcanologia (INGV), Italy

****Correspondence:***
Binbin Ren
renbinbin@nudt.edu.cn

Specialty section:
This article was submitted to Space Physics, a section of the journal Frontiers in Physics

Received: *28 March 2022*
Accepted: *23 May 2022*
Published: *15 June 2022*

Citation:
Ni S, Ren B, Chen F, Lu Z, Wang J, Ma P and Sun Y (2022) GNSS Spoofing Suppression Based on Multi-Satellite and Multi-Channel Array Processing.
Front. Phys. 10:905918.
doi: 10.3389/fphy.2022.905918

1 INTRODUCTION

Global Navigation Satellite System (GNSS) is a space-based radio navigation and positioning system that can provide users with all-weather location, navigation, and timing information. At present, the world's four major global satellite navigation system suppliers are: the GPS system of the United States, the "Beidou-3″ satellite navigation system of People's Republic of China, the GLONASS system of Russia, and the Galileo system of Europe Union [1]. Japan and India are also focusing on the regional satellite navigation system research in their own countries [2]. From transportation in the civilian field [3], weather forecasting [4], power system [5], smart wear, hydrological monitoring [6], disaster relief [7], financial security [8], to individual combat in the military field Satellite navigation systems play an irreplaceable role in all aspects such as precision strikes, and sea escort [9, 10].

Since the civilian signal systems of navigation signals are open, its terminals are very vulnerable to spoofing and jamming. Spoofing and jamming means that the spoofing party enters the acquisition and tracking loop of the GNSS receiver by forging false signals with the same structure as the real satellite signal but different positioning or timing information or forwarding the real satellite navigation signal, so that the navigation user terminal can solve the wrong Positioning, Navigation and Timing (PNT) information, thus not working properly [11, 12]. Spoofing interference is mainly divided into: generative spoofing and forwarding spoofing. Among them, the message and spreading code of the civil code are public, and the deceiver can easily forge the navigation signal. Therefore, the research on the suppression of forwarding spoofing is particularly important.

Research on spoofing is also widely carried out, among which spoofing detection and single-antenna spoofing suppression are the main ones. The methods of spoofing detection are signal quality monitoring [13, 14], parameter estimation [15], automatic gain control [16], residual vector analysis method [17], correlating antenna motion and carrier phase [18, 19], mobile internet detection [20] and correlating carrier phase with rapid antenna motion [21]. Spoofing inhibition is

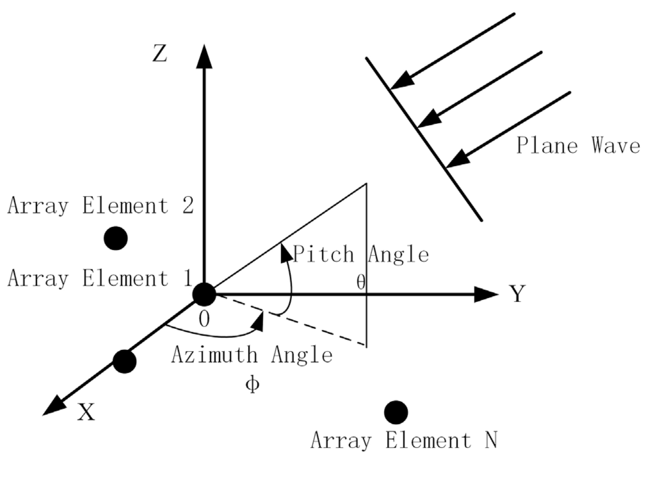

FIGURE 1 | Schematic diagram of antenna array and incident signal.

mainly based on single-antenna and Receiver Autonomous Integrity Monitoring (RAIM) processing: Lu Mingquan's team of Tsinghua University proposed iterative RAIM and cooperative RAIM algorithms to detect and suppress forwarding spoofing interference [22]. [23] proposed a spoofing suppression method using pseudorange and carrier phase [24]. proposed a jamming suppression method based on estimating spoofing signal steering vector, which eliminated the spoofing signal by constructing an orthogonal projection matrix based on spoofing jamming, but its estimation accuracy was poor, which would affect its suppression effect [25]. proposed an anti-spoofing jamming method based on improved RAIM, which uses an iterative algorithm to detect and eliminate the meaning of suspected spoofing satellites, and achieve spoofing suppression at the signal layer. However, the iterative algorithm is computationally intensive, and cannot suppress the spoofing of multiple satellites being forwarded at the same time. In contrast, there are in-depth studies on the suppression of jamming at present [26], analyzed the performance of adaptive space-time array in anti-jamming processing [27], proposed the use of multi-level nested Wiener filters (MSNWF) to suppress narrowband interference [28], analyzed in detail the performance of using the power inversion algorithm to suppress jamming. Team from National University of Defense Technology designed a variety of anti-jamming algorithms through delay constraints [29, 30] and array element constraints [31–33], respectively, without reducing the anti-jamming performance, effectively improving the accuracy of pseudo-range measurements [34]. proposed a new algorithm for adaptive notch filtering and parametric spectral estimation of multiple narrowband or sinusoidal signals in an additive broadband process [35, 36]. designed anti-jamming algorithms from the temporal and spatial domains, respectively, to further improve the convergence speed.

As can be seen from the above, the current methods of spoofing suppression are still relatively based on single-antenna, array processing is rarely used, and they all have certain limitations. This paper proposes a multi-satellite and multi-channel array processing GNSS spoofing signal suppression algorithm. By estimating and weighting the angle of arrival (AOA) of the multi-satellite spoofing signal, the estimation accuracy of the AOA of the spoofing signal is improved, and then the spoofing signal is suppressed in the airspace by the orthogonal subspace method. The main structure of this paper is as follows: In the second section, the model of the antenna array receiving spoofed signals is introduced; In the third section, the error of estimating the arrival angle of only one satellite and its influence on the real signal carrier-to-noise ratio (CNR) are analyzed; In the fourth section, proposes a multi-satellite fusion AOA estimation spoofing suppression algorithm, and the algorithm is verified by simulation, and finally the full text is summarized.

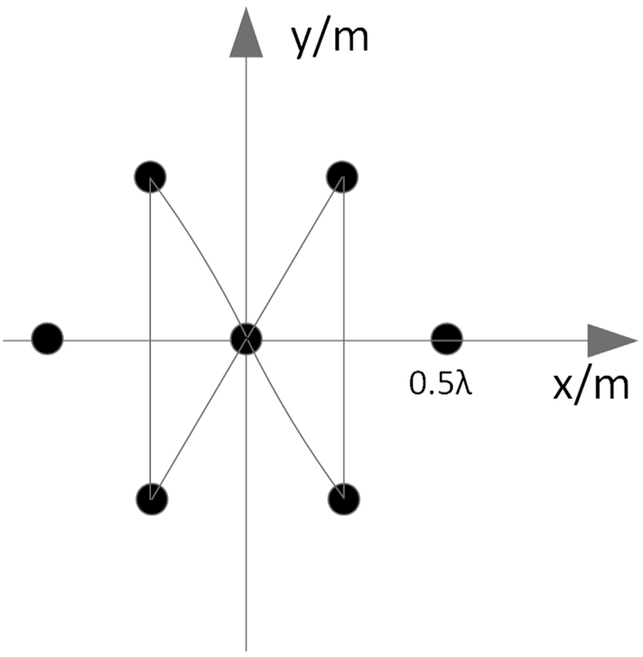

FIGURE 2 | Schematic diagram of the arrangement of antenna array elements.

2 SIGNAL MODEL

It is assumed that the receiving antenna array of the navigation receiver is composed of N ideal omnidirectional array elements, as shown in **Figure 1**. The antenna array used in this paper is set as shown in **Figure 2**.

K navigation signals and L spoofing signals are incident on the antenna array as plane waves from the space far field, then the complex baseband form of the signal received by the navigation receiver antenna array can be expressed as:

$$\boldsymbol{x}(t) = \sum_{k=1}^{K} \boldsymbol{\alpha}_k s_k(t) + \sum_{l=1}^{L} \boldsymbol{\beta}_l j_l(t) + \boldsymbol{n}(t) \tag{1}$$

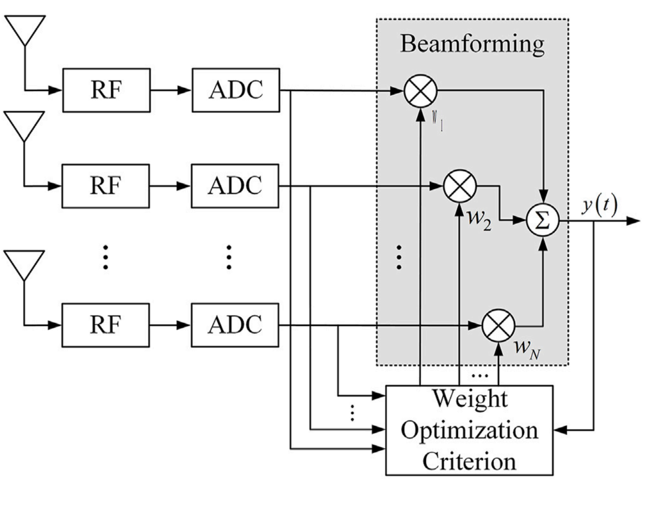

FIGURE 3 | Schematic diagram of antenna array spatial filtering.

where, $\boldsymbol{n}(t)$ is the noise vector, it consists of the noise of each array element channel $n_i(t)$ (i = 1,2, . . . ,N), the variance of each noise component is σ_n^2 , mean is 0, and is IID Gaussian white noise, $\boldsymbol{x}(t) = [x_1(t), x_2(t), \ldots, x_N(t)]^T$ is the N-dimensional signal vector, each row corresponds to the mixed signal received by an array element, $[\cdot]^T$ means transpose. $s_k(t) j_l(t)$ are the k th satellite signal and the l th spoofing signal received at the reference array element. $\boldsymbol{\alpha}_k \boldsymbol{\beta}_l$ are the steering vectors of the real signal and the spoofed signal, respectively. It contains all the spatial information of the received signal of the antenna array, and the expression is:

$$\boldsymbol{\alpha}_k = \begin{bmatrix} e^{j\left(2\pi \boldsymbol{p}_1 \boldsymbol{e}(\theta_k,\phi_k)/\lambda\right)} \\ e^{j\left(2\pi \boldsymbol{p}_2 \boldsymbol{e}(\theta_k,\phi_k)/\lambda\right)} \\ \vdots \\ e^{j\left(2\pi \boldsymbol{p}_N \boldsymbol{e}(\theta_k,\phi_k)/\lambda\right)} \end{bmatrix}, k = 1, 2, \ldots L \tag{2}$$

In the formula, $\boldsymbol{e}(\theta_k, \phi_k) = [\cos\theta_k \cos\phi_k, \cos\theta_k \sin\phi_k, \sin\phi_k]^T$ is the unit propagation vector of the plane wave, θ_k is the pitch angle of the incident signal, ϕ_k is the azimuth angle of the incident signal, λ is the signal wavelength, p_n (n = 1,2, . . . N) is the position coordinate of the n th array element. An important property of the steering vector is:

$$\boldsymbol{\alpha}_k^H \boldsymbol{\alpha}_k = N \tag{3}$$

where $(\cdot)^H$ represents the conjugate transpose operation.

The antenna array can use the spatial characteristics of the signal to filter the signal in the space-time field through weighting algorithms of different criteria. Among them, pure spatial filtering is the most basic method in array signal processing. **Figure 3** shows the schematic diagram of antenna array spatial processing.

Each channel of the array input signal is multiplied by the weights (n = 1, 2... N) generated under a specific criterion, and then summed, and finally the array output signal is obtained, which is in the form:

$$y(t) = \sum_n^N \mathrm{w}_n^* x_n(t) = \boldsymbol{w}^H \boldsymbol{x}(t) \tag{4}$$

In the formula, $(\cdot)^*$ represents the conjugate of complex numbers, $\boldsymbol{w} = [w_1, w_2, \ldots w_N]^T$ is the weight vector, and each row corresponds to the weight of an array element.

3 SPOOFING SUPPRESSION FOR SINGLE-SATELLITE

In general, the energy of forwarding spoofing is greater than the real signal. Therefore, if the antenna array does not take anti-spoofing measures, the receiver will capture and track the spoofing signal and solve the message. Taking advantage of this feature, a single-satellite AOA estimation spoofing suppression algorithm is designed, and the algorithm processing flow is shown in **Figure 4**.

The algorithm consists of three parts. The first is to reconstruct the spoofing signal for maximum likelihood estimation of the angle of arrival, which includes the spoofing detection link. The current satellite position is calculated from the message information of the received signal, and the angle of arrival is calculated and compared with the estimated value., if the deviation is too large, it is considered to be spoofing. By default, the detection and identification of the spoofing signal has been completed, so it will not be described in detail. Then, an orthogonal subspace is constructed according to the estimated angle of arrival of the spoofing signal, and the weights of the antenna array are generated to suppress the spoofing signal. The principle of maximum likelihood estimation of spoofing signals and the orthogonal subspace are introduced below, and the estimation performance and the influence of estimation error on spoofing suppression are analyzed.

3.1 Theoretical Analysis

3.1.1 Maximum Likelihood Estimation

Only considering when L signals are incident to the antenna array from the far field in the form of plane waves, **Eq. 1** can be transformed into:

$$\begin{aligned} \boldsymbol{x}(t) &= \sum_{l=1}^{L} \boldsymbol{a}_l s_l(t) + \boldsymbol{n}(t) \\ &= \boldsymbol{A}(\boldsymbol{\Theta}) \boldsymbol{s}\ t + \boldsymbol{n}\ t \end{aligned} \tag{5}$$

The noise is independent and identically distributed, and its autocorrelation matrix is $\boldsymbol{R}_n = E[\boldsymbol{n}(t)\boldsymbol{n}^H(t)] = \sigma_n^2 \boldsymbol{I}$.

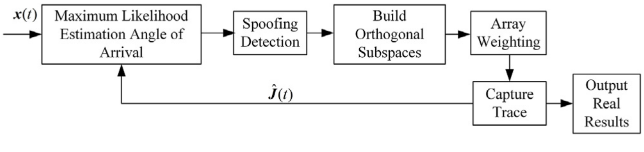

FIGURE 4 | Algorithm processing block diagram.

$$\boldsymbol{A}(\boldsymbol{\Theta}) = \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_L \tag{6}$$

$$\boldsymbol{\Theta} = [\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, \ldots, \boldsymbol{\theta}_L] \tag{7}$$

$$\boldsymbol{\theta}_l = (\theta_l, \phi_l) \tag{8}$$

$\boldsymbol{A}(\boldsymbol{\Theta})$ is the $N \times L$ dimensional steering vector matrix. $\boldsymbol{\theta}_l$ is the combined vector of the lth signal pitch angle θ_l and azimuth angle ϕ_l.

The l-th signal $s_l(t)$ can be written as:

$$s_l(t) = \gamma_l y_l(t) \tag{9}$$

where, $y_l(t)$ represents the waveform of a known signal, γ_l represents the amplitude of the signal, written in matrix form as:

$$\boldsymbol{s}(t) = \boldsymbol{\Gamma}\boldsymbol{y}(t) \tag{10}$$

where, $\boldsymbol{y}(t) = [y_1(t), y_2(t), \ldots, y_L(t)]^T$, $\boldsymbol{\Gamma} = diag[\gamma_1, \gamma_2, \ldots, \gamma_L]$, $diag$ () represents a diagonal matrix.

The signal received by the antenna array can be expressed as:

$$\mathbf{x}(t) = \mathbf{A}(\mathbf{\Theta})\boldsymbol{\Gamma}\boldsymbol{y}(t) + \boldsymbol{n}(t) \tag{11}$$

When the waveform of the signal is known, the negative log-likelihood of the array output vector is:

$$L(\Theta, \gamma, \boldsymbol{R}_n) = \ln|\boldsymbol{R}_n| + tr\left\{\boldsymbol{R}_n^{-1}\frac{1}{m}\sum_{i=1}^{m}[x(t_i) - \boldsymbol{B}\boldsymbol{y}(t_i)][x(t_i) - \boldsymbol{B}\boldsymbol{y}(t_i)]^H\right\} \tag{12}$$

where, m is the number of snapshots in the airspace, $\boldsymbol{B} = \boldsymbol{A}(\mathbf{\Theta})\mathbf{\Gamma}$, $|\cdot|$ represents the determinant of a matrix, when solving the likelihood function, $\boldsymbol{R}_n$ is estimated to be:

$$\hat{\boldsymbol{R}}_n = \frac{1}{m}\sum_{i=1}^{m}\left[\boldsymbol{x}(t_i) - \hat{\boldsymbol{B}}\boldsymbol{y}(t_i)\right]\left[\boldsymbol{x}(t_i) - \hat{\boldsymbol{B}}\boldsymbol{y}(t_i)\right]^H \tag{13}$$

Then the estimated likelihood function for the angle of arrival of a single signal is

$$\mathrm{LLR} = \sum_{i=1}^{m}[\boldsymbol{x}(t_i) - \boldsymbol{a}_l\gamma_l y_l(t_i)]^H \boldsymbol{R}_n^{-1}[\boldsymbol{x}(t_i) - \boldsymbol{a}_l\gamma_l y_l(t_i)] \tag{14}$$

During the solution process, $\boldsymbol{R}_n$ is estimated by the following formula:

$$\boldsymbol{R}_n = \hat{\boldsymbol{R}}_{xx} - \hat{\boldsymbol{R}}_{sx}^{*} R_{ss}^{-1}\hat{\boldsymbol{R}}_{sx} \tag{15}$$

where,

$$\hat{\boldsymbol{R}}_{sx} = \frac{1}{m}\sum_{i=1}^{m}\hat{s}_l(t_i)\boldsymbol{x}^H(t_i) \tag{16}$$

$$\hat{\boldsymbol{R}}_{xx} = \frac{1}{m}\sum_{i=1}^{m}\boldsymbol{x}(t_i)\boldsymbol{x}^H(t_i) \tag{17}$$

$$\hat{\boldsymbol{R}}_{ss} = \frac{1}{m}\sum_{i=1}^{m}\hat{s}_l(t_i)\hat{s}_l^H(t_i) \tag{18}$$

According to the above likelihood function, for the estimation of the angle of arrival of a single satellite, we rearrange the Nm sampled data into an m*N dimensional array, and project the estimated l th spoofing signal $\hat{\boldsymbol{s}}_l$ to the sampled data space to obtain the following expression:

$$\boldsymbol{b}_l = \frac{\boldsymbol{X}\hat{\boldsymbol{s}}_l^H}{\varepsilon_l} \tag{19}$$

$$\hat{\boldsymbol{s}}_l = [\hat{s}_l(t_1), \hat{s}_l(t_2), \ldots, \hat{s}_l(t_m)] \tag{20}$$

$$\boldsymbol{X} = [\boldsymbol{x}(t_1), \boldsymbol{x}(t_2), \ldots, \boldsymbol{x}(t_m)] \tag{21}$$

$$\varepsilon_l = \hat{\boldsymbol{s}}_l\hat{\boldsymbol{s}}_l^H = \sum_{i=1}^{m}\hat{\boldsymbol{s}}_l(t_i)\hat{\boldsymbol{s}}_l^H(t_i) \tag{22}$$

Then the estimated value of the angle of arrival of the signal is as follows:

$$\hat{\boldsymbol{\theta}}_l = \max_{\theta_l}\frac{\left|\boldsymbol{a}_l^H\boldsymbol{R}_n^{-1}\boldsymbol{b}_l\right|}{\boldsymbol{a}_l^H\boldsymbol{R}_n^{-1}\boldsymbol{a}_l} \quad l = 1, \ldots, L \tag{23}$$

So far, the angle of arrival of each signal can be estimated according to **Eq. 23**.

3.1.2 Orthogonal Subspace Spoofing Suppression Principle

When using the maximum likelihood method to estimate the AOA of the spoofing, the waveform of the spoofing signal $y_l(t)$ needs to be known. Using the publicly known properties of the satellite signal waveform, the receiver can capture and track the spoofing signal, and then the doppler and pseudocode phase parameters of the spoofing signal can be obtained, and the spoofing signal can be reconstructed according to the format of the navigation signal as:

$$\hat{s}_l(t_i) = \gamma' y'_l(t_i) \quad i = 1, 2, \ldots, m \tag{24}$$

where, γ' is the estimated signal amplitude based on the carrier-to-noise ratio calculated by the receiver, $y'_l(t_i)$ is the waveform of the reconstructed spoofing signal. AOA estimation needs to be processed for the forwarded satellite spoofing signals of different PRN numbers, and **formula (24)** is brought into **formula (14)**, and the AOA information of each spoofing signal can be obtained after calculation.

Assuming that the repeating signals all come from the same repeating spoofing device, multiple satellite signals are delayed and forwarded. In this scenario, all spoofed signals have the same origin. After obtaining the angle of arrival information of the spoofing signal, substitute $\hat{\boldsymbol{\theta}} = (\theta, \phi)$ into the steering vector calculation formula to obtain the steering vector of the spoofing signal as:

$$\boldsymbol{\beta} = \begin{bmatrix} e^{j\left(2\pi\boldsymbol{p}_1\boldsymbol{e}(\theta,\phi)/\lambda\right)} \\ e^{j\left(2\pi\boldsymbol{p}_2\boldsymbol{e}(\theta,\phi)/\lambda\right)} \\ \vdots \\ e^{j\left(2\pi\boldsymbol{p}_N\boldsymbol{e}(\theta,\phi)/\lambda\right)} \end{bmatrix} \tag{25}$$

Then the orthogonal subspace of the spoofing signal can be constructed:

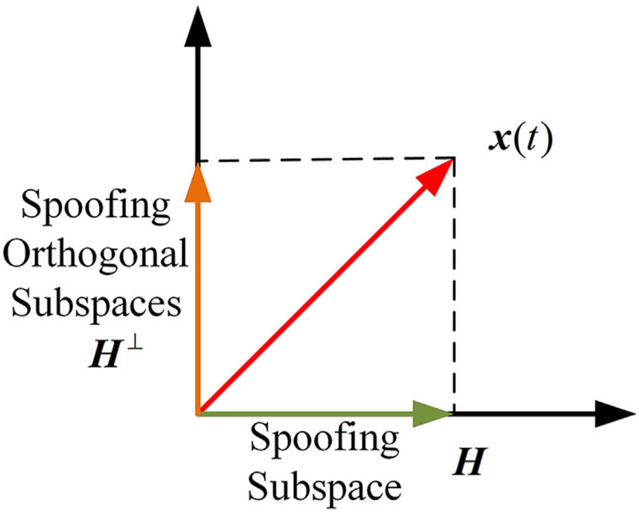

FIGURE 5 | Schematic diagram of the principle of subspace projection.

$$\boldsymbol{H}^{\perp} = \boldsymbol{I} - \boldsymbol{\beta}\left(\boldsymbol{\beta}^{H}\boldsymbol{\beta}\right)^{-1}\boldsymbol{\beta}^{H} \tag{26}$$

$$\begin{aligned}\boldsymbol{H}^{\perp}\boldsymbol{\beta} &= \left(\boldsymbol{I} - \boldsymbol{\beta}\left(\boldsymbol{\beta}^{H}\boldsymbol{\beta}\right)^{-1}\boldsymbol{\beta}^{H}\right)\boldsymbol{\beta} \\ &= \boldsymbol{\beta} - \boldsymbol{\beta}\left(\boldsymbol{\beta}^{H}\boldsymbol{\beta}\right)^{-1}\boldsymbol{\beta}^{H}\boldsymbol{\beta} \\ &= \boldsymbol{0}\end{aligned} \tag{27}$$

The interference can be suppressed by projecting the array signal to the spoofed orthogonal subspace. The principle is shown in **Figure 5**.

The array output signal after projection is:

$$\begin{aligned}\boldsymbol{x}'(t) &= \boldsymbol{H}^{\perp}\boldsymbol{x}(t) \\ &= \boldsymbol{H}^{\perp}\left(\sum_{k=1}^{K}\boldsymbol{\alpha}_k s_k(t) + \boldsymbol{\beta}\sum_{l=1}^{L} j_l(t) + \boldsymbol{n}(t)\right) \\ &= \boldsymbol{H}^{\perp}\sum_{k=1}^{K}\boldsymbol{\alpha}_k s_k(t) + \boldsymbol{H}^{\perp}\boldsymbol{n}(t)\end{aligned} \tag{28}$$

Therefore, it is only necessary to set the weight of the antenna array to a column in the orthogonal subspace which is not all zeros after normalization, that is, the spoofing can be eliminated from the airspace.

3.2 Influence of Estimation Accuracy on Real Signal Carrier-To-Noise Ratio

The maximum likelihood estimation algorithm is used to estimate the AOA of a single spoofing signal, and the Cramér–Rao bound theory formula of the estimated variance is:

$$\mathrm{CRB}(\boldsymbol{\theta}_l) = \frac{\left|\breve{\boldsymbol{a}}_l^{H}\breve{\boldsymbol{a}}_l\right|}{2m\sigma_l^2\breve{\boldsymbol{d}}_l^{H}\boldsymbol{P}_{\breve{\boldsymbol{a}}_l}^{\perp}\breve{\boldsymbol{d}}_l} \quad l = 1, \ldots, L \tag{29}$$

where, σ_l^2 is the power of the l th spoofing signal, and

$$\breve{\boldsymbol{a}}_l = R_n^{-1/2}\boldsymbol{a}_l \tag{30}$$

TABLE 1 | Simulation parameter settings.

Parameter	Value
Number of different real satellite signals	1–6
Number of different satellite spoofs	1–6
AOA of spoofing signal (azimuth, pitch)	(60°, 35°)
spoofed signal carrier-to-noise ratio	–60 dBHz
Forward Spoofing Delay	1 chip
Power Spectral Density of Noise	–205 dBW/Hz
receiver bandwidth	20 MHz
Sampling Rate	20.48 MHz
number of snapshots	204,800
Monte Carlo times	1000

$$\breve{\boldsymbol{d}}_l = R_n^{-1/2}\boldsymbol{d}_l \tag{31}$$

$$\boldsymbol{d}_l = \frac{\partial \boldsymbol{a}_l}{\partial \boldsymbol{\theta}_l} \tag{32}$$

$$\boldsymbol{P}_{\breve{\boldsymbol{a}}_l}^{\perp} = \boldsymbol{I} - \boldsymbol{P}_{\breve{\boldsymbol{a}}_l} \tag{33}$$

$$\boldsymbol{P}_{\breve{\boldsymbol{a}}_l} = \breve{\boldsymbol{a}}_l\left(\breve{\boldsymbol{a}}_l^{H}\breve{\boldsymbol{a}}_l\right)^{-1}\breve{\boldsymbol{a}}_l^{H} \tag{34}$$

When using the maximum likelihood estimation algorithm to estimate the AOA of a spoofing signal, it is necessary to pay attention to its estimation accuracy under different power levels of the spoofed signal or the level of the carrier-to-noise ratio. In this section, the estimation accuracy of maximum likelihood estimation for the AOA of a single spoofed signal is simulated, as well as the Cramér–Rao bound at the current CNR of the spoofed signal.

According to the array structure shown in **Figure 2**, the specific setting parameters of the simulation scene are shown in **Table 1**.

Figure 6 respectively show the changes of the azimuth and pitch variances of the maximum likelihood estimation and the corresponding Cramér–Rao bounds as the spoofing signal CNR gradually increases from 36 dBHz to 63 dBHz.

As can be seen from **Figure 6**, when the carrier-to-noise ratio of the spoofed signal is low, the estimation accuracy of the azimuth and pitch angles is very poor. It can be seen that when the spoofing signal carrier-to-noise ratio is 36 dBHz, the estimated error of the azimuth angle reaches 5°, and the estimated error of the pitch angle is nearly 10°, while at 58 dBHz, the estimated error is close to 0.

The error of the AOA estimation will make the generated subspace not completely orthogonal to the spoofed signal, which will affect the suppression of the spoofed signal and cause the real signal to be suppressed as well. In order to analyze the influence of error on spoofing suppression and real signal, the following simulation analyzes the influence of the error of estimated azimuth and pitch angle on the real signal and spoofing signal output carrier-to-noise ratio after projection subspace processing. In this paper, only one real signal is considered, and its arrival pitch angle and azimuth angle are (70°, 100°), and the specific parameter settings are shown in **Table 2**.

The effect results are shown in **Figure 7**.

As can be seen from **Figure 7A**, when the estimation error of the AOA of the spoofed signal is large, the carrier-to-noise ratio of the

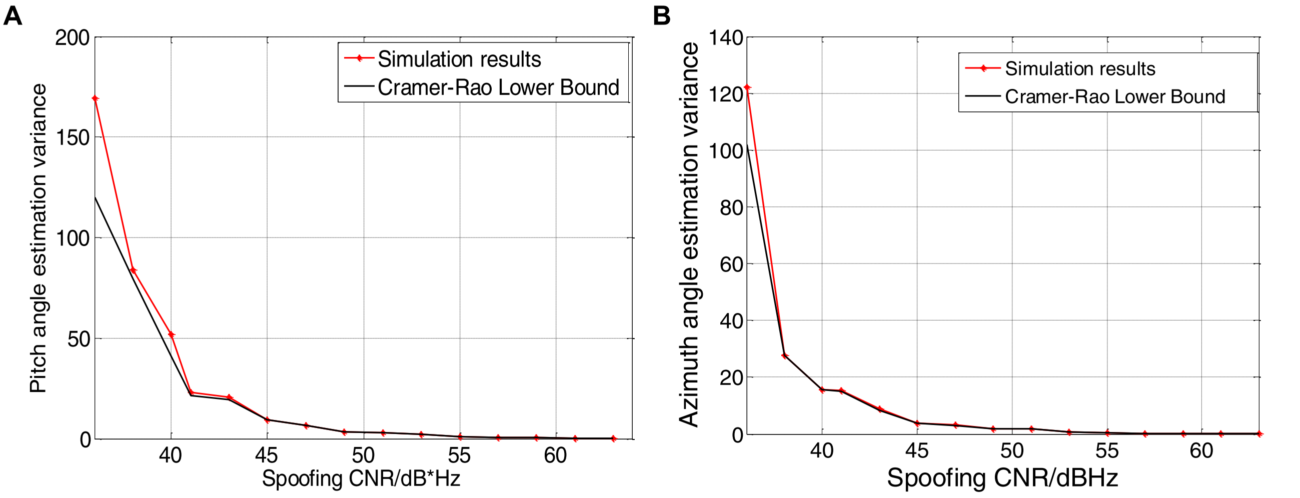

FIGURE 6 | Angle of arriver estimation error. Result of pitch angle is shown in figure **(A)**, and result of. azimuth angle is shown in figure **(B)**.

TABLE 2 | Parameter setting of real and spoofing signals.

Parameter	Value
AOA of real signal (azimuth, pitch)	(100°, 70°)
AOA of spoofing signal (azimuth, pitch)	(60°, 35°)
CNR of real signal	42 dBHz
CNR of spoofing signal	47 dBHz
Pitch deviation of spoofing	±15°
Azimuth deviation of spoofing	±20°
Forward Spoofing Delay	1chip
Power Spectral Density of Noise	−205 dBW/Hz
receiver bandwidth	20 MHz
Sampling Rate	20.48 MHz
Number of snapshots	204,800
Monte Carlo times	1000

real signal will fluctuate accordingly. When the estimation error makes the arrival angle of the spoofed signal far away from the true signal azimuth, it will affect its carrier-to-noise ratio by about 2dB. When the estimation error makes the spoofed signal's arrival angle close to the true signal azimuth, it will cause more than 10dB of attenuation to the carrier-to-noise ratio. As can be seen from **Figure 7B**, when the estimation error is large, the carrier-to-noise ratio of the spoofing signal suppressed by the orthogonal subspace algorithm will fluctuate greatly. When accurately estimated, the carrier-to-noise ratio tends to be infinitely small; when the azimuth angle deviation is 25° and the pitch angle deviation is 15°, the carrier-to-noise ratio is about 30 dBHz.

Through the above simulation and analysis, the estimation error of the angle of arrival of the spoofing signal will have a

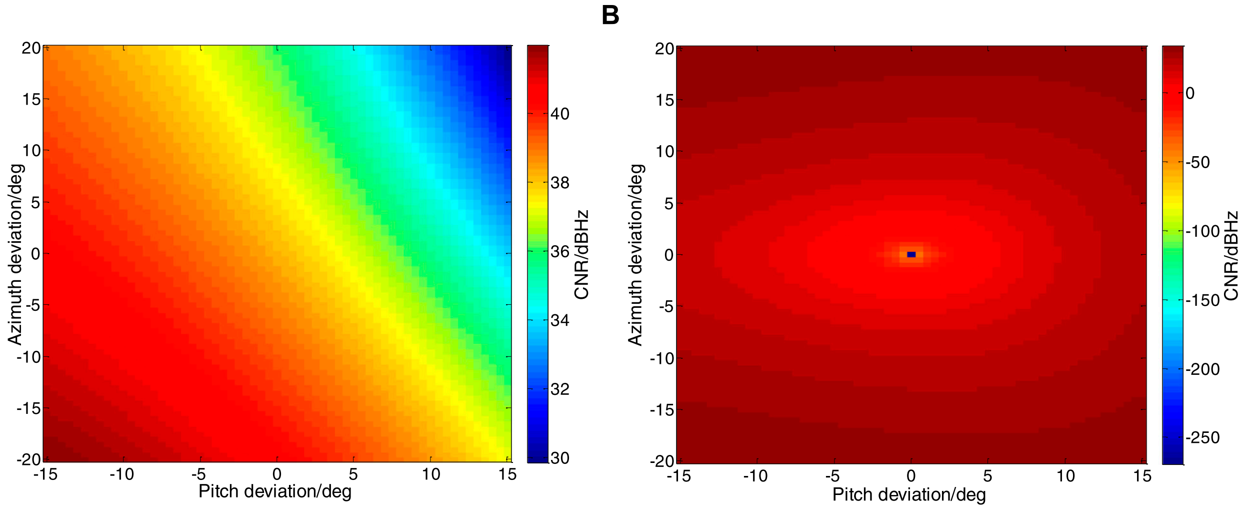

FIGURE 7 | Effect of Arrival Angle Estimation Error on Signal Carrier-to-Noise Ratio. Real signal is. shown in figure **(A)**, and spoofing signal is shown in figure **(B)**.

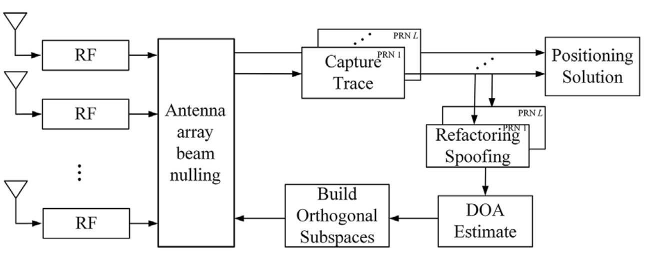

FIGURE 8 | Schematic diagram of the algorithm structure.

TABLE 3 | Parameter setting of spoofing signal.

Parameter	Value
Number of different satellite spoofs	1–6
AOA of spoofing signal (azimuth, pitch)	(60°, 35°)
CNR of spoofing signal	36–62 dBHz
Forward Spoofing Delay	1 chip
Power Spectral Density of Noise	−205 dBW/Hz
Receiver Bandwidth	20 MHz
Sampling Rate	20.48 MHz
number of snapshots	204,800
Monte Carlo times	1000

great impact on the performance of the receiver's spoofing suppression, which will make the suppression of the spoofing signal worse, and cause greater attenuation of the real signal power, so that the receiver cannot normally capture and track the real signal. As a result, the normal positioning solution cannot be performed.

4 MULTI-SATELLITE FUSION AOA ESTIMATION SPOOFING SUPPRESSION ALGORITHM

It can be seen from the above analysis that the error of AOA estimation for the spoofed signal will attenuate the power of the real signal. For satellite navigation systems, the power of the real signal is very weak, and this effect will make the receiver unable to capture the real signal. lose the ability to work properly, in response to this problem, this section proposes a multi-satellite fusion AOA estimation spoofing suppression algorithm, which estimates the AOA values of all current spoofing signals, according to the estimated variance corresponding to the carrier-to-noise ratio of each spoofing signal, the azimuth angle and the pitch angle are weighted respectively, which greatly improves the accuracy of the AOA estimation of the spoofing signal. Then the orthogonal subspace projection algorithm is used to suppress the spoofing. The algorithm processing flow is shown in **Figure 8**.

Assuming that the number of satellites to be forwarded is L, the detailed processing steps of the algorithm are as follows:

1) The *N* array elements of the antenna array respectively receive the mixed signal containing the forwarding spoofing signal and the real signal, and obtain the intermediate frequency signal through the processing of the RF front-end;
2) The receiver captures and tracks the spoofed signal corresponding to each PRN number, reconstructs the local replica signal according to the pseudocode phase information output by the tracking loop, and estimates the carrier-to-noise ratio of each spoofed signal;
3) Using the reconstructed local replica signal, perform maximum likelihood estimation on the spoofing signal according to the method in **Section 3 1**, and obtain arrival angle information;

TABLE 4 | Carrier-to-noise ratio settings.

PRN number	CNR (dBHz)
2	P_1+4
3	P_1+2
4	P_1-2
5	P_1-4
6	P_1

4) Calculate the estimated variance of the azimuth and elevation angles under the current carrier-to-noise ratio of the spoofed signal, and weight the azimuth and elevation angles with the variance basis respectively according to the principle of unequal precision weighting to achieve accurate estimation of the AOA of the spoofing;
5) Bring the weighted AOA value into **Eq. 29**, and use the orthogonal subspace algorithm to generate the antenna array weight to suppress deception.

4.1 AOA Estimation Fusion Weighting Algorithm

From the analysis in the previous section, it can be seen that for different carrier-to-noise ratios of spoofing signals, the accuracy of the maximum likelihood estimation of the AOA is also different. In order to improve the accuracy of the AOA estimation, this paper introduces the AOA estimation method of multi-satellite fusion weighting, the essence of which is to deal with the problem of unequal precision measurement.

In unequal precision measurement, each measurement result is obtained under different measurement conditions. The measurement conditions include: the measurement method, the instruments used in the measurement, the measurement personnel, the environmental conditions, and the measurement times when each result is obtained, etc. The difference in the accuracy of the measurement results is the result of the combined effect of these factors. Since the accuracy of each measurement result is not equal, the degree of trust in them is also different, which involves a so-called weight problem. The so-called weight is the quantitative performance of the relative reliability of each measurement result. For the content of this chapter, the different measurement conditions are the

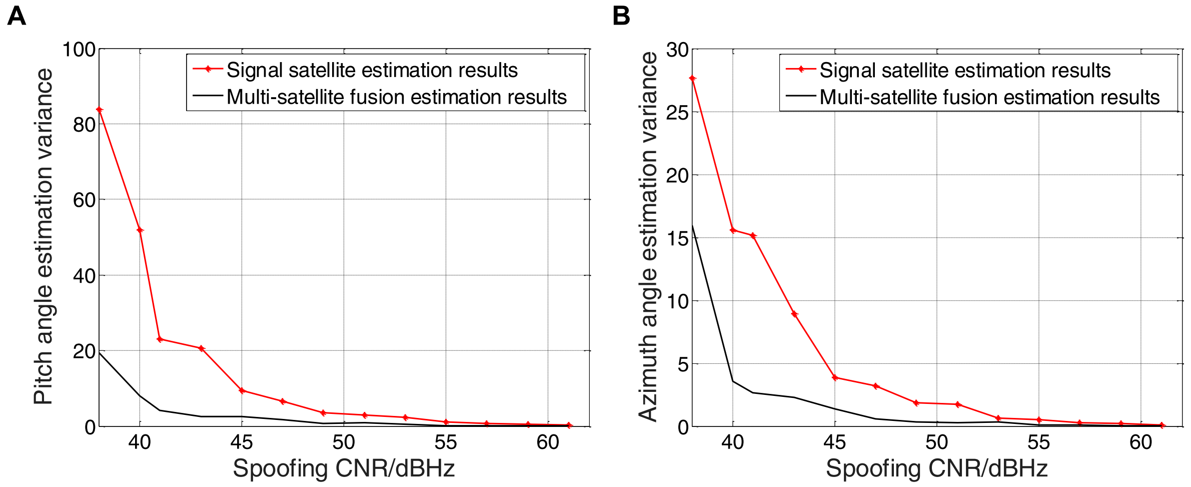

FIGURE 9 | Angle of arriver estimation error. Result of pitch angle is shown in figure **(A)**, and result of azimuth angle is shown in figure **(B)**.

carrier-to-noise ratio of each spoofing signal, since the carrier-to-noise ratio of each satellite of the real signal reaching the receiving antenna of the transponder is different, after amplification and forwarding, the carrier-to-noise ratio of each satellite in the spoofed signal is also different. This causes the maximum likelihood to estimate the AOA of each satellite with different accuracy.

Assuming that the number of satellites to be relayed is L, the maximum likelihood estimates the pitch θ_l and azimuth ϕ_l corresponding to each satellite. Estimate the power value of each signal $\sigma_1, \sigma_2, \ldots, \sigma_L$, and then bring it into **Eq. 29** respectively, calculate the estimated variance of the pitch angle $\sigma^2_{\theta_l}$ and the estimated variance of the azimuth angle $\sigma^2_{\phi_l}$, and weight the azimuth angle and the pitch angle respectively, which is:

$$w_{\phi_1}\colon w_{\phi_2}\colon \ \ldots\colon w_{\phi_L} = \sigma^{-2}_{\phi_1}\colon \sigma^{-2}_{\phi_2}\colon \ \ldots\colon \sigma^{-2}_{\phi_L} \tag{35}$$

$$w_{\theta_1}\colon w_{\theta_2}\colon \ \ldots\colon w_{\theta_L} = \sigma^{-2}_{\theta_1}\colon \sigma^{-2}_{\theta_2}\colon \ \ldots\colon \sigma^{-2}_{\theta_L} \tag{36}$$

From the above formula, the weighted pitch angle $\tilde{\theta}$ and azimuth angle $\tilde{\phi}$ are expressed as:

$$\tilde{\theta} = \frac{1}{\sigma^{-2}_{\theta_1} + \sigma^{-2}_{\theta_2} + \ldots + \sigma^{-2}_{\theta_L}} \left(\frac{\theta_1}{\sigma^2_{\theta_1}} + \frac{\theta_2}{\sigma^2_{\theta_2}} + \ldots + \frac{\theta_L}{\sigma^2_{\theta_L}} \right) \tag{37}$$

$$\tilde{\phi} = \frac{1}{\sigma^{-2}_{\phi_1} + \sigma^{-2}_{\phi_2} + \ldots + \sigma^{-2}_{\phi_L}} \left(\frac{\phi_1}{\sigma^2_{\phi_1}} + \frac{\phi_2}{\sigma^2_{\phi_2}} + \ldots + \frac{\phi_L}{\sigma^2_{\phi_L}} \right) \tag{38}$$

In order to analyze the estimation accuracy under the algorithm, in this section, the estimation accuracy of the angle of arrival of the spoofing signal after the weighting of the algorithm is simulated, and compared with the estimation error of a single satellite.

Set the simulation scene as shown in **Table 3**, the antenna array is the 7-element center circular array shown in **Figure 2**.

TABLE 5 | Real satellite signal parameter settings.

PRN number	AOA	CNR (dBHz)	Code phase (chip)
1	(70°, 140°)	45	20
2	(92°, 118°)	43	12
3	(60°, 279°)	41	10
4	(78°, 148°)	47	1
5	(70°, 100°)	49	4
6	(87°, 172°)	45	10

Assuming that the carrier-to-noise ratio with the PRN number one of the forwarding spoofing is P_1, the remaining five satellite CNR settings are shown in **Table 4**.

The single-satellite estimation in the simulation process only estimates the satellite whose PRN number is 1, so the carrier-to-noise ratio of the abscissa corresponds to P_1, The carrier-to-noise ratio of the abscissa of the multi-satellite fusion estimation is the largest carrier-to-noise ratio among all the forwarding satellites, which is equivalent to comparing the multi-satellite fusion estimation with only the spoofing signal with the highest carrier-to-noise ratio. **Figure 9** show that as the CNR of the spoofed signal gradually increases from 36 dBHz to 61 dBHz, changes in azimuth and pitch variance for maximum likelihood estimates.

It can be clearly seen from **Figure 9** that the estimation accuracy is improved by 80% when the CNR is 50 dBHz, the estimation accuracy under multi-satellite fusion has been greatly improved compared with that of single-satellite estimation.

4.2 Algorithm Simulation

In order to verify the simulation performance of the algorithm for spoofing suppression, the following simulations are carried out. The simulation conditions are: the real signal PRN numbers are one to six, and the values of the AOA, carrier-to-noise ratio and code phase are shown in **Table 5**.

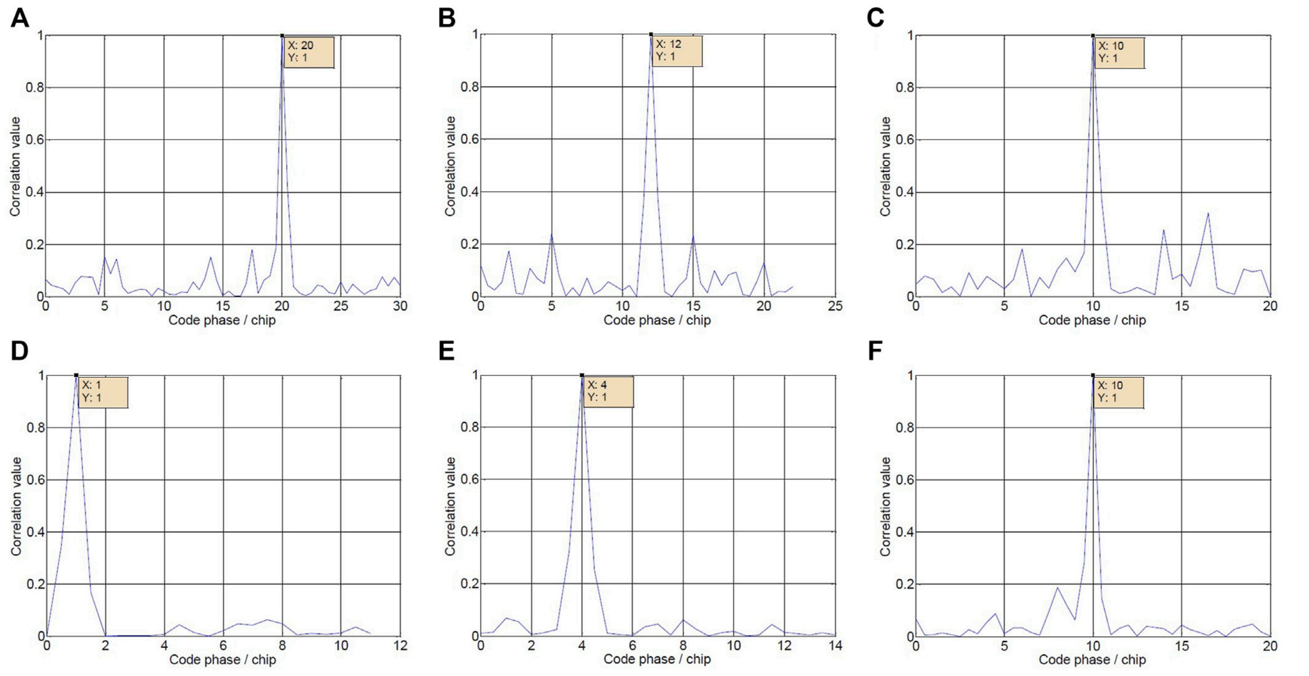

FIGURE 10 | Code Phase Results. The captured results of PRN one to six satellites signal after algorithm processing are shown in figures **(A–D)**.

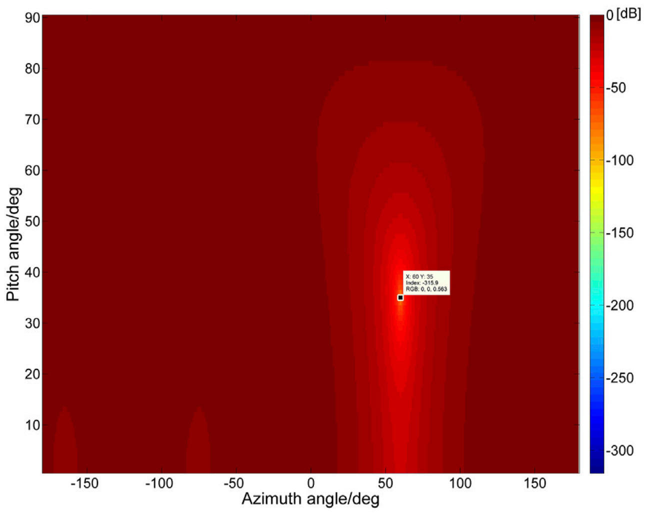

FIGURE 11 | The beam pattern of the antenna array.

The real navigation signal and the forwarding spoofing signal with a set delay of one chip and a spoofing-to-signal ratio of 10 dB are simulated. The forwarded signals all come from one direction (60°, 35°). The spoofing suppression algorithm is used to process the signal, and the software receiver is used to capture and process the processed signal to obtain the code phase of the output signal and the beam pattern of the antenna array to test the effect of the algorithm to suppress spoofing.

First, the code phase information captured by the software receiver is given, as shown in **Figure 10**.

As can be seen from **Figure 10**, after the signal processed by the algorithm is captured by the software receiver, its code phase is the code phase of the real satellite, which verifies the effectiveness of deception suppression.

The beam pattern of the antenna array at this time is shown in **Figure 11**.

It can be seen that the antenna array accurately forms a 315.9dB null in the direction of the spoofing signal, which completely suppresses the spoofing signal. Analysis proves that the algorithm can accurately estimate the angle of arrival of forwarding spoofing, and can effectively suppress spoofing.

5 CONCLUSION

For the suppression of forwarding spoofing interference, this research proposed a multi-satellite and multi-channel array processing GNSS spoofing signal suppression algorithm. Firstly, the maximum likelihood estimation method is used to estimate the AOA of the current spoofing signals of all satellites, the estimated azimuth and pitch angles of each satellite are weighted and summed according to the estimated variance corresponding to the carrier-to-noise ratio of the spoofed signal, which improves the estimation accuracy of the AOA of the spoofed signal and reduces the impact on the CNR of the real signal. The simulation results show that in the case of different CNR of each satellite, the multi-satellite fusion estimation has a lower estimation error than the spoofing signal with the highest CNR. Then the orthogonal subspace of the spoofing signal is constructed, and the spoofing is suppressed in the airspace by using the antenna array weighting to form a null. Finally, by simulating real navigation signals, it is proved that the algorithm can accurately estimate the AOA of forwarding spoofing, and has a good spoofing suppression effect.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

AUTHOR CONTRIBUTIONS

Conceptualization: SN and BR; methodology and validation: BR and FC; formal analysis and investigation: ZL and JW; resources: PM and YS; writing—original draft preparation: SN; writing—review and editing: BR and ZL; supervision: FC and PM; project administration: YS.

FUNDING

This research was funded by the National Natural Science Foundation of China (62003354 and U20A0193).

ACKNOWLEDGMENTS

The authors would like to thank the College of Electronic Sciences for providing the test platform.

REFERENCES

1. Zhang Z, Pan L. Current Performance of Open Position Service with Almost Fully Deployed Multi-GNSS Constellations: GPS, GLONASS, Galileo, BDS-2, and BDS-3. *Adv Space Res* (2022) 69(5):1994–2019. doi:10.1016/j.asr.2021.12.002
2. Odijk D, Nadarajah N, Zaminpardaz S, Teunissen PJG. GPS, Galileo, QZSS and IRNSS Differential ISBs: Estimation and Application. *GPS Solut* (2017) 21(2):439–50. doi:10.1007/s10291-016-0536-y
3. Akhmedov D, Moldabekov M, Yeryomin D, Zhaxygulova D, Kaliyeva R. Application of the Automated Control System for Reference GNSS Station Network in the Transport Sector. *J Phys Conf Ser* (2020) 1626(1):012076. doi:10.1088/1742-6596/1626/1/012076
4. Rahimi Z, Mohd Shafri HZ, Norman M. A GNSS-Based Weather Forecasting Approach Using Nonlinear Auto Regressive Approach with Exogenous Input (NARX). *J Atmos Solar-Terrestrial Phys* (2018) 178:74–84. doi:10.1016/j.jastp.2018.06.011
5. Noack PO, Eder D, Bleisteiner N. Infuence of Electric Power Lines on the Reception of GNSS-Signals in Automatic Steering Systems. *Landtechnik* (2018) 73(3):52–61. doi:10.15150/lt.2018.3182
6. Materna K, Feng L, Lindsey EO, Hill EM, Ahsan A, Alam AKMK, GNSS Characterization of Hydrological Loading in South and Southeast Asia. *J Int* (2020) 224(3):1742–52. doi:10.1093/gji/ggaa500
7. Gao GX, Sgammini M, Lu M, Kubo N. Protecting GNSS Receivers from Jamming and Interference. *Proc IEEE* (2016) 104(6):1327–38. doi:10.1109/JPROC.2016.2525938
8. Jing D, He B, Silin L. Study of Key Issues for the Combat Application of GNSS. In: ICCDE' 19: Proceedings of the 2019 5th International Conference on Computing and Data Engineering; Shanghai, China, May 2019 (2019). doi:10.1145/3330530.3330533
9. Wang F, Yang D, Niu M, Yang L, Zhang B. Sea Ice Detection and Measurement Using Coastal GNSS Reflectometry: Analysis and Demonstration. *IEEE J Sel Top Appl Earth Observations Remote Sensing* (2022) 15:136–49. doi:10.1109/JSTARS.2021.3133431
10. Jiao J, Deng Z, Arain QA, Li F. Smart Fusion of Multi-Sensor Ubiquitous Signals of Mobile Device for Localization in GNSS-Denied Scenarios. *Wireless Pers Commun* (2021) 116(3):1507–23. doi:10.1007/s11277-018-5725-2
11. Carroll JV. Vulnerability Assessment of the U.S. Transportation Infrastructure that Relies on the Global Positioning System. *J Navigation* (2003) 56:185–93. doi:10.1017/s0373463303002273
12. Capon J. High-resolution Frequency-Wavenumber Spectrum Analysis. *Proc IEEE* (1969) 57(8):1408–18. doi:10.1109/PROC.1969.7278
13. Wen H, Huang P. Countermeasures for GPS Signal Spoofing. In: Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005); September 2005; Long Beach, CA, USA (2005). p. 1285–90.
14. Pini M, Fantino M. Signal Quality Monitoring Applied to Spoofing Detection. In: Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation; September 20 - 23, 2011; Portland, OR (2011). p. 1888–96.
15. Dovis F, Chen X. Detection of Spoofing Threats by Means of Signal Parameters Estimation. In: Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation; Portland, OR, January 2011 (2011). p. 416–21.
16. Akos DM. Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *J Inst Navig* (2012) 59(4):281–90. doi:10.1002/navi.19
17. Wang Q, Li H. Residual Vector Analysis Method (RVAM) for Evaluating the Performance of GNSS Part of Channels' Replay Attacks. In: IEEE China Summit & International Conference on Signal and Information Processing; 6-10 July 2013; Beijing, China (2013). p. 561–5.
18. Psiaki M, Powell S. GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-phase Data. In: Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation; September 2013; Nashville, TN (2013). p. 2949–91.
19. Psiaki M, Powell S. GNSS Spoofing Detection, Correlating Carrier Phase with Rapid Antenna Motion. *GPS World* (2013) 24(6):53–58.
20. Nielsen J, Broumandan A, Lachapelle G. GNSS Spoofing Detection for Single Antenna Handheld Receivers. *Navigation* (2011) 58(4):335–44. doi:10.1002/j.2161-4296.2011.tb02590.x
21. Psiaki ML, O'Hanlon BW, Bhatti JA, Shepard DP, Humphreys TE. GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals. *IEEE Trans Aerosp Electron Syst* (2013) 49(4):2250–67. doi:10.1109/TAES.2013.6621814
22. Gao Y, Li H, Lu M, Feng Z. Intermediate Spoofing Strategies and Countermeasures. *Tinshhua Sci Technol* (2013) 18:599–605. doi:10.1109/tst.2013.6678905
23. Stenberg N, Axell E, Rantakokko J, Hendeby G. Results on GNSS Spoofing Mitigation Using Multiple Receivers. *navi* (2022) 69(1):510. doi:10.33012/navi.510
24. Zhang Y, Wang L, Wang W, Lu D, Jia Q, Wu R. Spoofing Interference Suppression for GNSS Based on Estimating Steering Vectors. In: China Satellite Navigation Conference; 02 April 2015; China (2015). p. 765–71. doi:10.1007/978-3-662-46638-4_66
25. Magiera J, Katulski R. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *J Appl Res Tech* (2015) 13(1):45–57. doi:10.1016/S1665-6423(15)30004-3
26. Fante RL, Vaccaro JJ. Wideband Cancellation of Interference in a GPS Receive Array. *IEEE Trans Aerosp Electron Syst* (2000) 36(2):549–64. doi:10.1109/7.845241
27. Wilbur LM, Zoltowski M, Goldstein J. GPS Jammer Suppression with Low-Sample Support Using Reduced-Rank Power Minimization. In: Proceedings of the Tenth IEEE Workshop on Statistical Signal and Array Processing; 16-16 Aug. 2000; Pocono Manor, PA (2000). p. 514.
28. Compton RT. The Power-Inversion Adaptive Array: Concept and Performance. *IEEE Trans Aerosp Electron Syst* (1979) 15(6):803–14. doi:10.1109/TAES.1979.308765

29. Lu Z, Song J, Huang L, Ren C, Xiao Z, Li B. Distortionless 1/2 Overlap Windowing in Frequency Domain Anti-jamming of Satellite Navigation Receivers. *Remote Sensing* (2022) 14:1801. doi:10.3390/rs14081801

30. Song J, Lu Z, Xiao Z, Li B, Sun G. Optimal Order of Time-Domain Adaptive Filter for Anti-jamming Navigation Receiver. *Remote Sensing* (2022) 14(48):48. doi:10.3390/rs14010048

31. Lu Z, Nie J, Wan Y, Ou G. Optimal Reference Element for Interference Suppression in GNSS Antenna Arrays under Channel Mismatch. *IET Radar, Sonar & Navigation* (2017) 11(7):1161–9. doi:10.1049/iet-rsn.2016.0582

32. Huang L, Lu Z, Xiao Z, Ren C, Song J, Li B. Suppression of Jammer Multipath in GNSS Antenna Array Receiver. *Remote Sensing* (2022) 14:350. doi:10.3390/rs14020350

33. Lu Z, Chen H, Chen F, Nie J, Ou G. Blind Adaptive Channel Mismatch Equalisation Method for GNSS Antenna Arrays. *IET Radar, Sonar &amp; Navigation* (2018) 12:383–9. doi:10.1049/iet-rsn.2017.0416

34. Nehorai A. A Minimal Parameter Adaptive Notch Filter with Constrained Poles and Zeros. *IEEE Trans Acoust Speech, Signal Process* (1985) 33(5): 983–96. doi:10.1109/TASSP.1985.1164643

35. Mao W-L, Ma W-J, Chien Y-R, Ku C-H. New Adaptive All-Pass Based Notch Filter for Narrowband/FM Anti-jamming GPS Receivers. *Circuits Syst Signal Process* (2011) 30(3):527–42. doi:10.1007/s00034-010-9242-0

36. Krim H, Viberg M. Two Decades of Array Signal Research: The Parametric Approach. *IEEE Signal Process Mag* (1996) 13:37–94. doi:10.1109/79.526899

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.