sensors

MDPI

Article

Adaptive Spoofing Suppression Algorithm for GNSS Based on Multiple Antennas Array

Guangwei Fan [1,2], Xingli Gan [1,2,*], Baoguo Yu [1,2], Qiang Rong [1,2] and Chuanzhen Sheng [1,2]

[1] State Key Laboratory of Satellite Navigation System and Equipment Technology, Shijiazhuang 050081, China; fgweihb@163.com (G.F.); yubg@sina.cn (B.Y.); rong_54@163.com (Q.R.); shengchuanzhen@163.com (C.S.)

[2] The 54th Research Institute of China Electronics Technology Group Corporation, Shijiazhuang 050081, China

* Correspondence: ganxingli@163.com; Tel.: +86-133-1510-8398

Received: 20 January 2020; Accepted: 14 February 2020; Published: 18 February 2020

Abstract: The signals of navigation satellites are easily affected by spoofing interference, causing the wrong position, speed or Universal Time Coordinate of the receiver to be calculated. Traditional detection and suppression algorithms are used only to eliminate the spoofing signals, which may lead to an insufficient number of satellites for positioning. An adaptive spoofing suppression algorithm (ASSA) based on a multiple antenna array is proposed in this study. The ASSA can use the cross-correlation gain of multiple antenna array to adaptively generate nulling and realize the simultaneous suppression of multiple spoofing signals. Moreover, ASSA does not need to capture and track spoofing separately, thus reducing the complexity of implementation and calculation. Experiments were conducted to verify the proposed system under different conditions, and the results show that ASSA can suppress multiple spoofings with little impact on positioning performance. Under the condition of spoofing, ASSAs were (2.22 m, 2.41 m, 4.43 m) in the static test and (2.27 m, 2.43 m, 4.64 m) in the kinematic test, which are good positioning performances for both. In addition, the ASSA is applied before capturing signals, which is beneficial to identifying and eliminating spoofing earlier and faster.

Keywords: satellite navigation; spoofing; suppression; cross-correlation; adaptive nullification

1. Introduction

Global satellite navigation systems (GNSSs) are widely used in civil aviation, transportation, power, finance and other fields [1]. However, due to the low power of their navigation signals, they are easily affected by various interferences, such as spoofing and suppression. Spoofing interference is a great threat to GNSS security [2,3]. In 2001, a report on the vulnerability of GNSS was assessed by the US Department of transportation, which pointed out that there are serious security risks in transportation systems [4]. In 2009, the US naval surface operations center issued a report on the problem of GNSS spoofing interference [5], stating that GNSS should not only focus on positioning accuracy, but also on application security [6].

Signal processing algorithms have been studied as a means to detect spoofing interference. The difference in a Doppler shift between a satellite's navigation signal and spoofing to identify the spoofing [7,8]. Monitoring a received signal's power, carrier noise ratio and noise level can also be used to detect spoofing [9–11]. A new signal-quality assessment model has been proposed to detect and identify spoofing [12] that can work well even when the strength of a received signal's spoofing and authentic signal are very close to each other. However, the performance of this algorithm may deteriorate when the code phase differences between authentic signals and spoofing signals are <1.5 chips and the Doppler frequency differences between authentic signals and spoofing signals are relatively small. Sensitivity models have been formulated that include a vestigial signal-to-interference and noise ratio (SINR) that is quantified and characterized to detect the probability of a false alarm [13].

Power-distortion detectors identify spoofing by analyzing the distortion of the received power via a correlation function [14]. This enables civil global positioning system receivers and other civil global navigation satellite system receivers to reliably detect carry-off spoofing and jamming.

Data processing algorithms have also been studied as a means of detecting spoofing. When an antenna is rotating, the power measurements of the spoofing signals coming from the same direction change similarly and the correlation coefficients between them are close to 1, but the power measurements of the authentic signals are uncorrelated [15]. A new approach for GPS spoofing detection based on a multi-layer neural network (NN) whose inputs are indices of features is presented in [16]. This method demonstrated adequate detection accuracy from the NN with a short detection time. The autonomous integrity information of the receiver can also be used to detect and identify spoofing [17], and it is able to resist attacks from one or many spoofing satellites. Inertial Navigation System (INS)/GNSS integrated navigation can also be used to detect and identify spoofing, using a Kalman filter (KF) and non-linear approximation techniques such as an extended Kalman filter (EKF), (Sigma Point Kalman Filter (SPKF)) or divided difference filters (DDF) [18,19].

Finally, suppression algorithms using multiple antennas have been studied as a means of detecting spoofing interference. If a spoofing transmitter transmits spoofing signals from several different satellites at the same time, the spatial correlation of each spoofing signal can be detected by multi antenna direction finding (similar to an interferometer) [20,21]. Since the baseline between the antennas is known, the direction of arrival of the received signal can be obtained using the same satellite to reach the antenna carrier phase difference [22]; if different satellite signals come from the same direction, it can be judged that their own party has been deceived. After determining the direction of the spoofing, the spoofing can be eliminated or suppressed. A new approach [23] has also been proposed combing a generalized side-lobe canceller (GSC) and space-time adaptive faltering (which is used to suppress spoofing). In addition, an encryption algorithm based on a signal's authentication sequence has been analyzed that can resist a spoofing signal's attack [24,25], but the signal format needs to be modified, as it is not suitable for the GNSS civil navigation signal that has been applied at present.

In the following sections, an adaptive spoofing-interference suppression algorithm is proposed for satellite navigation based on a multi antenna array. The cross-correlation gain of the spread spectrum signal received by the array is determined to be higher than the noise level, and the direction of the received signal does not need to be estimated, as this algorithm can realize the adaptive filtering of satellite navigation spoofing. It reduces the complexity of satellite navigation spoofing suppression and improves its performance. The main contributions of this paper are as follows:

1. An adaptive spoofing interference suppression algorithm is proposed for satellite navigation based on a multi antenna array. This algorithm improves the real-time performance of spoofing suppression and reduces the complexity of spoofing interference suppression.
2. A cross-correlation model of satellite navigation spoofing signals received by multiple elements is established. The feasibility of using the spread spectrum signals received between different array elements as a cross-correlation by which to suppress spoofing interference is analyzed.
3. The complexity of the implementation of the adaptive spoofing suppressor for satellite navigation based on a multi antenna array is analyzed, and the performances of the two algorithms are verified by comparing them with the algorithm that first finds the direction of a signal and then suppresses it. The location performances of the two algorithms are tested under static and dynamic conditions.

2. Spoofing Suppression Algorithm

2.1. Signal Receiving Model of a Multiple Antenna Array for Spoofing

Assume an arbitrary M-element antenna array configuration. In this configuration, one antenna is chosen as the reference antenna. Without loss of generality, assume that the navigation satellite signals can be received at a certain time L. The received signal on the m array element can now be expressed as

$$x_m(t) = \sum_{i=1}^{L} sa_i(t)a_m(\theta_i) + n(t) \tag{1}$$

where $n(t)$ is additive white Gaussian noise, $a_m(\theta_i)$ is the direction vector of satellite i, θ_i is the direction of arrival of the i th satellite signal, τ_i is the delay of the ith satellite signal $sa_i(t)$ is the navigation signal of the ith satellite received, and t is the signal arrival time. The navigation signal composition is as follows:

$$sa_i(t) = \sqrt{P_i}b_i(t-\tau_i)c_i(t-\tau_i) \tag{2}$$

where P_i is the total transmit power of the ith satellite, $b_i(t) \in [0, T_b]$ is the ith satellite data bit, and c_i is the binary spreading (ranging) code of the ith satellite [26].

If the received signal contains a spoofing signal, the received signal can be written as

$$x_m(t) = \sum_{i=1}^{L} sa_i(t)a_m(\theta_i) + \sum_{k=1}^{K} sp_k(t)a_m(\theta_k) + n(t) \tag{3}$$

where θ_k is the direction of the spoofing signal, K is the number of spoofings, $sp_k(t)$ is the spoofing signal for the kth satellite, $sp_k(t) = \sqrt{P_{sk}}b_k(t-\tau_{sk})c_k(t-\tau_{sk})a_m(\theta_k)$, τ_{sk} is the delay of the spoofing signal, and c_k is the binary spreading (ranging) code of the kth spoofing signal. Spoof signals are often similar to currently visible satellite signals. The received signal of the mth array element can now be written as

$$x_m(t) = \sum_{i=1}^{N} \sqrt{P_i}b_i(t-\tau_i)c_i(t-\tau_i)a_m(\theta_i) + \sum_{k=1}^{K} sp_k(t) + n(t) \tag{4}$$

M receives spatial samples of authentic and spoofing signals impinging on the antenna array before despreading, which can be written in a matrix form as

$$\boldsymbol{X}_M = \begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_M(t) \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{L} sa_i(t)a_1(\theta_i) \\ \sum_{i=1}^{L} sa_i(t)a_2(\theta_i) \\ \vdots \\ \sum_{i=1}^{L} sa_i(t)a_M(\theta_i) \end{bmatrix} + \begin{bmatrix} \sum_{i=1}^{L} sp_i(t)a_1(\theta_i) \\ \sum_{i=1}^{L} sp_i(t)a_2(\theta_i) \\ \vdots \\ \sum_{i=1}^{L} sp_i(t)a_M(\theta_i) \end{bmatrix} + \begin{bmatrix} n_1(t) \\ n_2(t) \\ \vdots \\ n_m(t) \end{bmatrix} \tag{5}$$

The use of arrays to receive satellite navigation signals can enhance or suppress signals from different directions, thereby achieving suppression of satellite navigation interference signals.

2.2. Suppressing Spoofing Based on Direction of Arrival (DOA)

Filtering (despread) the received signal $x(t)$ of the array according to the spreading code $c_i(t-\tau_i)$ of the ith desired satellite results in the nth bit of the processed signal being written as follows:

$$y_{mi}(n) = \frac{1}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} x(t)c_i(t-\tau_i)dt = \sqrt{T_bP_i}b_i(n)e^{-j\varphi(\theta)}a_m(\theta_i) + \sqrt{T_bP_{si}}b_i(n)e^{-j\varphi(\beta)}a_m(\beta_i) + n(t) \tag{6}$$

where T_b is the binary spreading (ranging) code period, c_i is the binary spreading (ranging) code of the ith spoofing signal, P_i is the navigation signal gain, P_{si} is the gain of spoofing, $b_i(n)$ is the ith satellite data bit, θ_i is the direction of arrival of the ith navigation signal, and β_i is the direction of arrival of the ith spoofing signal.

Let $\boldsymbol{y}_i(n) = [y_{1i}, y_{2i}, \cdots, y_{Mi}]^{\mathrm{H}}$, $\boldsymbol{A}(\theta_i) = [a_1(\theta_i), a_2(\theta_i), \cdots, a_M(\theta_i)]^{\mathrm{H}}$. Then the covariance matrix of the despread signal $\boldsymbol{y}_i$ can be approximated as

$$\boldsymbol{R}_{y_i y_i} = \frac{1}{T_c} E\left\{\boldsymbol{y}_i(n)\boldsymbol{y}_i^*(n)\right\} = GP_i\boldsymbol{A}(\theta_i)\boldsymbol{A}^{\mathrm{H}}(\theta_i) + GP_{si}\boldsymbol{A}(\beta_i)\boldsymbol{A}^{\mathrm{H}}(\beta_i) + \sigma_n^2\boldsymbol{I} \tag{7}$$

where σ_n^2 is the variance of thermal noise, $\boldsymbol{I}$ is the unit matrix, T_c is the chip interval, and $G = \frac{T_b}{T_c}$ is the spreading gain.

After despreading, the signal power becomes G times that of the original. With reference to the general satellite transmitted signal, the gain G of the despreading processing is determined to be about 43 db. Generally, the level of the satellite navigation signal reaching the antenna interface is about −20 dB, and spoofing is usually about 5–10 dB higher than the satellite signal in order to achieve a good spoofing effect. After dispreading, the signal power is 23–30 dB higher than the noise power. Therefore, the traditional Direction of Arrival (DOA) estimation algorithm [27–29] can be used to measure the direction of arrival of the spoofing. In this paper, we use the multiple signal classification (MUSIC) algorithm [30] as an example to introduce the process of estimating the direction of arrival of spoofing.

Assume that there is one desired signal and K spoofing. After performing the feature decomposition on the covariance matrix (7), $\boldsymbol{R}_{y_i y_i}$ can be expressed as

$$\boldsymbol{R}_{y_i y_i} = \sum_{i=1}^{K+1} \lambda_i \boldsymbol{u}_i \boldsymbol{u}_i^{\mathrm{H}} + \sigma_n^2 \sum_{i=K+2}^{M} \boldsymbol{u}_i \boldsymbol{u}_i^{\mathrm{H}} \tag{8}$$

where eigenvalues of the covariance matrix $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_{K+1} > \lambda_{K+2} = \cdots = \lambda_M = \sigma_n^2$ are the corresponding M eigenvalues, of which the corresponding feature vector is $\mathbf{u}_i$ ($i = 1, 2, \cdots, M$). This is written as

$$\boldsymbol{D}_{\mathrm{s}} = diag(\lambda_1, \lambda_2, \cdots, \lambda_{K+1}) \tag{9}$$

$$\boldsymbol{D}_{\mathrm{n}} = diag(\lambda_{K+2}, \lambda_{K+3}, \cdots, \lambda_M) \tag{10}$$

The corresponding signal subspace of the large eigenvalue expansion is $\boldsymbol{U}_{\mathrm{s}} = [\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_{K+1}]$, and the noise subspace is $\boldsymbol{U}_{\mathrm{N}} = [\boldsymbol{u}_{K+2}, \boldsymbol{u}_{K+3}, \cdots, \boldsymbol{u}_M]$. The signal subspace and noise subspace are orthogonal to each other.

Simultaneously, the array direction vector of the received signals is also orthogonal to the noise subspace. As such, the spatial spectrum function of the MUSIC algorithm $\boldsymbol{U}_{\mathrm{N}}^{\mathrm{H}}\boldsymbol{A}(\theta_i) = 0$ can be expressed as:

$$P_{MUSIC}(\theta) = \frac{1}{\boldsymbol{A}^{\mathrm{H}}(\theta)\boldsymbol{U}_{\mathrm{N}}\boldsymbol{U}_{\mathrm{N}}^{\mathrm{H}}\boldsymbol{A}(\theta)} \tag{11}$$

Estimating the direction of arrival of the spoofing signal and the navigation signal is achieved via Equation (11).

After determining the direction of arrival of the received signals, spoofing and navigation signals are identified based on their energy and direction angle. The array flow pattern $\boldsymbol{B}_{\mathrm{S}} = \begin{bmatrix} a(\widehat{\theta}_1^s) & a(\widehat{\theta}_2^s) & \cdots & a\left(\theta_M^s\right) \end{bmatrix}$ can be obtained according to the array steering vector of the spoof signal. The spoofing signal subspace [31] can now be expressed as

$$\boldsymbol{U}_{\mathrm{S}_0} = \boldsymbol{B}_{\mathrm{S}}\left(\boldsymbol{B}_{\mathrm{S}}^{\mathrm{H}}\boldsymbol{B}_{\mathrm{S}}\right)^{-1}\boldsymbol{B}_{\mathrm{S}} \tag{12}$$

According to the orthogonality of the signal subspace and the noise subspace, the noise subspace can be obtained:

$$\boldsymbol{U}_{\mathrm{N}_0} = \boldsymbol{I} - \boldsymbol{U}_{\mathrm{S}_0} = \boldsymbol{I} - \boldsymbol{B}_{\mathrm{S}}\left(\boldsymbol{B}_{\mathrm{S}}^{\mathrm{H}}\boldsymbol{B}_{\mathrm{S}}\right)^{-1}\boldsymbol{B}_{\mathrm{S}} \tag{13}$$

The optimization problem of beam weighting minimizes the power of residual interference and noise in the output. Since the optimal weight vector does not change the power of the target signal, the output signal-to-interference and noise ratio can be maximized. Using the Lagrangian multiplier algorithm, the solution of the optimal filter processor can be expressed as

$$\boldsymbol{w}_{\text{opt}}=\left[\boldsymbol{s}^{\text{H}}\boldsymbol{U}_{\text{N}_0}\boldsymbol{s}\right]^{-1}\boldsymbol{U}_{\text{N}_0}\boldsymbol{s} \tag{14}$$

where $\boldsymbol{s}$ is the constraint vector of $M\times 1$; without constraint, the vector is $\boldsymbol{s}=[1,0,\cdots,0]^{\text{H}}$. When the direction of arrival of the satellite signal is known, the value of constraint vector can be determined in order to enhance the satellite signal using $\boldsymbol{s}=[1,a_1(\alpha),\cdots,a_M(\alpha)]^{\text{H}}$, where α is the satellite navigation signal constraint direction. The output of filtering processing is

$$y_{\text{out}}=\boldsymbol{w}_{\text{opt}}^{\text{H}}\boldsymbol{X}_M \tag{15}$$

where y is the signal after spoofing suppression.

A block diagram of the implementation of the spoofing suppression algorithm based on DOA is shown in Figure 1.

The implementation process of this algorithm is complicated and not conducive to real-time implementation. The implementation process of the algorithm can be described as follows:

Algorithms:

1. The received signal of the array antenna is $\boldsymbol{X}_M=[x_1(t),x_2(t),\cdots x_M(t)]$
2. Despreading the signals received by multiple antennas for one satellite is expressed as $y_{mi}(n)=\frac{1}{\sqrt{T_b}}\int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1}x(t)c_i(t-\tau_i)dt=\sqrt{T_bP_i}b_i(n)e^{-j\varphi(\theta)}a_m(\theta_i)+\sqrt{T_bP_{si}}b_i(n)e^{-j\varphi(\beta)}a_m(\beta_i)+n(t)$
3. The autocorrelation matrix $\boldsymbol{R}_{y_iy_i}$ of the despreading signal is determined along with the eigenvalues of the matrix. The signal subspace $\boldsymbol{U}_{\text{s}}=[\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_{K+1}]$ and noise subspace $\boldsymbol{U}_{\text{N}}=[\boldsymbol{u}_{K+2},\boldsymbol{u}_{K+3},\cdots,\boldsymbol{u}_M]$ are built.
4. The spatial spectrum function $P_{MUSIC}(\theta)=\frac{1}{\boldsymbol{A}^{\text{H}}(\theta)\boldsymbol{U}_{\text{N}}\boldsymbol{U}_{\text{N}}^{\text{H}}\boldsymbol{A}(\theta)}$ is constructed. The spectrum peak is determined, and discrimination of the spoofing and navigation signals is carried out based on search spectrum peak-to-peak size, number and direction of incidence angle.
5. Subspace $\boldsymbol{U}_{\text{S}_0}=\boldsymbol{B}_{\text{S}}\left(\boldsymbol{B}_{\text{S}}^{\text{H}}\boldsymbol{B}_{\text{S}}\right)^{-1}\boldsymbol{B}_{\text{S}}$ of the spoofing signal is constructed based on array flow pattern $\boldsymbol{B}_{\text{S}}=\left[\begin{array}{cccc}\widehat{a(\theta_1^s)} & \widehat{a(\theta_2^s)} & \cdots & a\left(\theta_M^s\right)\end{array}\right]$ of the spoofing signal incidence angle. The corresponding noise subspace $\boldsymbol{U}_{\text{N}_0}=\boldsymbol{I}-\boldsymbol{U}_{\text{S}_0}=\boldsymbol{I}-\boldsymbol{B}_{\text{S}}\left(\boldsymbol{B}_{\text{S}}^{\text{H}}\boldsymbol{B}_{\text{S}}\right)^{-1}\boldsymbol{B}_{\text{S}}$ is determined, and the optimal weight of spoofing suppression without constraints or satellite signal direction constraints is identified and shown as $\boldsymbol{w}_{\text{opt}}=\left[\boldsymbol{s}^{\text{H}}\boldsymbol{U}_{\text{N}_0}\boldsymbol{s}\right]^{-1}\boldsymbol{U}_{\text{N}_0}\boldsymbol{s}$.
6. According to the optimal weight vector, the received signal of array antenna is filtered, and the filtered navigation signal is obtained, shown as $y_{\text{out}}=\boldsymbol{w}_{\text{opt}}^{\text{H}}\boldsymbol{X}_M$. The filtered signal y_{out} is sent to the baseband receiver for acquisition tracking.

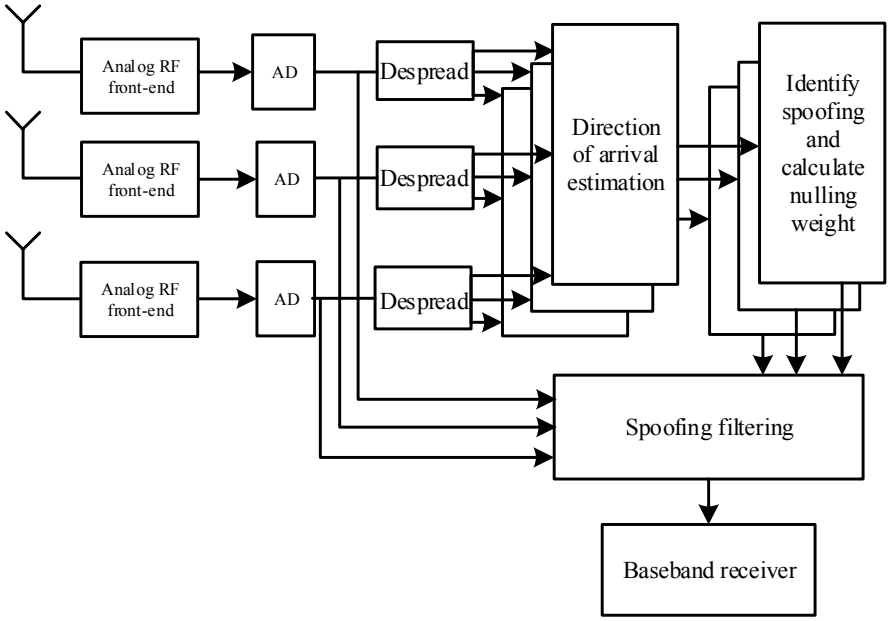

Figure 1. Suppressing spoofing based on Direction of Arrival (DOA).

2.3. Adaptive Spoofing Suppression Algorithm (Assa)

Without estimating the direction of arrival of the spoofing signal, adaptive spoofing suppression is an effective way to reduce the complexity of the spoofing interference suppression.

According to Equation (1), the cross-correlation of received signals from different array elements can be defined as:

$$q_m(n) = \frac{1}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} x_m(t) x_q(t) dt \tag{16}$$

where $\boldsymbol{x}_q(t)$ is the received signal of the reference array element, and $\boldsymbol{x}_m(t)$ is the received signal of the mth array element. Expanding on this, Equation (16) can be written as:

$$\begin{aligned} q_m(n) &= \frac{1}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} \left(\sum_{i=1}^{L} sa_i(t) a_m(\theta_i) + \sum_{k=1}^{K} sp_k(t) a_m(\theta_k) + n(t) \right) \left(\sum_{i=1}^{L} sa_i(t) a_q(\theta_i) + \sum_{k=1}^{K} sp_k(t) a_q(\theta_k) + n(t) \right) dt \\ &\approx \frac{1}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} \left(\sum_{i=1}^{L} sa_i(t) a_m(\theta_i) + \sum_{k=1}^{K} sp_k(t) a_m(\theta_k) \right) \left(\sum_{i=1}^{L} sa_i(t) a_q(\theta_i) + \sum_{k=1}^{K} sp_k(t) a_q(\theta_k) \right) dt + n(t) \end{aligned} \tag{17}$$

The low cross-correlation gain between different satellite signals is due to general pseudo-code characteristics, and the spoofing signal is less than the number of currently visible navigation satellites, $K \leq L$. Equation (17) can therefore be written as:

$$\begin{aligned} q_m(n) = \; & \frac{1}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} \left(\sum_{i=1}^{L} sa_i^2(t) a_m(\theta_i) a_q(\theta_i) \right) dt + \frac{1}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} \left(\sum_{k=1}^{K} sp_k^2(t) a_m(\theta_k) a_q(\theta_k) \right) dt + \cdots \\ & \frac{1}{\sqrt{T_b}} \left(\int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} \left(\sum_{i=1}^{L} sa_i(t) a_m(\theta_i) \right) \left(\sum_{k=1}^{K} sp_k(t) a_q(\theta_k) \right) + \left(\sum_{i=1}^{L} sa_i(t) a_q(\theta_i) \right) \left(\sum_{k=1}^{K} sp_k(t) a_m(\theta_k) \right) \right) dt + n(t) \end{aligned} \tag{18}$$

Because real satellite signals come from different directions, it can be assumed that all spoofing signals come from the same source, such as $\theta_k = \theta_K (k = 1, 2, \cdots K)$. t can be further be simplified as:

$$q_m(n) = \frac{1}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} \left(\sum_{i=1}^{L} sa_i^2(t) a_m(\theta_i) a_q(\theta_i) \right) dt + \frac{a_m(\theta_K) a_q(\theta_K)}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} \left(\sum_{k=1}^{K} sp_k^2(t) \right) dt + \cdots$$
$$\frac{1}{\sqrt{T_b}} \left(\int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} a_q(\theta_k) \left(\sum_{i=1}^{K} sa_i(t) sp_i(t) a_m(\theta_i) \right) + a_m(\theta_K) \left(\sum_{i=1}^{K} sa_i(t) sp_i(t) a_q(\theta_i) \right) \right) dt + n(t) \tag{19}$$

Generally, the received power of the spoofing is about 5–10 dB higher than that of the satellite navigation signal. In other words, the spoofing gain is about 10–20 dB higher than the navigation signal after correlation despreading. The power of the satellite navigation signal to the receiving antenna is usually about 20 dB less than the noise. Taking the BeiDou B1 signal as an example, the gain of correlation despreading is about 21 dB. Different satellite navigation signals arrive from different directions, and array signal processing will restrict signal enhancement from a certain direction; therefore, the signals energy will not exceed the noise after cross-correlation between different channels. The cross-correlation gain of the spoofing signal is 10–20 dB higher than that of the navigation signal, which is to say that the level of the cross-correlation spoofing signal is above the noise. If the spoofing signal is a single-address broadcast spoofing signal, the array can receive multiple spoofing signals to achieve a superposition from the same direction.

Therefore, formula (19) can be approximately equal to:

$$q_m(n) \approx \frac{a_m(\theta_K) a_q(\theta_K)}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} \left(\sum_{k=1}^{K} sp_k^2(t) \right) dt + n(t) \tag{20}$$

By expanding the components of Equation (20), we can get:

$$q_m(n) = \sqrt{T_b} a_m(\theta_K) a_q(\theta_K) \sum_{k=1}^{K} P_{sk} b_k(n) + n(t) \tag{21}$$

The cross-correlation gain generated by cross-correlation processing between the signals received by different antenna elements is shown in the Figure 2:

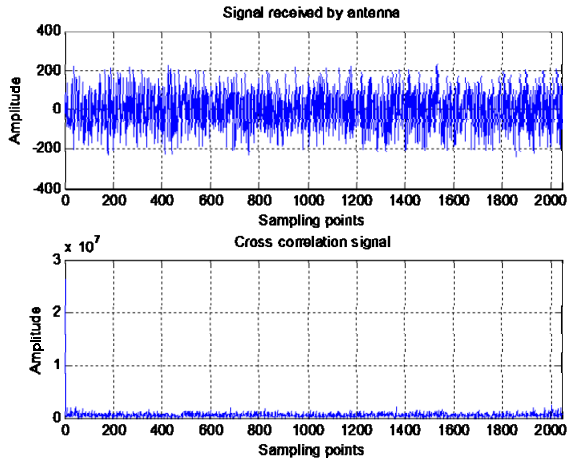

Figure 2. Signal comparison before and after cross-correlation.

The signals received by the array elements are completely submerged under the noise, and the adaptive notch algorithm cannot be used to achieve the suppression of spoofing. When the signals received by the two array elements are cross-correlated and coherently accumulated, a peak can be formed that is equivalent to that the energy of the received signal and higher than the noise. Therefore, the adaptive notch algorithm can be used to suppress spoofing.

Assume the cross-correlation data length is N; the received signal after cross-correlation can be expressed as $\boldsymbol{Q}_N = [q_1\ q_2 \cdots q_M]$. The covariance matrix after cross-correlation can now be expressed as

$$\boldsymbol{R}_Q = (\sum_{n=1}^{N} \boldsymbol{Q}_N * {\boldsymbol{Q}_N}^{\mathrm{H}})/N \tag{22}$$

After obtaining the covariance matrix after cross-correlation, the optimal weight of the adaptive notch can be calculated according to the following formula:

$$\boldsymbol{w}_{\mathrm{opt}} = \boldsymbol{R}_{\mathrm{Q}}^{-1} * \boldsymbol{s} \tag{23}$$

Without directional constraints, $\boldsymbol{s} = [1, 0, \cdots, 0]^{\mathrm{H}}$. In practical applications, satellite signals usually come from the area with a high elevation angle, while spoofing usually occurs in a place with a low elevation due to the limitations of the actual environment angle. Constraints are put on specific directions, and the value of the constraint vector is determined as $\boldsymbol{s} = [1, a_1(\alpha), \cdots, a_M(\alpha)]^{\mathrm{H}}$, where α is the signal-constraint enhancement direction.

The output of the adaptive filtering processing is

$$y_{\mathrm{out}} = \boldsymbol{w}_{\mathrm{opt}}^{\mathrm{H}} \boldsymbol{X}_M \tag{24}$$

Figure 3 shows the processing flow of the adaptive spoofing suppression algorithm, which does not require a direction to be established. Multiple spoofing interferences can be suppressed by the adaptive nulling algorithm after a cross-correlation. The algorithm flow can be described as follows:

Algorithms:

1. The array antenna receiving signal is $\boldsymbol{X}_M = [x_1(t), x_2(t), \cdots x_M(t)]$.
2. Any one of these can be selected as a cross-correlation reference signal using $x_q(t) = x_1(t)$.
3. The cross-correlation vector of each signal and the reference signal are calculated for $m = 1, 2, \cdots, M$, $q_m = \frac{1}{\sqrt{T_b}} \int_{(n-1)T_b+\tau_1}^{nT_b+\tau_1} x_m(t) x_q(t) dt$, end.
4. The cross-correlation matrix $\boldsymbol{Q}_N = [q_1\ q_2 \cdots q_M]$ is calculated. The sample lengths of each channel in the N-point covariance matrix are $\boldsymbol{R}_Q = (\sum_{n=1}^{N} \boldsymbol{Q}_N * {\boldsymbol{Q}_N}^{\mathrm{H}})/N$.
5. The constraint vector of the adaptive notch is generated according to constraint conditions s.
6. The weight vector of adaptive notch is calculated by $\boldsymbol{w}_{\mathrm{opt}} = \boldsymbol{R}_{\mathrm{Q}}^{-1} * \boldsymbol{s}$.
7. The array's received signals are filtered by the calculated weights: $y_{\mathrm{out}} = \boldsymbol{w}_{\mathrm{opt}}^{\mathrm{H}} \boldsymbol{X}_M$.

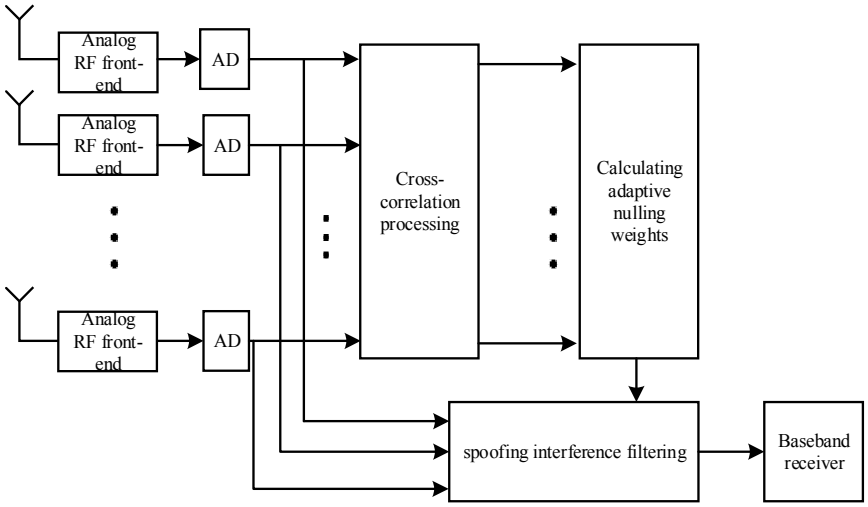

Figure 3. Adaptive spoofing suppression.

2.4. Complexity Analysis

There are three steps in the computation process of the spoofing suppression algorithm based on DOA. The first is despreading the received signal, assuming that the signal is despread in the form of Fast Fourier Transformation (FFT) transform (the computation amount of one channel is $\frac{3N}{2}\log_2 N + N$, the operation amount of M channels is $M\left(\frac{3N}{2}\log_2 N + N\right)$, N is the number of sampling points). The second step is estimating the direction of arrival after despreading, assuming the MUSIC algorithm is adopted (the computation amount is $M^3 + NM^2 + (2M-1)MP$, P is the search times of the algorithm in azimuth and pitch direction). The third step is to establish fixed-direction nulling (the operation amount of this part is $M^3 + 6M^2 + 5M + 1$). The total computation amount is $Q_1 = M\left(\frac{3N}{2}\log_2 N + N\right) + 2M^3 + 6M^2 + 5M + 1 + NM^2 + (2M-1)MP$. Tf K spoofing signals are suppressed, the amount of computation needs to be increased K times.

The calculation process of the adaptive spoofing suppression algorithm based on a multiple antenna array proposed in this paper is divided into two parts: The first is the amount of cross-correlation calculations (the computation amount of M channels is $M\left(\frac{3N}{2}\log_2 N + N\right)$). The second is adaptive nulling generation (the amount of computation is $M^3 + M^2$) The calculation amount of the algorithm in this paper is $Q_2 = M\left(\frac{3N}{2}\log_2 N + N\right) + M^3 + M^2$. An increase in the amount of spoofing will not cause an increase in the amount of computation.

Comparing the computation of the two algorithms, $Q_2 << Q_1 < KQ_1$, and as the number of array elements increases the gap between the two algorithms increases geometrically. The spoofing suppression algorithm based on DOA needs to capture and track the signal first, which is equivalent to a baseband navigation receiver behind each channel, and the synchronization of time and code between different receivers is complex. The ASSA based on a multiple antenna array proposed in this paper is implemented before acquisition and tracking, and has good real-time performance. The back end only needs a baseband navigation receiver, and the amount of equipment is small. Therefore, the algorithm proposed in this paper can greatly reduce the computation of array deception suppression.

3. Implementations and Evaluation

In order to verify the spoofing suppression performance of the algorithm proposed in this paper, we needed to build a satellite navigation anti-spoofing verification environment and collect spoofing data for verification. The equipment components of the verification environment included a spoofing scenario simulation device, spoofing signal digital simulation computer, interference signal analog sources, receiving array antenna, multiple channel signal acquisition and processing equipment, anti-spoofing performance evaluation computer, timing receiver and interference transmitting antenna,

and resource allocation within the system needed to be optimized [32]. The test connection relationship is shown in Figure 4, which includes purchased commercial equipment and self-developed equipment.

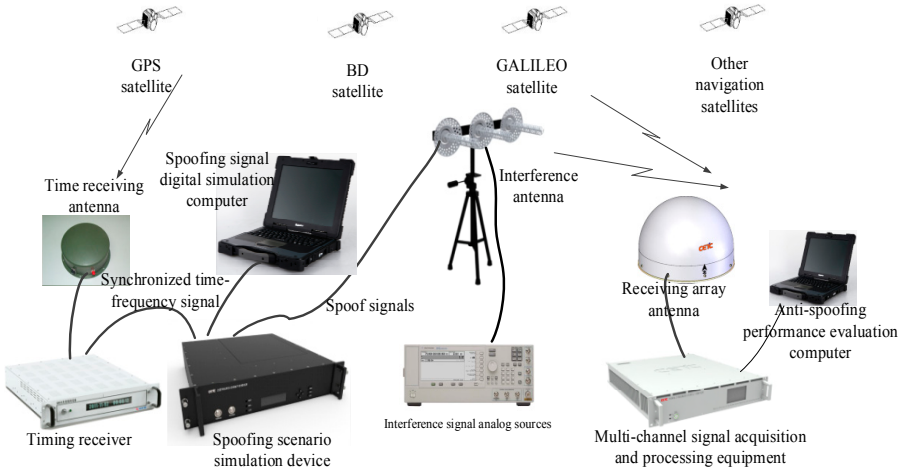

Figure 4. Composition of the wireless anti-spoofing test.

An anti-spoofing test environment was set up at an outdoor test site. The test site was on a hill more than 100 m high, and about 30 m above the flat ground below the hill. The spoofing interference source was installed at the top of the mountain, and could simultaneously transmit eight spoofing interference signals. The spoofing signal had the same pseudo-code structure as the satellite signal visible in the current area. The test trajectory is shown by the red curve in Figure 5. The receiving array used a seven-element Y-shaped circular array, and used signal acquisition and processing equipment to collect satellite navigation and spoofing signals. The test schematic is shown in Figure 5, with a background taken from Google Maps.

Figure 5. Wireless anti-spoofing test environment.

The spoofing simulator generated a spoofing signal with the same pseudo code as the visible satellite in the current area. On the basis of synchronization with the navigation time of the satellite in the sky, eight spoofing signals were transmitted simultaneously by means of single-point broadcasting. The power at the receiving end of the spoofing signal was 5–15dB higher than that of navigation signal.

This test site was located in Cuiwei hill, Luquan District, Shijiazhuang, Hebei Province. The spoofing interference suppression test was completed in October 2019. The weather on the test day was clear, and the ionosphere and troposphere conditions were relatively stable.

3.1. Performance Analysis

The BeiDou B1 signal was used as an example to analyze the spoofing interference suppression performance of the spoofing suppression algorithm. The test equipment composition and test environment are shown in Figures 4 and 5. The signal acquisition and processing equipment saved the collected signals into files, and Matlab was used to analyze the spoofing suppression performance of the two algorithms.

Figures 6 and 7 are a spatial spectrum diagram and a gradient projection diagram of the spoofing suppression algorithm based on DOA, respectively. Figure 8 shows that the algorithm only produces nulls in the direction of spoofing, while the other directions are relatively flat. There is also less impact on the reception of navigation signals as the spoofing suppression is completed. This algorithm has the same implementation process for the suppression of spoofing in different satellites, but to save space the processing of other satellite channels is not listed one by one. This algorithm requires a large amount of calculations and a complicated implementation, but the advantage is that the algorithm can achieve spoof interference suppression in which the direction of the spoof interference emission is greater than the number of array elements because the satellite channels are processed separately and not limited by the number of array elements.

Figure 7 is the spatial spectrum and gradient projection of the ASSA. Figure 9 shows that the algorithm can also form nulls in the direction of spoofing, but that compared with the algorithm that finds the direction first then suppresses backwards, the formed nulls are shallower. The zero trap formed by this algorithm is flat, and there are many redundant nulls, but the algorithm can also achieve a suppression of spoofing.

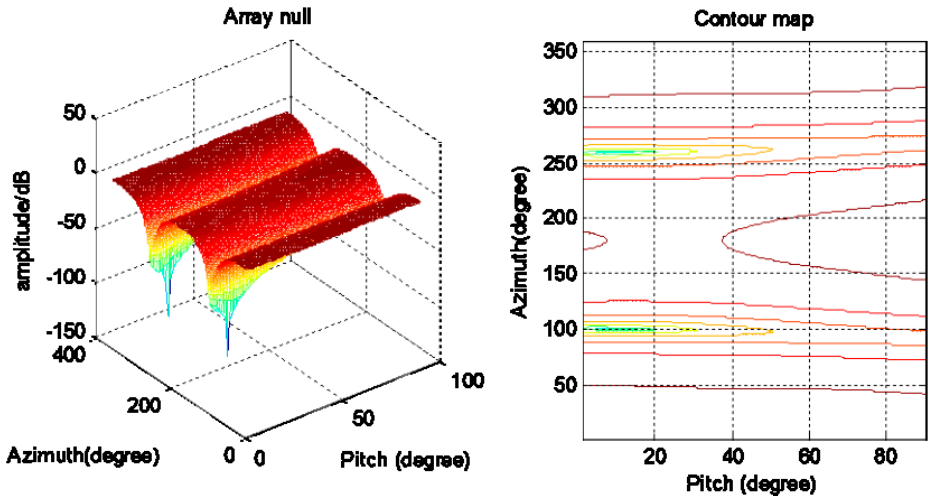

Figure 6. Spoofing suppression based on DOA.

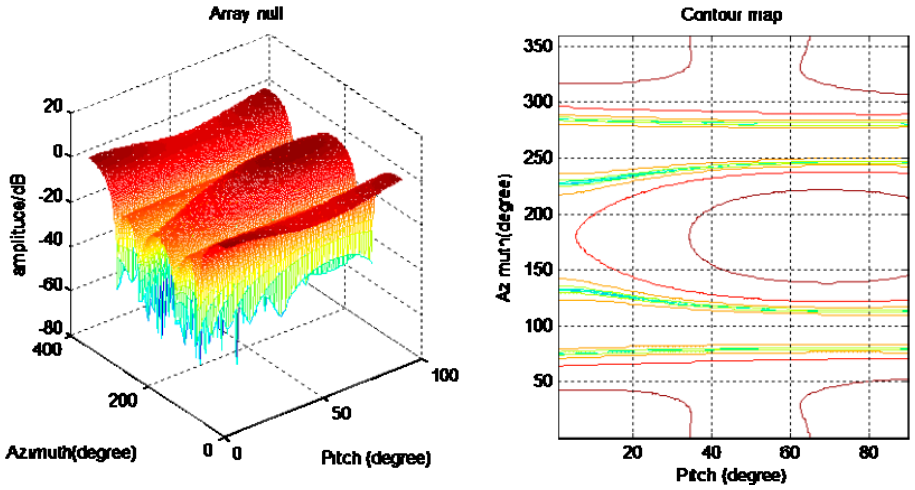

Figure 7. Adaptive spoofing suppression.

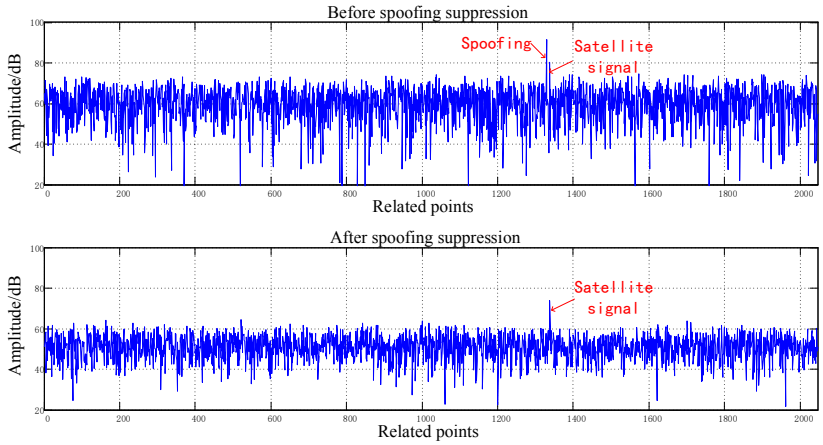

Figure 8. Comparison before and after spoofing suppression (1).

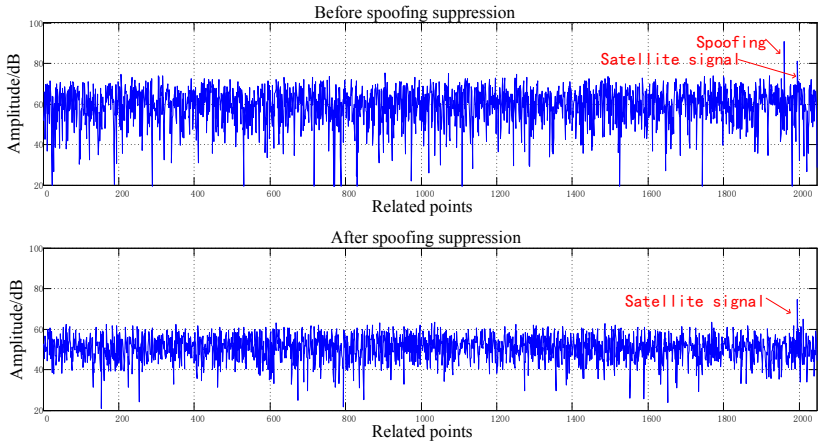

Figure 9. Comparison before and after spoofing suppression (2).

Figures 8–15 correspond respectively to the received signals of the eight satellites being cheated, and show comparisons of the correlated despread signal before and after the spoofing suppression.

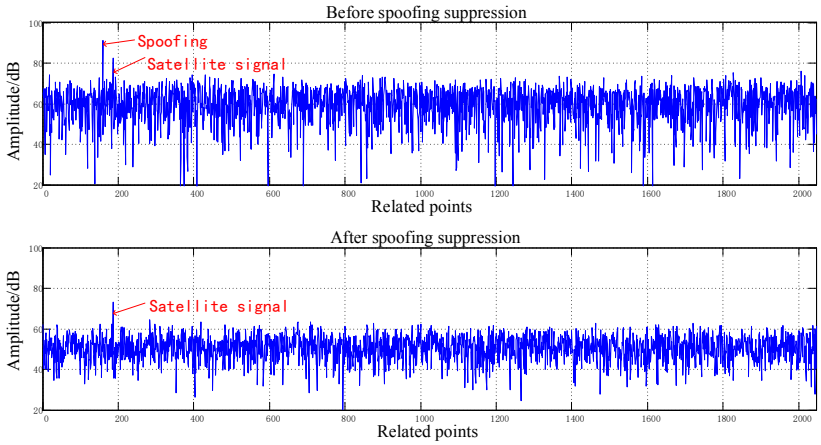

Figure 10. Comparison before and after spoofing suppression (3).

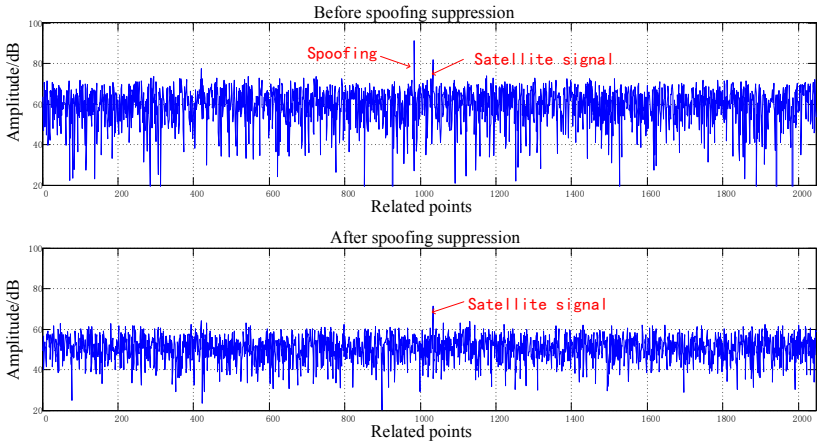

Figure 11. Comparison before and after spoofing suppression (4).

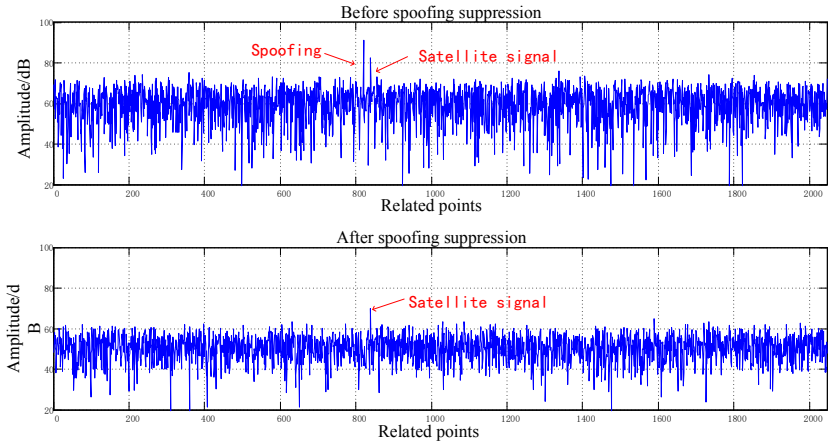

Figure 12. Comparison before and after spoofing suppression (5).

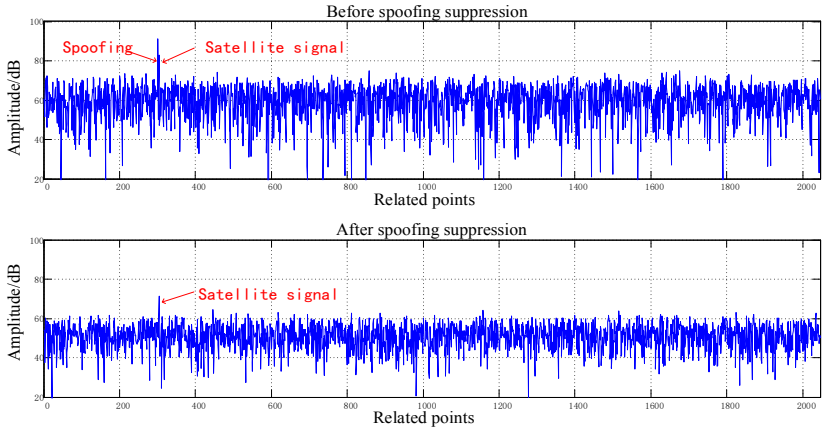

Figure 13. Comparison before and after spoofing suppression (6).

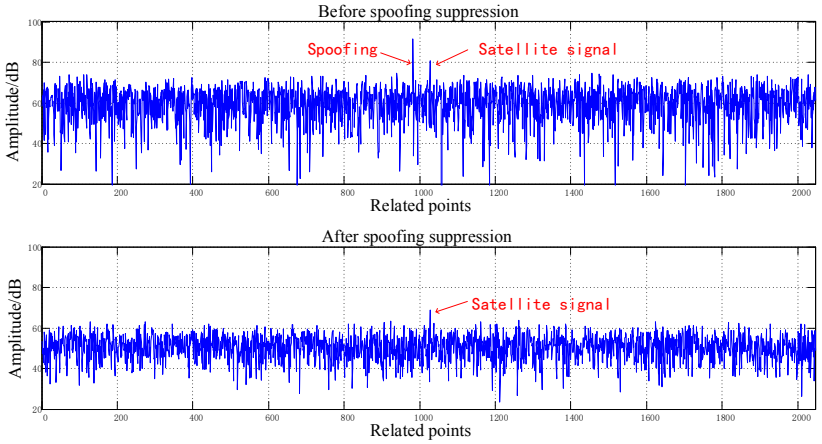

Figure 14. Comparison before and after spoofing suppression (7).

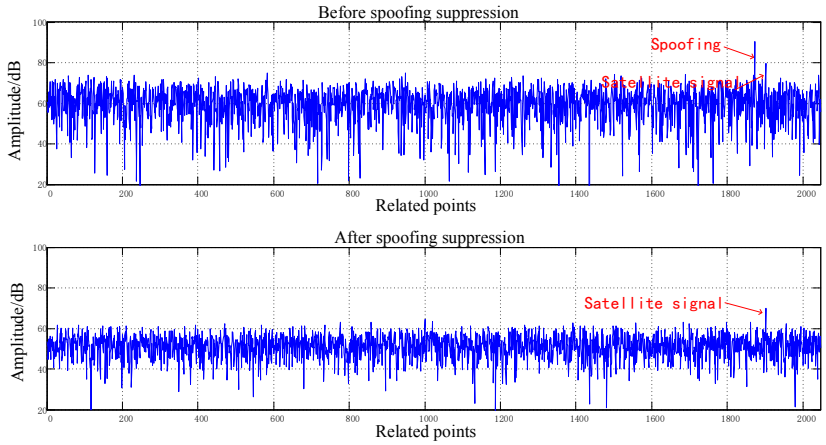

Figure 15. Comparison before and after spoofing suppression (8).

The ASSA can achieve the simultaneous suppression of multiple spoofing interferences. Figures 10–17 show that there were two signals before suppression, a spoofing signal and navigation signals, and that only one navigation signal remained after suppression. Although the algorithm processing process causes the loss of satellite signal energy, the carrier-to-noise ratio is reduced by less than 1 dB, which has little effect on the receiver's acquisition and tracking.

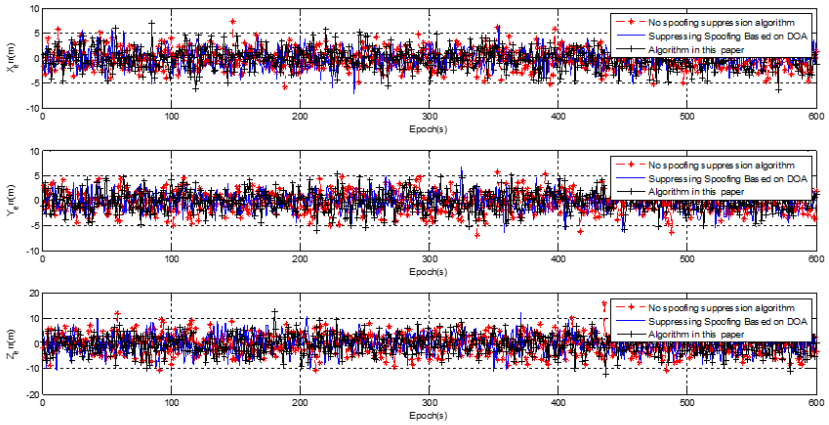

Figure 16. Static positioning error without spoofing.

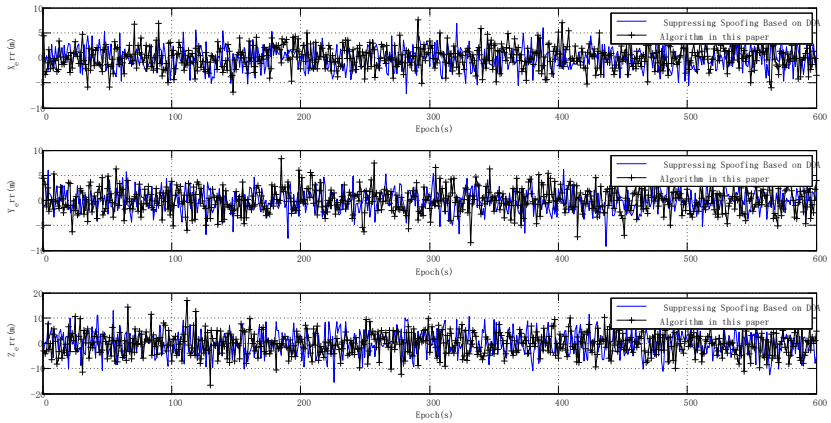

Figure 17. Static positioning error with spoofing.

3.2. Static Test Results

To validate the usability of the ASSA on the positioning performance, the static navigation performance of the general navigation software receiver was compared with the software receiver loaded with the spoofing suppression algorithm based on DOA and the software receiver loaded with the ASSA. In the experiment, the receiving antenna was placed at a known point calibrated in advance, and the coordinates of the local Cartesian coordinate system were (4235045.81 m, 530526.85 m, 97.84 m). Figure 16 shows the static positioning error without spoofing interference.

Without spoofing interference, the navigation signal had little effect on the performance of navigation and positioning after being processed by the two algorithms introduced in this paper. In order to more intuitively evaluate the impact of the two algorithms on positioning performance, mean square error was used. The mean square error of the positioning can be defined as:

$$X_{rmse} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - x_0)^2} \tag{25}$$

$$Y_{rmse} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - y_0)^2} \tag{26}$$

$$Z_{rmse} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(z_i - z_0)^2} \tag{27}$$

where $X_{rmse}$is the positioning mean square errors in the X axis, Y_{rmse} is the positioning mean square errors in the Y axis, Z_{rmse} is the positioning mean square errors in the Z axis, and N is the number of positionings. (x_0, y_0, z_0) is the true coordinate point. (x_i, y_i, z_i) is the ith positioning result. The mean square error of positioning in Figure 16 is shown in Table 1.

Table 1. Static positioning performance without spoofing.

Parameter	No Spoofing		
	No Spoofing Suppression Algorithm	**Suppressing Spoofing Based on DOA**	**Adaptive Spoofing Suppression Algorithm(ASSA)**
X_{rmse}(m)	1.90	1.92	2.20
Y_{rmse}(m)	1.95	1.95	2.13
Z_{rmse}(m)	3.93	3.96	4.11

Without spoofing, the two spoofing suppression algorithms had little impact on navigation and positioning. The algorithm of the spoofing suppression algorithm based on DOA had almost no effect on navigation and positioning. The adaptive spoofing suppression algorithm had an impact on navigation and positioning in the X, Y, Z directions of ≤0.2 m.

With spoofing, the general software receiver without spoofing suppression could not locate signals correctly; therefore, Figure 17 shows the positioning error only after suppression using the two algorithms.

Figure 17 shows the static positioning errors after using the two spoofing suppression algorithms. The receiver could locate signals correctly, and the positioning error did not increase significantly. The mean square error of positioning processed by the two algorithms is shown in Table 2.

Table 2. Static positioning performance with spoofing.

Parameter	Spoofing		
	No Spoofing Suppression Algorithm	**Suppressing Spoofing Based on DOA**	**Adaptive Spoofing Suppression Algorithm(ASSA)**
X_{rmse}(m)	×	2.14	2.22
Y_{rmse}(m)	×	2.29	2.41
Z_{rmse}(m)	×	4.32	4.43

With spoofing, the positioning performance of the spoofing suppression algorithm based on DOA was slightly better than the adaptive spoofing suppression algorithm. The adaptive spoofing suppression algorithm was better than 2.5 m in the horizontal direction and better than 4.5 m in the elevation direction. In the static test, although the positioning performance of the adaptive spoofing suppression algorithm was slightly worse than the spoofing suppression algorithm based on DOA, the calculation and implementation complexity of the adaptive spoofing suppression algorithm were much lower.

3.3. Kinematic Test Results

Figure 5 shows the kinematic test on a curve trajectory during human walking with a receiver from point (530524.69 m, 4235054.23 m, 95.86 m) to point (530579.18 m, 4235094.16 m, 104.10 m), which is shown by the red line in Figure 5. Post real-time kinematic (RTK) with the BeiDou B3 frequency was adopted to assess the positioning performance. The accuracy of the post-processing RTK was better than 5 cm, which meets the needs of dynamic positioning performance comparison. The positioning error for spoofing after suppression using the two algorithms is shown in Figure 18.

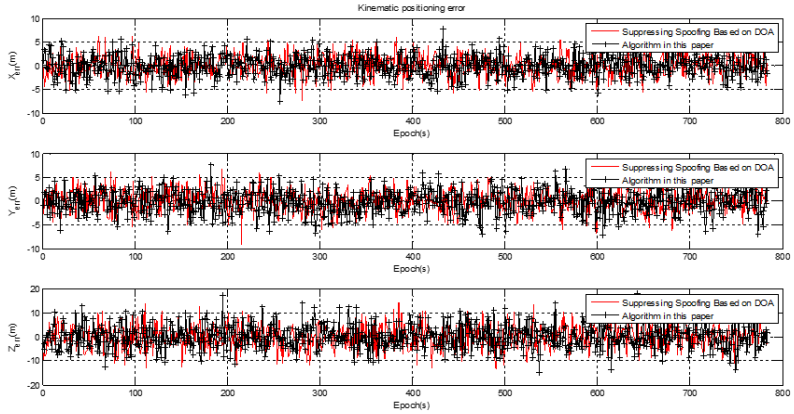

Figure 18. Kinematic positioning error with spoofing.

The kinematic positioning error had no obvious change compared with the static positioning error, which indicates that the adaptive spoofing suppression algorithm was not sensitive to the carrier motion state. The kinematic positioning mean square error is shown in Table 3.

Table 3. Kinematic positioning performance with spoofing.

Parameter	Spoofing		
	No Spoofing Suppression Algorithm	**Suppressing Spoofing Based on DOA Algorithm**	**Adaptive Spoofing Suppression Algorithm(ASSA)**
X_{rmse}(m)	×	2.38	2.27
Y_{rmse}(m)	×	2.27	2.43
Z_{rmse}(m)	×	4.73	4.64

The kinematic positioning error in the X, Y, Z axis direction was (2.38 m, 2.27 m, 4.73 m) for the spoofing suppression algorithm based on DOA, and (2.27 m, 2.43 m, 4.64 m) for the adaptive spoofing suppression algorithm. The positioning performance of the spoofing suppression algorithm based on DOA had no obvious advantage over the adaptive spoofing suppression algorithm. Compared with the static positioning performance, the positioning accuracy was almost unchanged in the horizontal direction, and the positioning accuracy was slightly worse in the elevation direction than in the static. This was caused by the fact that the dilution of precision (DOP) value of the navigation satellite in the elevation direction was worse than in the horizontal direction, and had nothing to do with the algorithm itself.

4. Conclusions

The adaptive spoofing suppression algorithm for GNSS based on a multiple antenna array was been proposed that could utilize the cross-correlation gain of the multiple antenna array to adaptively generate nulling and achieve the simultaneous suppression of multiple spoofing signals. The performance of the proposed algorithm was verified through static and dynamic tests. The results show that: (1) ASSA has a better suppression performance on spoofing, and can form nulls in the direction of spoofing; (2) ASSA has a small impact on navigation and positioning, with positioning errors caused by ASSA less than 0.2 m; (3) after spoofing suppression, the static positioning error in the X, Y, Z axis was (2.22 m, 2.41 m, 4.43 m) for the ASSA, which is worse than the spoofing suppression algorithm based on DOA, but the calculation and implementation complexity of the ASSA were much lower; (4) after spoofing suppression, the kinematic positioning error in the X, Y, Z axis direction was (2.27 m, 2.43 m, 4.64 m) for the ASSA, with a performance similar to the spoofing suppression algorithm based on DOA. The algorithm proposed in this paper is not sensitive to the movement state of the carrier, and has good

positioning performance under both stationary and moving conditions. In the future, this algorithm will be applied to navigation receiving terminals to improve their spoofing countermeasure performances.

Author Contributions: All authors contributed to the manuscript and discussed the results. All authors together developed the idea that led to this paper. G.F. and X.G. conceived the experiments and analyzed the data. B.Y. provided critical comments and contributed to the final revision of the paper. Q.R. and C.S. contributed to the expression and the design of programs. G.F. wrote the manuscript and all the authors participated in amending the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Key Research and Development Plan of China (project: Indoor Hybrid Intelligent Positioning and Indoor GIS Technology (No. 2016YFB0502100, 2016YFB0502101)).

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

References

1. Lechner, W.; Baumann, S. Global navigation satellite systems. *Comput. Electron. Agric.* **2000**, *25*, 67–85. [CrossRef]
2. Grejner-Brzezinska, D.A.; Toth, C.; Moore, T.; Raquet, J.F.; Miller, M.M.; Kealy, A. Multisensor Navigation Systems: A Remedy for GNSS Vulnerabilities? *Proc. IEEE* **2016**, *104*, 1339–1353. [CrossRef]
3. Carroll, J.V. Vulnerability Assessment of the U.S. Transportation Infrastructure that Relies on the Global Positioning System. *J. Navig.* **2003**, *56*, 185–193. [CrossRef]
4. Volpe, J.A. *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*; Technical Report; National Transportation Research Center: Cambridge, MA, USA, 2001.
5. Naval Surface Warfare Center. *Global positioning system impact to critical civil infrastructure (GICCI)*; Technical Report; Mission Assurance Division, Naval Surface Warfare Center: Crane, Indiana, USA, 2009.
6. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
7. Qi, W.; Zhang, Y.; Liu, X. A GNSS anti-spoofing technology based on Doppler shift in vehicle networking. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 725–729.
8. Motella, B.; Pini, M.; Fantino, M.; Mulassano, P.; Nicola, M.; Fortuny-Guasch, J.; Wildemeersch, M.; Symeonidis, D. Performance assessment of low cost GPS receivers under civilian spoofing attacks. In Proceedings of the 2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Rotterdam Netherlands, 8–10 December 2010.
9. Broumandan, A.; Jafarnia-Jahromi, A.; Lachapelle, G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solutions* **2015**, *19*, 475–487. [CrossRef]
10. Nielsen, J.; Broumandan, A.; Lachapelle, G. GNSS Spoofing Detection for Single Antenna Handheld Receivers. *Navig.* **2011**, *58*, 335–344. [CrossRef]
11. Jahromi, A.J.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 181–191. [CrossRef]
12. Hu, Y.; Bian, S.; Cao, K.; Ji, B. GNSS spoofing detection based on new signal quality assessment model. *GPS Solutions* **2018**, *22*, 28. [CrossRef]
13. Zhang, Z.; Zhan, X.; Feng, S.; Ochieng, W.Y. Sensitivity analysis of the vestigial signal defence-based civil GNSS spoofing detection algorithm. *IET Radar Sonar Navig.* **2016**, *11*, 861–872. [CrossRef]
14. Wesson, K.D.; Gross, J.N.; Humphreys, T.E.; Evans, B.L. GNSS Signal Authentication via Power and Distortion Monitoring. *IEEE Trans. Aerosp. Electron. Syst.* **2018**, *54*, 739–754. [CrossRef]
15. Dobryakova, L.A.; Lemieszewski, L.S.; Ochin, E. GNSS Spoofing Detection Using Static or Rotating Single-Antenna of a Static or Moving Victim. *IEEE Access* **2018**, *6*, 79074–79081. [CrossRef]
16. Shafiee, E.; Mosavi, M.R.; Moazedi, M. Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers. *J. Navig.* **2017**, *71*, 169–188. [CrossRef]
17. Han, S.; Luo, D.; Meng, W.; Li, C. Antispoofing RAIM for dual-recursion particle filter of GNSS calculation. *IEEE Trans. Aerosp. Electron. Syst.* **2016**, *52*, 836–851. [CrossRef]
18. Benzerrouk, H.; Nebylov, A.V. Integrated Navigation System INS/GNSS Based on Joint Application of Linear and Nonlinear Filtering. *IFAC Proc. Volumes* **2012**, *45*, 208–213. [CrossRef]
19. Tanil, C.; Khanafseh, S.; Joerger, M.; Pervan, B. An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position. *IEEE Trans. Aerosp. Electron. Syst.* **2018**, *54*, 131–143. [CrossRef]

20. Van Der Merwe, J.R.; Rugamer, A.; Goicoechea, A.F.-D.; Felber, W. Blind Spoofing Detection Using a Multi-Antenna Snapshot Receiver. In Proceedings of the 2019 International Conference on Localization and GNSS (ICL-GNSS), Nuremberg, Germany, 4–6 June 2019; pp. 1–7.
21. 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, 5–8 April 2018; pp. 389–396.
22. Nguyen, V.H.; Falco, G.; Nicola, M.; Falletti, E. A Dual Antenna GNSS Spoofing Detector Based on the Dispersion of Double Difference Measurements. In Proceedings of the 2018 9th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, The Netherlands, 8–10 December 2018; pp. 1–8.
23. Guo, Y.; Fan, M.; Kong, M. Spoofing interference suppression using space-time process for GNSS receiver. In Proceedings of the 2012 5th International Congress on Image and Signal Processing, Chongqing, China, 22–24 October 2012; pp. 1537–1541.
24. Humphreys, T.E. Detection Strategy for Cryptographic GNSS Anti-Spoofing. *IEEE Trans. Aerosp. Electron. Syst.* **2013**, *49*, 1073–1090. [CrossRef]
25. Psiaki, M.L. Spoofing Detection for Civilian GNSS Signals. U.S. Patent 8,712,051, 29 April 2014.
26. Rycroft, M.J. Understanding GPS. Principles and applications. *J. Atmos. Solar-Terrestrial Phys.* **1997**, *59*, 598–599. [CrossRef]
27. Wang, H.; Wan, L.; Dong, M.; Ota, K.; Wang, X. Assistant Vehicle Localization Based on Three Collaborative Base Stations via SBL-Based Robust DOA Estimation. *IEEE Internet Things J.* **2019**, *6*, 5766–5777. [CrossRef]
28. Liu, T.; Wen, F.; Shi, J.-P.; Gong, Z.; Xu, H. A Computationally Economic Location Algorithm for Bistatic EVMS-MIMO Radar. *IEEE Access* **2019**, *7*, 120533–120540. [CrossRef]
29. Li, Z.; Shi, J.-P.; Wang, X.; Wen, F. Joint Angle and Frequency Estimation Using One-Bit Measurements. *Sensors* **2019**, *19*, 5422. [CrossRef]
30. Wang, X.; Wan, L.; Huang, M.; Shen, C.; Zhang, K. Polarization Channel Estimation for Circular and Non-Circular Signals in Massive MIMO Systems. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 1001–1016. [CrossRef]
31. Buckley, K.; Xu, X. Spatial-spectrum estimation in a location sector. *IEEE Trans. Acoust. Speech, Signal Process.* **1990**, *38*, 1842–1852. [CrossRef]
32. Wan, L.; Sun, L.; Kong, X.; Yuan, Y.; Sun, K.; Xia, F. Task-Driven Resource Assignment in Mobile Edge Computing Exploiting Evolutionary Computation. *IEEE Wirel. Commun.* **2019**, *26*, 94–101. [CrossRef]