sensors

MDPI

Article

A Two-Stage Interference Suppression Scheme Based on Antenna Array for GNSS Jamming and Spoofing

Jiaqi Zhang, Xiaowei Cui *, Hailong Xu and Mingquan Lu

Department of Electronic Engineering, Tsinghua University, Beijing 100084, China
* Correspondence: cxw2005@mail.tsinghua.edu.cn; Tel.: +86-10-62773907

Received: 2 August 2019; Accepted: 6 September 2019; Published: 7 September 2019

Abstract: Jamming and spoofing are the two main types of intentional interference for global navigation satellite system (GNSS) receivers. Due to the entirely different signal characteristics they have, a few techniques can deal with them simultaneously. This paper proposes a two-stage interference suppression scheme based on antenna arrays, which can detect and mitigate jamming and spoofing before the despreading of GNSS receivers. First, a subspace projection was adopted to eliminate the high-power jamming signals. The output signal is still a multi-dimensional vector so that the spatial processing technique can be used in the next stage. Then, the cyclostationarity of GNSS signals were fully excavated to reduce or even remove the noise component in the spatial correlation matrix. Thus, the signal subspace, including information of the power and the directions-of-arrival (DOAs) of the GNSS signals, can be obtained. Next, a novel cyclic correlation eigenvalue test (CCET) algorithm was proposed to detect the presence of a spoofing attack, and the cyclic music signal classification (Cyclic MUSIC) algorithm was employed to estimate the DOAs of all the navigation signals. Finally, this study employed a subspace projection again to eliminate the spoofing signals and provide a higher gain for authentic satellite signals through beamforming. All the operations were performed on the raw digital baseband signal so that they did not introduce additional computational complexity to the GNSS receiver. The simulation results show that the proposed scheme not only suppresses jamming and spoofing effectively but also maximizes the power of the authentic signals. Nonetheless, the estimated DOA of spoofing signals may be helpful for the interference source positioning in some applications.

Keywords: Global Navigation Satellite System (GNSS); anti-jamming; spoofing detection; spoofing mitigation; antenna array; subspace projection; Cyclic MUSIC algorithm

1. Introduction

With the extensive application of global navigation satellite systems (GNSS) in both military and civilian fields, the research of navigation countermeasure technology has gained more and more attention. Due to the inherent weakness of the satellite navigation systems, GNSS receivers are susceptible to both intentional and unintentional interference [1,2]. Jamming and spoofing are the two main kinds of intentional interference.

A jammer transmits high-power signals to the target receiver, which is very easy to implement because the power of the satellite signal reaching the ground is weak (about 20–30 dB below the thermal noise). It can degrade the carrier to noise ratio (C/N_0) performance of the victim receiver or even put it into an "unlock" state [3]. Many relatively mature technologies can suppress this type of interference [4–7]. Among them, spatial processing based on an antenna array is considered as the most effective one. It can shape the reception beam pattern of the antenna array to form nulls toward jamming sources, thus the interferences are suppressed [8,9].

Spoofing is a more insidious and damaging interference that aims to mislead the target GNSS receiver to generate an erroneous position and timing solutions without awareness [10]. It can be realized by using a signal generator to counterfeit GNSS signals, namely generator-based spoofing, or by replaying the recorded authentic satellite signals, namely receiver-based spoofing or meaconing. Since the spoofing signals have similar temporal and spectral characteristics to authentic signals, it is more challenging to detect and mitigate such interference. In recent years, an increasing number of research groups have been involved in the study of spoofing countermeasures [11,12]. Most of them focus on spoofing detection based on a single antenna, such as amplitude discrimination [13], polarization discrimination [14], and the time-of-arrival (TOA) discrimination [15]. However, merely detecting the presence of a spoofing attack is not enough, and the ultimate goal of anti-spoofing is to eliminate spoofing signals and recover the positioning and timing capabilities of the victim receiver. The anti-spoofing techniques based on the antenna array, which is rising recently, not only can analyze the spatial signature of the received signals and identify spatially correlated spoofing signals, but also mitigate them by nulling technology [12]. These kinds of techniques can be implemented at the pre-despreading or post-despreading stage of a GNSS receiver. A pre-despreading method in [16] cross-correlated the baseband samples from different antennas in order to form a spatial correlation matrix and extracted the eigenvector corresponding to the maximum eigenvalue as the spoofing subspace. Then, projecting the array signal into its orthogonal subspace mitigated the spoofing signals. The basic idea is that all spoofing signals come from the same direction, the power density of which is higher than the other directions. Although this method has low complexity, it is difficult to determine the detection threshold because the navigation signals arriving at the receiver are generally below the noise level, whether it is an authentic signal or spoofing signal. In the post-despreading methods, the correlation and accumulation processes have been applied to each antenna sample [17,18]. Then, the directions-of-arrival (DOAs) of all the incoming navigation signals are estimated to distinguish between the spoofing and authentic signals. This method can not only ensure the gain of the authentic satellite signals through beamforming [19] while eliminating the spoofing signals, but also provide support for interference source positioning in some applications. Nonetheless, higher computational complexity makes it difficult to put into practice due to a large number of correlators that are needed for the receiver.

It is worth mentioning that there is a more complicated interference scenario where jamming and spoofing coexist. For example, in a confrontational environment, the jamming makes the target receiver loss-of-lock in a short time, and then the spoofing with higher power than the satellite signal leads the receiver to lock onto a false peak during reacquisition. Another possibility is to transmit high-power jamming signals and latent spoofing signals at the same time. Since most receivers on the market have strong capabilities of anti-jamming, this strategy can raise the probability of making the victim receiver fail in its positioning.

For such complex situations, the existing countermeasures are mostly a combination of adaptive spatial filtering based on array antennas and single antenna-based spoofing detection. Some schemes can suppress both jamming and spoofing by spatial processing. The authors in [20] introduced the subspace projection technique to eliminate jamming signals and exploit the despread-respread method to suppress spoofing interference. The despread-respread method [21], as a post-despreading method, requires repeated multi-peak acquisition processes for all pseudo-random noise (PRN) codes, thus increasing the computational burden of the receiver significantly. However, the acquisition threshold is difficult to determine in practice. If the threshold is too large, it can miss the possible false signal. If it is too small, it can be susceptible to multipath effects, resulting in a high false alarm rate. As for the pre-despreading methods, the authors in [22] employed the cross-spectral self-coherence restoral (cross-SCORE) algorithm to mitigate jamming and spoofing signals simultaneously. It presents a new idea that the navigation signal component can be enhanced in the cross-covariance matrix due to the self-coherence of the C/A code. However, the authors found in the simulation that this approach

would fail when periodic jamming occurs, and the spoofing detection performance is sensitive to the location and length of the data block that is selected to estimate the cross-covariance matrix.

This paper aims to propose a novel GNSS interference suppression scheme using an antenna array that can detect and mitigate both jamming and spoofing signals before the despreading process of the receiver and reach a compromise between the computational cost and interference suppression capability. Since the two types of interference have entirely different signal characteristics, a two-stage structure was used to cope with them in turn. In the first stage, the spatial correlation matrix of the received signal is estimated. By performing the eigenvalue decomposition (EVD) on this matrix, the number of jamming signals and the jamming subspace can be easily determined because the jamming power is much higher than the noise level. Then, the array signal is projected into the jamming's orthogonal subspace to eliminate the jamming signals. In the next stage, in order to deal with the spoofing signals with low power, the authors make full use of the cyclostationarity of GNSS signals to construct a cyclic correlation matrix, in which the noise component is significantly reduced or even removed. Thus, the signal subspace, which includes information about the power and DOAs of the GNSS signals, can be obtained before the despreading process. Then, a novel cyclic correlation eigenvalue test (CCET) algorithm is proposed to detect the presence of a spoofing attack, in which a test statistic is calculated based on the principal eigenvalues of the cyclic correlation matrix and then compared to a predefined threshold. The only assumption on this spoofing detection method is that all the spoofing signals are transmitted from a single-antenna source. Afterward, the cyclic music signal classification (Cyclic MUSIC) algorithm is employed to estimate the DOAs of all the navigation signals. Finally, subspace projection is again utilized to eliminate spoofing signals and meanwhile perform beamforming for each authentic satellite signal to overcome the power reduction caused by interference nulls.

The main contributions of this paper can be summarized as follows:

(1) A two-stage GNSS interference suppression scheme is proposed, in which the subspace projection instead of the conventional adaptive spatial filtering technique is adopted to remove jamming signals so that spoofing signals can be detected and mitigated by the spatial processing technology based on the array antenna.
(2) Due to all of the above, the operations are performed on the digitized baseband samples before the despreading process. The proposed technique does not introduce additional computational complexity to the GNSS receiver. Therefore, it is convenient to apply in real systems.
(3) Compared with other anti-spoofing methods implemented at the pre-despreading stage, such as the above-mentioned one [16], the proposed scheme not only suppresses jamming and spoofing effectively but also provides a higher gain in the directions of the desired satellite signal. Nonetheless, the estimated DOA of spoofing signals may be helpful for the interference source positioning in some applications.
(4) The proposed technique is effective only when the number of array elements is higher than the number of signals (include interference and satellite signals). Therefore, a suboptimal scheme is provided for the applications using small arrays, in which the maximum gain requirement for the authentic signals is relaxed to ensure that the jamming and spoofing signals are successfully eliminated.

The rest of this paper is organized as follows. In Section 2, the interference scenario is described and the received signal model is introduced. Then, the two-stage interference suppression scheme is presented in Section 3. In Section 4, the performance of the proposed spoofing detection is evaluated through theoretical analysis and simulation results. In Section 5, more simulation results are provided to validate the proposed scheme in different application scenarios. Section 6 concludes this paper.

2. Signal Model

This paper focuses on the complicated interference scenario where both jamming and spoofing exist. As an example, Figure 1 illustrates an intentional attack on a GNSS receiver mounted on an aerial vehicle. Herein, there are likely one or several jamming sources emitting high-power radio frequency (RF) interference, while the spoofing source generally uses a single-antenna to transmit all the false signals, whether it is generator-based spoofing or receiver-based spoofing.

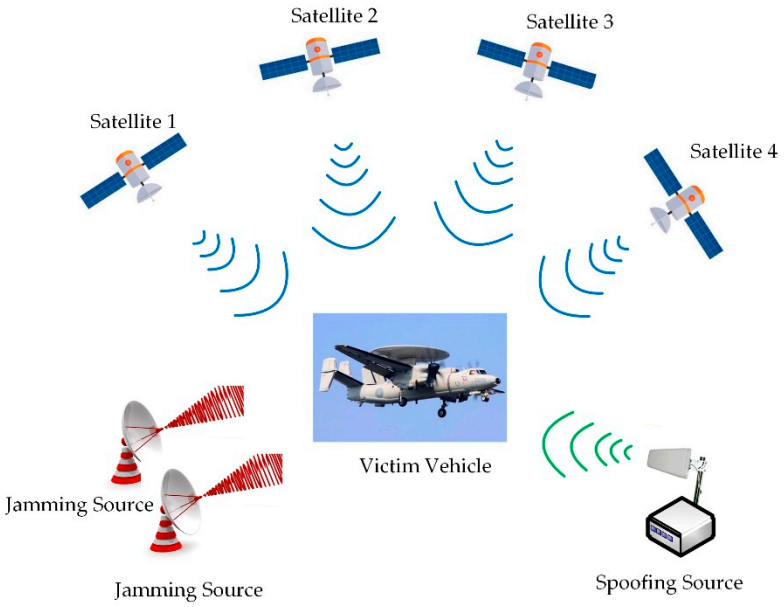


Figure 1. Illustration of an intentional attack on a global navigation satellite system (GNSS) receiver mounted on an aerial vehicle.

2.1. Received Array Signal

Without the loss of generality, it is assumed that M^A authentic satellite signals, M^S spoofing signals and M^J jamming signals arrive at an N-element antenna array. Each element of the antenna array is connected to an RF front end and the resulting baseband sampled signals constitute the $N \times 1$ array signal vector as follows:

$$\mathbf{x}(nT_s) = \sum_{m=1}^{M^A} \mathbf{a}_m^A s_m^A(nT_s) + \sum_{p=1}^{M^S} \mathbf{a}_p^S s_p^S(nT_s) + \sum_{q=1}^{M^J} \mathbf{a}_q^J j_q(nT_s) + \mathbf{n}(nT_s) \tag{1}$$

where T_s is the sampling interval. Each row of $\mathbf{x}(nT_s)$ denotes the received signal by the corresponding array element and $\mathbf{n}(nT_s)$ is a complex additive white Gaussian noise vector. $j_q(nT_s)$ $(q = 1, \cdots M^J)$ represents the jth jamming signal; $s_m^A(nT_s)$ $(m = 1, \cdots M^A)$ denotes the mth authentic satellite signal, $s_p^S(nT_s)$ $(p = 1, \cdots M^S)$ means the pth spoofing signal and

$$\begin{aligned} s_m^A(nT_s) &= \sqrt{P_m^A} D_m^A(nT_s - \tau_m^A) C_m^A(nT_s - \tau_m^A) e^{j2\pi(f_{IF} + f_m^A)nT_s + j\phi_m^A} \\ s_p^S(nT_s) &= \sqrt{P_p^S} D_p^S(nT_s - \tau_p^S) C_p^S(nT_s - \tau_p^S) e^{j2\pi(f_{IF} + f_p^S)nT_s + j\phi_p^S} \end{aligned} \tag{2}$$

in which f_{IF} is the intermediate frequency (IF), symbols P, τ, f, ϕ represent the power, code delay, Doppler frequency and phase of each signal, and the superscripts A, S refer to the authentic satellite and spoofing signal, respectively. $D(nT_s)$ is the navigation data bit and $C(nT_s)$ is the PRN sequence that identifies each satellite. Depending on the type of the spoofing attack, the number of spoofing PRNs can be the same or different from the authentic ones. The differences of the code delay and the Doppler

frequency between the spoofing and authentic signals can be designed optionally. However, the power level of each spoofing signal should be comparable to that of its corresponding authentic one.

In Equation (1), the symbols $\mathbf{a}_m^A$, $\mathbf{a}_p^S$, $\mathbf{a}_q^J$ denote the array steering vectors of the authentic satellite signals, the spoofing signals, and the jamming signals respectively. They describe the carrier phase differences of the received signals from the different antenna channels in specific directions [23]. Figure 2 shows the local antenna coordinate system, in which the x-axis and y-axis lie in the planar array and the z-axis points to the normal direction of the array, forming a right-hand coordinate system. Assume that the direction of the incoming signal is depicted by the angle pair $\boldsymbol{\gamma} = (\theta, \varphi)$, with θ as the angle off the x−y plane and φ as the angle off the x-axis within the x−y plane. The incident direction vector is presented as:

$$\mathbf{g}(\boldsymbol{\gamma}) = -[\cos\theta\cos\varphi, \cos\theta\sin\varphi, \sin\theta]^T \tag{3}$$

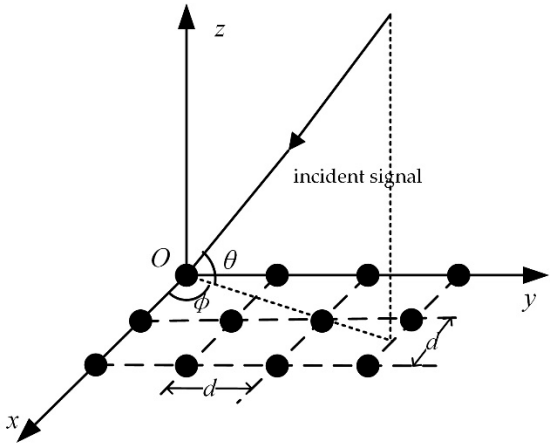


Figure 2. Local antenna coordinate system.

Ideally, the steering vector of this incoming signal can be expressed as follows:

$$\mathbf{a}(\boldsymbol{\gamma}) = \left[e^{-j\frac{2\pi}{\lambda}\mathbf{p}_1^{\mathrm{T}}\mathbf{g}(\boldsymbol{\gamma})}, e^{-j\frac{2\pi}{\lambda}\mathbf{p}_2^{\mathrm{T}}\mathbf{g}(\boldsymbol{\gamma})}, \cdots, e^{-j\frac{2\pi}{\lambda}\mathbf{p}_N^{\mathrm{T}}\mathbf{g}(\boldsymbol{\gamma})}\right]^T \tag{4}$$

where $\mathbf{p}_k = [x_k, y_k, z_k]^T$ $(k = 1, \cdots N)$ is the position vector of the kth element and λ denotes the wavelength of the incident signal.

It can be seen that the signals incident on the array in the same direction have the same steering vector. Therefore, based on the assumption of single-antenna spoofing source, the received signal model in Equation (1) can be rewritten as:

$$\mathbf{x}(nT_s) = \sum_{m=1}^{M^A} \mathbf{a}_m^A s_m^A(nT_s) + \mathbf{a}^S \sum_{p=1}^{M^S} s_p^S(nT_s) + \sum_{q=1}^{M^J} \mathbf{a}_q^J j_q(nT_s) + \mathbf{n}(nT_s) \tag{5}$$

in which $\mathbf{a}^S$ is the same steering vector of all the spoofing signals.

2.2. Cyclostationarity of Global Positioning System (GPS) L1 Signals

It is well known that most GNSS systems employ PRN codes that are derived from linear shift-register sequences owing to their superior correlation properties. Considering the civilian GPS L1 signal, the signal $C(nT_s)$ in Equation (2) is the periodic replication of a specific PRN code sequence of 1023 chips for each satellite [24]. Therefore, each GPS L1 signal exhibits a cyclostationarity at the code period $T_{C/A} = N_c T_c$, where $N_c = 1023$ and $T_c = 1/1.023$ MHz is the chip period.

A signal is considered to be cyclostationary if its cyclic autocorrelation function (CAF), defined as:

$$R_{ss}^{cc}(\tau) = E\{s(t)s^*(t-\tau)\} \tag{6}$$

is non-zero with some lag parameter τ [25]. Note that the CAF in this paper is the abbreviation of the cyclic autocorrelation function rather than the well-known cross-ambiguity function. Due to the periodicity of the PRN codes, the CAF of the individual GPS L1 signal is also periodic and is non-zero when and only when $\tau = lT_{C/A}\,(l = 1, 2, 3, \cdots)$. Therefore, it can be considered as a cyclostationary signal.

It is worth mentioning that the spoofing detection and mitigation technique proposed in this paper is applicable to all the GNSS signals with periodic PRN codes. For convenience, the following section is described in the context of GPS L1 C/A signals.

3. Proposed Interference Suppression Scheme

Figure 3 depicts the block diagram of the proposed interference suppression scheme. It is implemented in two stages, namely jamming suppression and spoofing detection and mitigation. In the jamming suppression module, the spatial covariance matrix of the received signal is firstly estimated. Then, the EVD of the covariance matrix is performed to determine the number of jamming signals and the eigenvectors of the jamming subspace. Finally, subspace projection is used to obtain a jamming-free signal vector. The second stage of this scheme is the detection and mitigation of a spoofing attack. It mainly contains five steps: (1) The cyclic correlation matrix estimation, (2) signal subspace determination, (3) spoofing detection based on the CCET algorithm, (4) DOA estimation and (5) subspace projection and beamforming. All the processing of the proposed scheme is performed on the raw digital baseband signal, and the resulting signals are passed to the despreading and tracking unit of the GNSS receiver for generating authentic PVT solutions. The details of these stages are provided in following subsections.

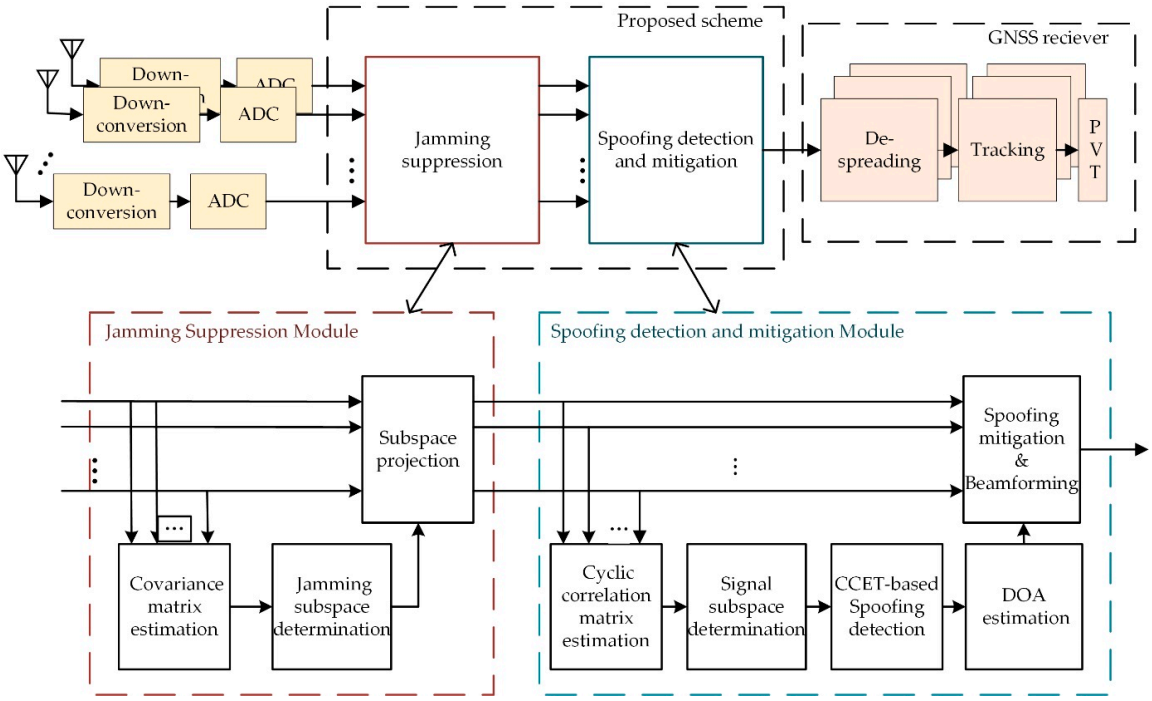


Figure 3. Block diagram of the proposed interference suppression scheme.

3.1. Jamming Suppression

Based on Equation (5), the covariance matrix of the received signal vector can be expressed as follows:

$$\begin{aligned}\mathbf{R}_x &= E\left\{\mathbf{x}(nT_s)\mathbf{x}^H(nT_s)\right\} \\ &= \sum_{q=1}^{M^J} R_q^J(nT_s)\mathbf{a}_q^J(\mathbf{a}_q^J)^H + \sum_{m=1}^{M^A} R_m^A(nT_s)\mathbf{a}_m^A(\mathbf{a}_m^A)^H + \left(\sum_{p=1}^{M^S} R_p^S(nT_s)\right)\mathbf{a}^S\left(\mathbf{a}^S\right)^H + \sigma_n^2\mathbf{I}\end{aligned} \tag{7}$$

which is generally estimated by K samples in practice using the following formula:

$$\hat{\mathbf{R}}_x = \frac{1}{K}\sum_{k=0}^{K-1}\mathbf{x}(kT_s)\mathbf{x}^H(kT_s) \tag{8}$$

In Equation (7),

$$\begin{aligned}R_q^J(nT_s) &= E\left\{s_q^J(nT_s)s_q^{J*}(nT_s)\right\} = P_q^J \\ R_m^A(nT_s) &= E\left\{s_m^A(nT_s)s_m^{A*}(nT_s)\right\} = P_m^A \\ R_p^S(nT_s) &= E\left\{s_p^S(nT_s)s_p^{S*}(nT_s)\right\} = P_p^S\end{aligned} \tag{9}$$

are the values of the autocorrelation function of the jth jamming signal, the mth satellite signal and the pth spoofing signal, respectively, indicating the corresponding signal strength. In most situations, the power of satellite signal is approximately *20~30* dB lower than the noise and the spoofing signal is slightly higher than the authentic signal but still below the noise level, while jamming is usually much stronger than the noise. That is, the power of them satisfies:

$$P_q^J \gg \sigma_n^2 \gg P_p^S \geq P_m^A \tag{10}$$

where $q = 1, \cdots, M^J$, $p = 1, \cdots, M^S$, $m = 1, \cdots, M^A$. Hence, the covariance matrix can be approximated as the sum of the jamming covariance matrix and the noise covariance matrix as follows:

$$\begin{aligned}\hat{\mathbf{R}}_x &\approx \hat{\mathbf{R}}_J + \hat{\mathbf{R}}_n \\ &\approx \sum_{q=1}^{M^J} P_q^J\mathbf{a}_q^J(\mathbf{a}_q^J)^H + \sigma_n^2\mathbf{I}\end{aligned} \tag{11}$$

In order to obtain the jamming subspace, the EVD of the covariance matrix and select corresponding eigenvectors of the M^J largest eigenvalues can be performed. Assume that the EVD of $\hat{\mathbf{R}}_x$ is given by

$$\hat{\mathbf{R}}_x = \sum_{i=1}^{N}\hat{\beta}_i\hat{\mathbf{e}}_i\hat{\mathbf{e}}_i^H \tag{12}$$

where $\hat{\beta}_1, \hat{\beta}_2, \cdots, \hat{\beta}_N$ are the eigenvalues in descending order and $\hat{\mathbf{e}}_1, \hat{\mathbf{e}}_2, \cdots, \hat{\mathbf{e}}_N$ are the normalized eigenvectors. Under the premise that the number of the jamming sources is unknown, we determine the number of the large eigenvalues are determined based on the following criterion [23]

$$\begin{cases}\dfrac{\hat{\beta}_j}{\sum_{i=1}^{N}\hat{\beta}_i} > T_1^J & (j = 1, \cdots, N) \\ \dfrac{\hat{\beta}_{j+1}}{\hat{\beta}_j} > T_2^J & (j = 1, \cdots, N-1)\end{cases} \tag{13}$$

in which T_1^J, T_2^J are the test thresholds. The first metric is the ratio of the jth eigenvalue to the sum of all the eigenvalues, denoting the percent of the total power contained in ... If it exceeds the threshold, $\hat{\beta}_j$ is considered as a large eigenvalue. The second metric is the ratio of the (j + 1) th eigenvalue to

the jth eigenvalue which has been declared to be large. If it is tiny, even approximately zero, then the eigenvalues $\hat{\beta}_k(k = j+1, \cdots, N)$ correspond to the noise subspace.

Then, the number of large eigenvalues is regarded as the dimension of the jamming subspace and the first $\hat{M}^J$ eigenvectors construct the jamming subspace:

$$\begin{cases} \mathbf{V}_J = [\hat{\mathbf{e}}_1, \hat{\mathbf{e}}_2, \cdots, \hat{\mathbf{e}}_{M^J}] & \hat{M}^J \geq 1 \\ \mathbf{V}_J = 0 & \hat{M}^J = 0 \end{cases} \tag{14}$$

Accordingly, the orthogonal complement space to $\mathbf{V}_J$ is defined as:

$$\mathbf{V}_\perp^J = \mathbf{I} - \mathbf{V}_J\left(\mathbf{V}_J^H \mathbf{V}_J\right)^{-1}\mathbf{V}_J^H \tag{15}$$

which meets:

$$\mathbf{V}_\perp^J \mathbf{a}_q^J \approx 0 \, (q = 1, \cdots, M^J) \tag{16}$$

Therefore, projecting the received signal in this orthogonal complement space can suppress jamming and the output signal vector is given by:

$$\begin{aligned} \mathbf{y}(nT_s) &= \mathbf{V}_\perp^J \mathbf{x}(nT_s) \\ &= \sum_{m=1}^{M^A} \mathbf{b}_m^A s_m^A(nT_s) + \mathbf{b}^S \sum_{p=1}^{M^S} s_p^S(nT_s) + \tilde{\mathbf{n}}(nT_s) \end{aligned} \tag{17}$$

where $\mathbf{b}_m^A = \mathbf{V}_\perp^J \mathbf{a}_m^A$, $\mathbf{b}^S = \mathbf{V}_\perp^J \mathbf{a}^S$ denote the new steering vectors of the authentic satellite signal and spoofing signals respectively, and $\tilde{\mathbf{n}}(nT_s) = \mathbf{V}_\perp^J \mathbf{n}(nT_s)$ is the new noise vector. Note that the new steering vector is still an N-dimensional column vector but the subspace projection reduces its spatial degree of freedom (DOF) to be $(N - \hat{M}^J)$.

3.2. Spoofing Detection and Mitigation

In the output of the jamming suppression module, the power of the spoofing signals and satellite signals are still below the noise level. In order to cope with the spoofing signals before the despreading operation of the receiver, the particular characteristics of the GPS signals have to be excavated sufficiently. As mentioned in Section 2, each GPS L1 signal is a cyclostationary sequence that has a periodic cyclic autocorrelation function, and the value of the CAF is non-zero when and only when the lag parameter is $\tau = lT_{C/A}$ $(l = 1, 2, 3, \cdots)$. Therefore, in order to concentrate on the signal components in the spatial correlation matrix and remove the noise component, the cyclic correlation matrix should be calculated, which is defined as the cross-correlation of the received signal vector and its delayed version as follows:

$$\begin{aligned} \mathbf{R}_y^c &= E\left\{\mathbf{y}(nT_s)\mathbf{y}^H(nT_s - T_{c/a})\right\} \\ &= \sum_{m=1}^{M^A} \mathbf{b}_m^A\left(\mathbf{b}_m^A\right)^H R_{m^A m^A}^{cc}(T_{C/A}) + \mathbf{b}^S\left(\mathbf{b}^S\right)^H \sum_{p=1}^{M^S} R_{p^S p^S}^{cc}(T_{C/A}) + \sum_{i=1}^{M^A} \mathbf{b}_i^A\left(\mathbf{b}^S\right)^H R_{i^S i^A}^{cc}(T_{C/A}) \end{aligned} \tag{18}$$

where $T_{c/a}$ is the C/A code period, which is almost equal to 1 ms for each GPS L1 signal without considering the influence of code Doppler.

$R_{m^A m^A}^{cc}(T_{C/A})$ denotes the value of the CAF of the mth $(m = 1, \cdots M^A)$ satellite signal at $T_{c/a}$. Neglecting the navigation data bits, it can be expressed as:

$$\begin{aligned} R_{m^A m^A}^{cc}(T_{C/A}) &= E\left\{s_m^A(nT_s)s_m^{A*}(nT_s - T_{C/A})\right\} \\ &= P_m^A e^{j2\pi(f_{IF} + f_m^A)T_{c/a}} \end{aligned} \tag{19}$$

Similarly,

$$\begin{aligned} R^{cc}_{p^S p^S}(T_{C/A}) &= E\left\{s^S_p(nT_s)s^{S*}_p(nT_s - T_{C/A})\right\} \\ &= P^S_p e^{j2\pi(f_{IF}+f^S_p)T_{c/a}} \end{aligned} \tag{20}$$

is the value of CAF of the pth ($p = 1, \cdots M^S$) spoofing signal at $T_{c/a}$.

Knowing that the Doppler frequency shifts for the baseband GPS signals are generally between −5 kHz and +5 kHz, the following approximation can be made:

$$e^{j2\pi(f_{IF}+f^A_m)T_{c/a}} \approx e^{j2\pi(f_{IF}+f^S_p)T_{c/a}} \approx e^{j2\pi f_{IF}T_{c/a}} \triangleq C_{IF} \tag{21}$$

where C_{IF} is defined as a complex constant, the norm of which is 1. Accordingly, Equation (19), (20) can be simplified to:

$$\begin{aligned} R^{cc}_{m^A m^A}(T_{C/A}) &\approx C_{IF}P^A_m \\ R^{cc}_{p^S p^S}(T_{C/A}) &\approx C_{IF}P^S_p \end{aligned} \tag{22}$$

The last term of Equation (18) is the cross correlation between the satellite and spoofing signals with the same PRN code $C^A_i(t) = C^S_i(t) = C_i(t)$, which can be expressed as:

$$\begin{aligned} R^{cc}_{i^S i^A}(T_{C/A}) &= E\left\{s^A_i(t)s^{S*}_i(nT_s - T_{C/A})\right\} \\ &\approx \sqrt{P^A_i}\sqrt{P^S_i}E\left\{C_i(nT_s - \tau^A_i)C_i(nT_s - \tau^S_i - T_{C/A})\right\}e^{j2\pi(f^A_i - f^A_i)T_{C/A}} \end{aligned} \tag{23}$$

As can be seen, its value depends on the code delay difference and the Doppler frequency difference between the satellite signal and its counterfeit signal. In general, the Doppler frequency difference between the spoofing signal and the corresponding satellite signal is a few Hz, it can be written $\left(f^A_i - f^A_i\right)T_{C/A} \ll 1$ and the phase rotation can be neglected. Equation (23) can be denoted as:

$$R^{cc}_{i^A i^S}(T_{C/A}) \approx \rho^{AS}_{ii}\sqrt{P^A_i}\sqrt{P^S_i} \tag{24}$$

where $\rho^{AS}_{ii}\left(0 \le \rho^{AS}_{ii} \le 1\right)$ is the correlation result of $C_i(nT_s - \tau^A_i)$ and $C_i(nT_s - \tau^S_i - T_{C/A})$. In general, the spoofing signals are designed to be more than one chip delay or advance relative to the authentic signals, and $C_i(nT_s - \tau^A_i)$ and $C_i(nT_s - \tau^S_i - T_{C/A})$ can be considered to be uncorrelated, that is, $R^{cc}_{i^S i^A}(T_{C/A}) = 0$ [24]. However, in some complicated scenarios, the code phase differences may be within one chip, which makes it difficult to distinguish between spoofing and authentic signals by the time-domain methods.

In Equation (18), the cross-correlation matrix of each GPS signal and noise vector and the cross-correlation matrix of the noise vector and its delayed version have been eliminated because the noise is assumed to be Gaussian.

Without the loss of generality, the authors regard spoofing detection as a binary statistical hypothesis testing problem with H_0 denoting the null hypothesis that there is no spoofing attack and with H_1 denoting the null hypothesis that spoofing attack is present. Equation (18) is reformulated as:

$$\mathbf{R}^c_y = \begin{cases} \sum\limits_{m=1}^{M^A}\left(C_{IF}P^A_m\right)\mathbf{b}^A_m\left(\mathbf{b}^A_m\right)^H & H_0 \\ \sum\limits_{m=1}^{M^A}\left(C_{IF}P^A_m\right)\mathbf{b}^A_m\left(\mathbf{b}^A_m\right)^H + \left(C_{IF}\sum\limits_{p=1}^{M^S}P^S_p\right)\mathbf{b}^S(\mathbf{b}^S)^H + \sum\limits_{i=1}^{M^A}\left(\rho^{AS}_{ii}\sqrt{P^A_i}\sqrt{P^S_i}\right)\mathbf{b}^A_i\left(\mathbf{b}^S\right)^H & H_1 \end{cases} \tag{25}$$

As can be observed, when there is no spoofing attack, the rank of the cyclic correlation matrix is equal to the number of satellite signals, i.e., $rank\left(\mathbf{R}^c_y\right) = M^A$. By computing the EVD, M^A non-zero eigenvalues and $(N - M^A)$ zero eigenvalues can be obtained. The first M^A eigenvectors is a set of the orthogonal basis of the signal space spanned by the signal steering vectors $\left\{\mathbf{b}^A_1, \mathbf{b}^A_2, \cdots, \mathbf{b}^A_{M^A}\right\}$,

and the remaining eigenvectors corresponding to the zero eigenvalues form the null space. Therefore, the DOAs of signals can be estimated by the Cyclic MUSIC algorithm [26]. The difference between this algorithm and the traditional MUSIC algorithm is that it uses the cyclic correlation matrix instead of the covariance matrix.

Whereas if a spoofing attack is present, H_1 consists of two cases. (i) When each spoofing signal is off the authentic counterpart by more than one chip in time, the last term in Equation (25) is negligible. The rank of the cyclic correlation matrix becomes $(M^A + 1)$ and the signal subspace contains the steering vectors of satellite signals and spoofing signals as $\left\{\mathbf{b}^S, \mathbf{b}_1^A, \mathbf{b}_2^A, \cdots, \mathbf{b}_{M^A}^A\right\}$. Due to the power of all the spoofing signals are combined in a specific steering vector, there should be a significantly larger eigenvalue in the $(M^A + 1)$ principal eigenvalues. The maximum peak location of the spatial power spectrum estimated by the Cyclic MUSIC algorithm indicates the DOA of the spoofing signals. (ii) When the code phase difference is within one chip, the performance of the Cyclic MUSIC algorithm depends on the correlation between the spoofing and authentic signals. If the spoofing is close to the authentic signal, the high correlation may cause rank deficiency of the signal subspace. In the follow-up simulations, it has been found that when the offset between spoofing and authentic signals is less than the 0.5 chips, the DOA of these signals cannot be estimated accurately. On the other hand, if the offset is more than the 0.5 chips, the correlation between the spoofing and authentic signals is not sufficient to make their DOA indistinguishable. In either case, because each pair of the correlated signals contains a spoofing signal, a significant component can still appear in the principal eigenvalues. The victim can detect the unusual eigenvalue and issue the spoofing alarm.

Therefore, in this section, the focus is on the case of weak correlation and a cyclic correlation eigenvalues test (CCET) algorithm is proposed to detect the presence of a spoofing attack and make the full use of the DOA estimation results to mitigate spoofing signals by subspace projection and enhance the authentic satellite signals through beamforming. The following subsections present the specific steps of the proposed technique.

3.2.1. Cyclic Correlation Matrix Estimation

In practice, the cyclic correlation matrix can not be obtained accurately and has to be estimated by finite samples as follows:

$$\tilde{\mathbf{R}}_y^c = \frac{1}{K}\mathbf{Y}_K\left(\mathbf{Y}_K^D\right)^H \tag{26}$$

where:

$$\mathbf{Y}_K = [\mathbf{y}(k), \mathbf{y}(k-1), \cdots, \mathbf{y}(k-K+1)]$$
$$\mathbf{Y}_K^D = [\mathbf{y}(k-D), \mathbf{y}(k-D-1), \cdots, \mathbf{y}(k-D-K+1)]$$

are the $N \times K$ data matrix and respective delayed matrix, K is the length of the data block and D is the number of samples in one code period (1 ms).

This is the most direct way of estimating the cyclic correlation matrix, which is the most employed in the literature [22]. However, the authors found through the experiments that it might yield poor estimation performance when applied to a real system. This is because the data samples used for cyclic correlation matrix estimation are selected randomly and the length of the data block is limited. Take one of the satellite or spoofing signals as an example, and GPS L1 C/A signal structure is shown in Figure 4. Several pairs of data blocks are marked in the figure, and it is noted that the Data Block G (purple line) is split between two adjacent symbols with opposite signs. If this data block is used for estimating $\widetilde{\mathbf{R}}_y^c$, the correlation result of this signal can be weakened.

This paper solves this problem by using multiple data blocks to get many more correlation matrixes. As shown in Figure 4, G $(1 \le G < 20)$ data blocks are selected and the averaging correlation matrix can be expressed as:

$$\hat{\mathbf{R}}_y^c = \frac{1}{G}\sum_{g=1}^{G}\left(\hat{\mathbf{R}}_y^c\right)^g = \frac{1}{G}\sum_{g=1}^{G}\frac{1}{K}\mathbf{Y}_K^g\left(\mathbf{Y}_K^{gD}\right)^H \tag{27}$$

where

$$\mathbf{Y}_K^g = [\mathbf{y}(k-gD), \mathbf{y}(k-1-gD), \cdots, \mathbf{y}(k-K+1-gD)]$$
$$\mathbf{Y}_K^{gD} = [\mathbf{y}(k-(g+1)D), \mathbf{y}(k-1-(g+1)D), \cdots, \mathbf{y}(k-K+1-(g+1)D)]$$

are the gth data block and the gth delayed data block. For each GPS L1 C/A signal, at most, one pair of these data blocks may suffer from symbol transition, while the others belong to one symbol.

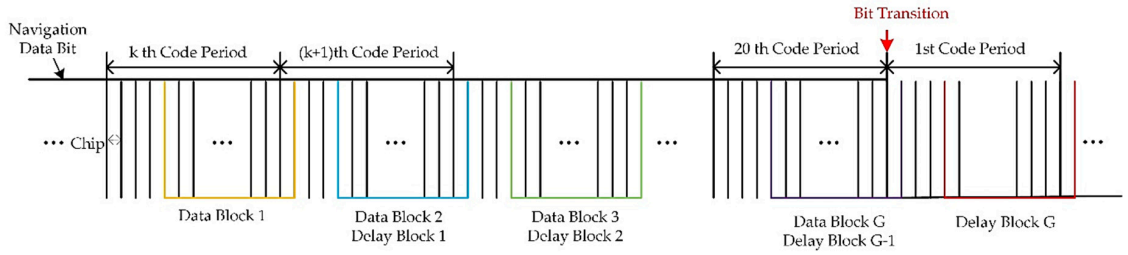


Figure 4. GPS L1 C/A signal structure and the data block for the cyclic correlation matrix estimation.

However, it is worth noting that Equation (27) is generally not Hermitian, resulting in the EVD cannot be performed. It needs to be turned into a conjugate symmetry matrix by:

$$\left(\hat{\mathbf{R}}_y^c\right)^{g*} = \frac{1}{2}\left(\frac{1}{K}\mathbf{Y}_K^g\left(\mathbf{Y}_K^{gD}\right)^H + \frac{1}{K}\mathbf{Y}_K^{gD}\left(\mathbf{Y}_K^g\right)^H\right) \tag{28}$$

which has been proved to have similar statistical properties with $\left(\hat{\mathbf{R}}_y^c\right)^g$ in [27].

Summing up the above, the estimation of the cyclic correlation matrix is given by:

$$\hat{\mathbf{R}}_y^c = \frac{1}{G}\sum_{g=1}^{G}\frac{1}{2K}\left(\mathbf{Y}_K^g\left(\mathbf{Y}_K^{gD}\right)^H + \mathbf{Y}_K^{gD}\left(\mathbf{Y}_K^g\right)^H\right) \tag{29}$$

3.2.2. Signal Subspace Determination

Due to the cyclic correlation matrix is estimated by finite samples, in practice, there are no zero eigenvalues but only small eigenvalues. The dimension of the signal subspace d based on the minimum description length (MDL) criterion [28] needs to be estimated before spoofing detection and DOA estimation. Denoting the EVD of $\hat{\mathbf{R}}_y^c$ as follows:

$$\hat{\mathbf{R}}_y^c = \sum_{i=1}^{N}\hat{\lambda}_i\hat{\mathbf{u}}_i\hat{\mathbf{u}}_i^H \tag{30}$$

where $\hat{\lambda}_1, \hat{\lambda}_2, \cdots, \hat{\lambda}_N$ are the eigenvalues in descending order and $\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2, \cdots, \hat{\mathbf{u}}_N$ are the normalized eigenvectors. The MDL estimator of the signal subspace dimension is given by:

$$\hat{d} = \arg\min_{d=0,\cdots N-\hat{M}^J}\left\{L_d(d) + \frac{1}{2}\left[d\left(N-\hat{M}^J-d\right)+1\right]\ln(GK)\right\} \tag{31}$$

where

$$L_d(d) = GK\left(N-\hat{M}^J-d\right)\ln\left\{\frac{\frac{1}{N-\hat{M}^J-d}\sum_{k=d+1}^{N-\hat{M}^J}\hat{\lambda}_k}{\left(\prod_{k=d+1}^{N}\hat{\lambda}_k\right)^{\frac{1}{N-\hat{M}^J-d}}}\right\} \tag{32}$$

is the log-likelihood function and GK is the number of all samples for estimating $\hat{\mathbf{R}}_y^c$. It is noticeable that the used set of eigenvalues is $\left\{\hat{\lambda}_1, \hat{\lambda}_2, \cdots, \hat{\lambda}_{N-\hat{M}^J}\right\}$ instead of $\left\{\hat{\lambda}_1, \hat{\lambda}_2, \cdots, \hat{\lambda}_N\right\}$. This is because

the jamming suppression module has reduced the rank of the correlation matrix through subspace projection, resulting in the latter $\hat{M}^J$ eigenvalues being negligible.

Then, the first $\hat{d}$ eigenvectors construct the signal subspace:

$$\hat{\mathbf{U}}_S = \begin{bmatrix} \hat{\mathbf{u}}_1 & \hat{\mathbf{u}}_2 & \cdots & \hat{\mathbf{u}}_{\hat{d}} \end{bmatrix} \tag{33}$$

and the remaining $\left(N - \hat{d}\right)$ eigenvectors form the null space:

$$\hat{\mathbf{U}}_N = \begin{bmatrix} \hat{\mathbf{u}}_{\hat{d}+1} & \hat{\mathbf{u}}_{\hat{d}+2} & \cdots & \hat{\mathbf{u}}_N \end{bmatrix} \tag{34}$$

3.2.3. Spoofing Detection Based on the CCET Algorithm

This subsection describes the proposed spoofing detection method based on the distribution of the principal eigenvalues of the cyclic correlation matrix, which is referred to as the CCET algorithm.

As mentioned before, there is a significantly larger eigenvalue in the principal eigenvalues $\left\{\hat{\lambda}_1, \hat{\lambda}_2, \cdots, \hat{\lambda}_{\hat{d}}\right\}$ if the spoofing attack exists. To clarify this point further, two groups of Monte-Carlo simulations were carried out with a 10-element uniform linear array (ULA) under H_0 and H_1. The four satellite signals were considered and the power of each signal was assumed to be –157 dBW. Under H_1, four spoofing signals with the same PRNs as the satellite signals have been assumed and the power of them was also −157 dBW. The code delay and Doppler frequency of each spoofing signals were randomly chosen but not equal to those of authentic signals. The power of additive White Gaussian noise was assumed to be −130 dBW. The run was repeated 1000 times. The normalized eigenvalues under H_0 and H_1 arranged in descending order, are shown in Figure 5.

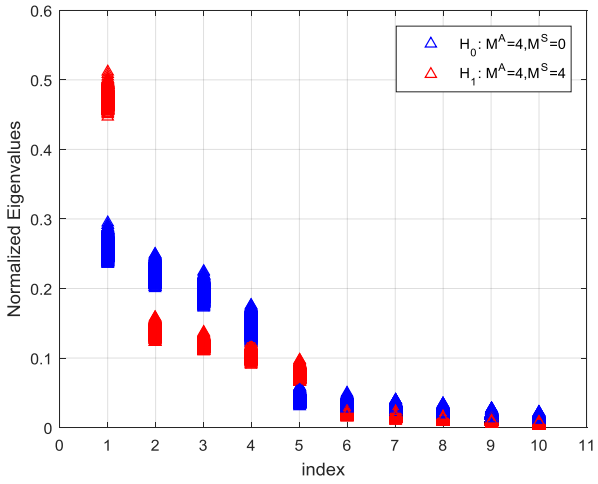


Figure 5. The distribution of the eigenvalues of the cyclic correlation matrix under H_0 and H_1.

As can be seen from the figure, the first four eigenvalues distribute approximately along a straight line concerning their indexes under H_0. In the other case, when several spoofing signals from one specific direction present, their power is superimposed to produce a significantly large eigenvalue, which is no longer consistent with the straight line formed by other ones. If a straight line is found to fit the points of $\hat{\lambda}_i\,(i = 1, \cdots, \hat{d})$ in a least-squares sense, the quality of the obtained solution can be assessed using the sum of squares of errors (SSE), which is defined by:

$$SSE = \sum_{i=1}^{\hat{d}} \left(\hat{\lambda}_i - \widetilde{\lambda}_i\right)^2 \tag{35}$$

where $\widetilde{\lambda}_i$ is the points on the straight line corresponding to $\hat{\lambda}_i$.

Under H_0, the SSE metric follows a non-central chi-squared (χ^2) distribution with $\hat{d}$ degrees of freedom and non-central parameter σ_0, which depends on the variance of the satellite signal power. When the power of all the satellite signals are equal, the residuals of the least- squares solution are unbiased and the SSE metric follows a central χ^2 distribution [29]. Under H_1, the SSE metric follows a non-central χ^2 distribution with the same degrees of freedom $\hat{d}$, but a bigger non-zero parameter σ_1 owing to the largest eigenvalue. Therefore, it is well-reasoned to take the SSE metric of linear fitting as the test statistic of spoofing detection, which follows:

$$T_{sse} \sim \begin{cases} \chi^2\left(\hat{d}, \sigma_0\right) & under\, H_0 \\ \chi^2\left(\hat{d}, \sigma_1\right) & under\, H_1 \end{cases} \tag{36}$$

Then the decision rule can be expressed as:

$$T_{sse} \underset{H_1}{\overset{H_0}{\lessgtr}} \eta \tag{37}$$

where $\eta > 0$ is a threshold chosen to achieve an expected detection performance.

The false alarm probability P_{FA} and the detection probability P_D are vital parameters used to evaluate the performance of detection algorithms. The detection probability is the probability of being under H_1 and accurately detecting the spoofing attack. The false alarm probability is the probability of being under H_0 but mistakenly detecting a spoofing. That is,

$$\begin{aligned} P_D &\triangleq \Pr(T > \eta | H_1) \\ P_{FA} &\triangleq \Pr(T > \eta | H_0) \end{aligned} \tag{38}$$

An optimal threshold is required to improve the detection probability and reduce the false alarm probability as much as possible. In practical applications, the receiver may be up against different spoofing scenarios where the number and power of spoofing signals are unknown and the incoming direction is randomly varied. It is difficult to predict the probability distribution function (PDF) of the test statistic under H_1. Nevertheless, when the H_0 hypothesis is true, the PDF of the test statistic in different scenarios can be obtained where the number and power level of satellite signals are varied but known. Once the PDF under H_0 is determined, given a desired false alarm probability P_{FA}, the detection threshold η can be calculated by satisfying:

$$\int_{\eta}^{\infty} f_{\chi^2}(x, d, \sigma_0) dx = P_{FA} \tag{39}$$

where $f_{\chi^2}(\cdot, d, \sigma_0)$ is the PDF of a χ^2 random variable with degree-of-freedom d and non- central parameter σ_0.

3.2.4. DOA Estimation and Spoofing Mitigation

After the spoofing detection unit, the Cyclic MUSIC algorithm is adopted to estimate the DOAs of the navigation signals. Its basic idea is to estimate the spatial power spectrum by the signal subspace $\hat{\mathbf{U}}_S$ obtained from the cyclic correlation matrix as follows:

$$Q(\boldsymbol{\gamma}) = \frac{1}{\mathbf{v}(\boldsymbol{\gamma})\left(\mathbf{I} - \hat{\mathbf{U}}_S \hat{\mathbf{U}}_S^H\right)\mathbf{v}^H(\boldsymbol{\gamma})} \tag{40}$$

in which $\mathbf{v}(\boldsymbol{\gamma}) = \mathbf{P}_{\perp}^{J}\mathbf{a}(\boldsymbol{\gamma})$ is the steering vector of an incoming signal from $\boldsymbol{\gamma} = (\theta, \varphi)$, and then search for its $\hat{d}$ largest peaks. In the spatial power spectrum, the location of the ith peak $\hat{\boldsymbol{\gamma}}_i = (\hat{\theta}_i, \hat{\varphi}_i)$ denotes the DOA of the ith signal and the value of the peak indicates the power density in that direction.

Depending on the result of spoofing detection, the subsequent process is distinct in the following two cases:

- Assume that H_1 is true

The location of the largest peak $\hat{\boldsymbol{\gamma}}_1 = (\hat{\theta}_1, \hat{\varphi}_1)$ denotes the DOA of the spoofing signals and the spoofing steering vector can be estimated as follows:

$$\hat{\mathbf{b}}^{S} = \mathbf{P}_{\perp}^{J}\mathbf{a}(\hat{\boldsymbol{\gamma}}_1) \tag{41}$$

In the same way, the steering vectors of $\left(\hat{d}-1\right)$ authentic satellite signals are obtained by:

$$\hat{\mathbf{b}}_i^{A} = \mathbf{P}_{\perp}^{J}\mathbf{a}(\hat{\boldsymbol{\gamma}}_{i+1}) \quad (i = 1, \cdots, \hat{d}-1) \tag{42}$$

Similar to the subspace projection method in Section 3.1, spoofing interference can be eliminated by projecting the array signal vector onto the null space of the spoofing subspace. The projection matrix is calculated by:

$$\mathbf{P}_{\perp}^{S} = \mathbf{I} - \frac{\hat{\mathbf{b}}^{S}(\hat{\mathbf{b}}^{S})^{H}}{(\hat{\mathbf{b}}^{S})^{H}\hat{\mathbf{b}}^{S}} \tag{43}$$

Furthermore, to reduce unavoidable attenuation on the array pattern in the directions of authentic satellite signals due to jamming and spoofing nulls, the power of each authentic signal is maximized individually by beamforming. The array weight vector for the ith authentic satellite signals can be represented by:

$$\mathbf{w}_i^{H} = \left(\hat{\mathbf{b}}_i^{A}\right)^{H}\mathbf{P}_{\perp}^{S} \tag{44}$$

and the final output of the ith signal channel is given by:

$$\mathbf{z}_i(nT_s) = \mathbf{w}_i^{H}\mathbf{y}(nT_s) \tag{45}$$

- Assume that H_0 is true

The locations of the $\hat{d}$ peak indicate the DOAs of the authentic satellite signals and the corresponding estimated value of the steering vectors is expressed as follows:

$$\hat{\mathbf{b}}_i^{A} = \mathbf{P}_{\perp}^{J}\mathbf{a}(\hat{\boldsymbol{\gamma}}_i) \quad (i = 1, \cdots, \hat{d}) \tag{46}$$

The spoofing mitigation is no longer required in this case and the array weight vector in Equation (44) becomes:

$$\mathbf{w}_i^{H} = \left(\hat{\mathbf{b}}_i^{A}\right)^{H} \tag{47}$$

3.3. Overall Interference Suppression Scheme

To summarize the proposed multiple interference suppression scheme, all the steps are listed in Algorithm 1.

Algorithm 1 Multiple Interference Suppression Scheme

Jamming Suppression
Input: $\mathbf{x}(nT_s)$

(1) Estimate the spatial covariance matrix $\hat{\mathbf{R}}_x = \frac{1}{K}\sum_{k=0}^{K-1}\mathbf{x}(kT_s)\mathbf{x}^H(kT_s)$.
(2) Compute the EVD of $\hat{\mathbf{R}}_x$, and obtain the jamming subspace $\mathbf{V}_J$ and its orthogonal subspace $\mathbf{P}_\perp^J$.
(3) Project the received signal onto the jamming-free subspace $\mathbf{y}(nT_s) = \mathbf{P}_\perp^J\mathbf{x}(nT_s)$.

Output: $\mathbf{y}(nT_s), \mathbf{P}_\perp^J, M^J$

Spoofing Detection and Mitigation
Input: $\mathbf{y}(nT_s), \mathbf{P}_\perp^J, M^J$

(1) Estimate the cyclic correlation matrix by Equation (28).
(2) Compute the EVD of $\hat{\mathbf{R}}_y^c$ and obtain the eigenvalues and eigenvectors of the signal subspace $\hat{\lambda}_i, \hat{\mathbf{u}}_i\left(i = 1, \cdots, \hat{d}\right)$.
(3) Compute the test statistic T_{sse} based on the CCET algorithm.
(4) Decision. If $T_{sse} > \eta$, then the spoofing signals exist; otherwise, there is no spoofing signal.
(5) Estimate the spoofing steering vector $\hat{\mathbf{b}}^S$ and the authentic steering vectors $\hat{\mathbf{b}}_i^A (i = 1, \cdots, \hat{d} - 1)$ by the Cyclic MUSIC algorithm.
(6) Compute the array weight vector for each satellite signal $\mathbf{w}_i^H = \left(\hat{\mathbf{b}}_i^A\right)^H \mathbf{P}_\perp^S$ (under H_1) or $\mathbf{w}_i^H = \left(\hat{\mathbf{b}}_i^A\right)^H$ (under H_0)
(7) Obtain the output signal $\mathbf{z}_i(nT_s) = \mathbf{w}_i^H\mathbf{y}(nT_s)$

Output: $\mathbf{z}_i(nT_s)$

3.4. Countermeasure in the Case of Small Arrays

Notably, the above method is proposed under the premise that the number of array elements is higher than the number of signals (include interference and satellite signals). That is to say, after jamming the suppressing module, the remaining degree of freedom is still higher than the number of other signals so that the DOAs of the satellite signals and the spoofing signals can be obtained. However, in some small or agile applications, it may be not possible to install a large enough array. Under the circumstances, the requirement for the gain of the authentic signal must be relaxed to ensure that the spoofing signals are successfully eliminated.

When the EVD of $\hat{\mathbf{R}}_y^c$ contains $\hat{d} = N - M^J$ non-zero eigenvalues, it denotes the inability to obtain the number of the signal sources and estimate their directions accurately. In this case, only spoofing signals can be detected by observing whether there is a relatively large eigenvalue. Similar to jamming detection, the authors predicate the existence of the spoofing attack if the largest eigenvalue satisfies:

$$\begin{cases} \frac{\hat{\lambda}_1}{\hat{\lambda}_2} > T_1^S & (a) \\ \frac{\hat{\lambda}_1}{\sum_{i=1}^{N-M^J}\hat{\lambda}_i} > T_2^S & (b) \end{cases} \tag{48}$$

where T_1^S, T_2^S are the test threshholds. It is worth mentioning that the spoofing detection performance of this method is superior to that of the traditional pre-despreading technique. As the noise component has been greatly attenuated by the cyclic correlation process, the eigenvalues of $\hat{\mathbf{R}}_y^c$ directly reflect the percent of the signal power in a specific direction in the total power.

Then project the array signal vector onto the null space of the spoofing subspace, and the final output is given by:

$$z(t) = \mathbf{w}_S^H\mathbf{P}_\perp^S\mathbf{y}(t) \tag{49}$$

where $\mathbf{P}_{\perp}^{S} = \mathbf{I} - \hat{\mathbf{u}}_1 \hat{\mathbf{u}}_1^{H}{}_1$ is the projection matrix for spoofing mitigation and $\mathbf{w}_S = [1, 0, \cdots, 0]^H$ denotes the weight vector resulting in the quiescent beam pattern [22], with the value of *1* corresponding to the reference element.

4. Performance Evaluation of the Spoofing Detection Method

In the proposed scheme, the jamming suppression module is simple in principle and significantly effective, while the spoofing detection and mitigation module is implemented in multiple steps and each step may involve errors when applied to real systems. In this section, both theoretical analysis and simulation results are presented to evaluate the performance of the proposed spoofing detection method.

The common simulation parameters are given as follows. A 10-element ULA was employed and the spacing between adjacent elements was half signal wavelength. The authentic and spoofing signals were generated with a Matlab-based GPS L1 C/A signal generator and they were sampled at a rate of 5 MHz. The additive Gaussian noise on each antenna was assumed to be white with spectral density N_0 = −204 dBW/Hz. The power of authentic and spoofing signals varied based on the simulation scenarios.

4.1. Finite-Sample Effect on the Cyclic Correlation Matrix Estimation

In Section 3.2.2, the authors explained that the estimation performance of the cyclic correlation matrix can be improved by using multiple pairs of data blocks. In essence, it can be proved [30] that $\hat{\mathbf{R}}_y^c$ in Equation (29) is an asymptotically unbiased estimator of $\mathbf{R}_y^c$ and:

$$E\left\{\hat{\mathbf{R}}_y^c\right\} = (1-\rho)\mathbf{R}_y^c \tag{50}$$

$$E\left\{\hat{\mathbf{R}}_y^c \hat{\mathbf{R}}_y^{c\,H}\right\} = \left(1 + \left(\frac{2}{G} - 2\right)\rho\right)\left(\frac{N\left(N + \widetilde{\sigma}^2\right)}{K}\mathbf{R}_y^c + \frac{N\left(1 + \widetilde{\sigma}^2\right)}{K}\mathbf{I}\right) \tag{51}$$

On the right-hand side of Equation (51) is the expected cyclic correlation matrix multiplied by a constant and $\rho = T_{code}/T_{nav}$, in which T_{code} and T_{nav} denote the periods of the PRN code and the navigation data bit. For GPS L1 C/A signal, $T_{nav} = 20T_{code}$. This attenuation coefficient $(1-\rho)$ is due to the term cancellation when one of the G $(1 \le G < 20)$ data blocks split between the two adjacent navigation symbols with opposite signs.

Assume that:

$$\hat{\mathbf{R}}_y^c = (1-\rho)\mathbf{R}_y^c + \mathbf{N} \tag{52}$$

$\mathbf{N}$ is a zero-mean error matrix, the variance of which can be expressed as:

$$\mathrm{var}\{\mathbf{N}\} = \left(1 + \left(\frac{2}{G} - 2\right)\rho\right)\left(\frac{N\left(N + \widetilde{\sigma}^2\right)}{K}\mathbf{R}_y^c + \frac{N\left(1 + \widetilde{\sigma}^2\right)}{K}\mathbf{I}\right) - (1-\rho)^2 \mathbf{R}_y^c \mathbf{R}_y^{c\,H} \tag{53}$$

The above equation reveals that the estimation accuracy increases with the number of data blocks used G and the number of samples per data block K.

Compared with the matrix $\hat{\mathbf{R}}_y^c$, greater concern is warranted for its EVD result. In subsequent processes, the eigenvalues were used to determine the signal subspace dimension d and detect a spoofing attack, and the eigenvectors were for the DOA estimation. Herein, the simulation results are provided to illustrate the influence of the value of G and K on the estimation accuracy of the signal number and DOA.

For simplicity, the case is considered when there is no interference. Assume that four satellite signals are considered with the same power –157 dBW. The Monte Carlo simulations have been performed 1000 times, in which the DOAs of signals were changed randomly from 0° to 180°, while the

initial phases of signals were selected randomly. In each trial, the cyclic correlation matrixes were estimated under different values of G and K to determine the signal subspace dimension and DOAs. Figure 6 shows the probability of correct signal subspace dimension estimation versus the data block number for the different sample number per data block. Figure 7 presents the root-mean-square-error (RMSE) of the DOA estimation results under the different values of G and K. The estimation accuracy of the subspace dimension can be seen, but also, the DOA estimation performance is shown to improve as G and K increase. When *G* is large enough, the performance gain of a larger *K* is not so obvious. However, the increase of G also means that more sample buffering is needed. Therefore, when this technique applies in the real system, the proper values of *G* and *K* should be selected according to the actual situation to achieve a compromise between algorithm performance and computational complexity.

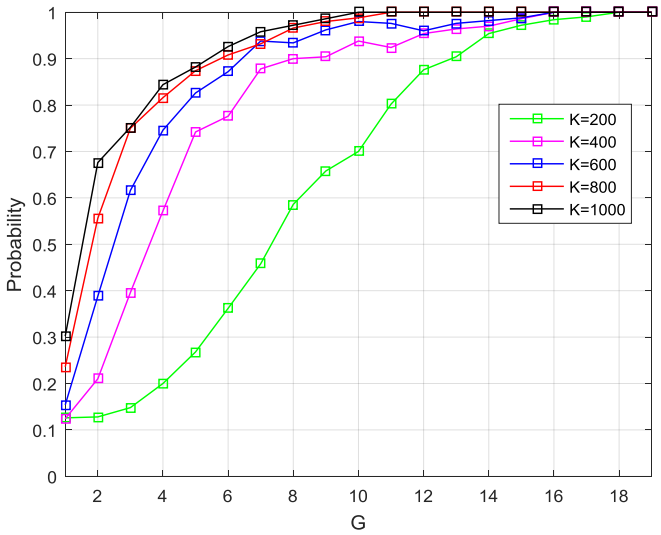


Figure 6. Probability of correct signal subspace dimension estimation versus G for different *K*.

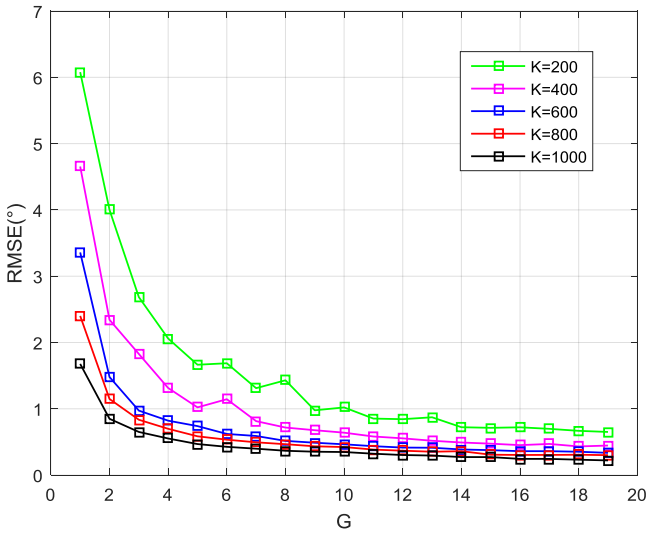


Figure 7. The root-mean-square-error (RMSE) of the directions-of-arrival (DOA) estimation versus G for different *K*.

4.2. Spoofing Detection Performance

In Section 3.2.3, the CCET algorithm was proposed to detect the presence of the spoofing attack. Herein, the performance of the proposed method is evaluated through simulations. These include:

(1) The determination of the detection threshold with a given false alarm probability. (2) The influence of the number and power of spoofing signals on the detection probability.

4.2.1. Determination of the Detection Threshold

Considering the situation of no spoofing attack, three groups of Monte Carlo simulations were performed to predict the PDF of the proposed test statistic under different signal numbers. The number of satellite signals was assumed to be $M^A = 4, 5, 6$, respectively. In each group of simulations, two cases were considered. In one case, it was assumed that the power of each authentic signal was equal and set to be –157 dBW, which indicated the non-central parameter $\sigma_0 = 0$ in Equation (36). In the other case, the power of each signal was randomly chosen between –158 dBW to –156 dBW, which is more coincident with the real situations.

The empirical PDFs of the obtained SSE metrics in Equation (35) for different signal number are shown in Figure 8. Then, the detection threshold for a given false alarm probability can be calculated by Equation (39). Table 1 shows the threshold values corresponding to different P_{fa} at different values of M^A, σ_0.

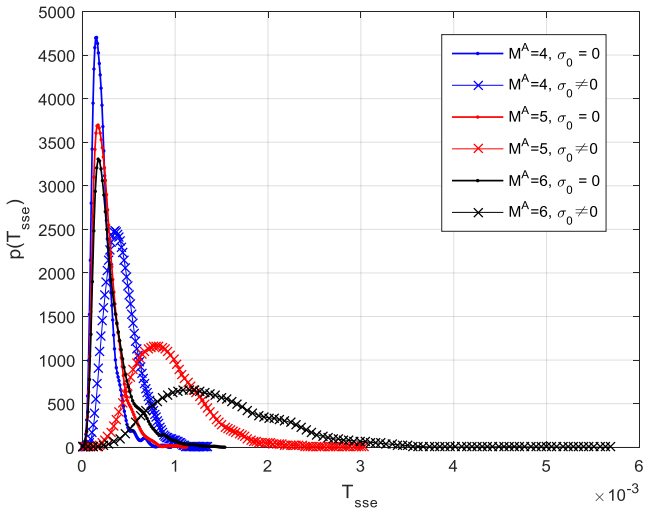


Figure 8. Empirical probability distribution functions (PDFs) of the *SSE* metrics for different signal numbers.

Table 1. Detection thresholds for given P_{fa} with different M^A, σ_0.

		$P_{fa} = 10^{-1}$	$P_{fa} = 10^{-2}$	$P_{fa} = 10^{-3}$	$P_{fa} = 10^{-4}$	$P_{fa} = 10^{-5}$
$M^A = 4$	$\sigma_0 = 0$	0.38×10^{-3}	0.66×10^{-3}	0.87×10^{-3}	0.91×10^{-3}	0.94×10^{-3}
	$\sigma_0 \neq 0$	0.68×10^{-3}	0.96×10^{-3}	1.15×10^{-3}	1.29×10^{-3}	1.32×10^{-3}
$M^A = 5$	$\sigma_0 = 0$	0.45×10^{-3}	0.73×10^{-3}	1.01×10^{-3}	1.11×10^{-3}	1.11×10^{-3}
	$\sigma_0 \neq 0$	1.44×10^{-3}	2.12×10^{-3}	2.64×10^{-3}	2.89×10^{-3}	2.98×10^{-3}
$M^A = 6$	$\sigma_0 = 0$	0.61×10^{-3}	1.04×10^{-3}	1.38×10^{-3}	1.48×10^{-3}	1.52×10^{-3}
	$\sigma_0 \neq 0$	2.41×10^{-3}	3.45×10^{-3}	4.99×10^{-3}	5.46×10^{-3}	5.64×10^{-3}

4.2.2. Probability of Spoofing Detection

Once the detection threshold values were determined, the next simulations were conducted to evaluate the probability of spoofing detection. It was assumed that the number of spoofing signals was equal to that of the authentic signals and each spoofing signal had the same PRN code as the corresponding authentic signal. The power of each authentic satellite was –157 dBW and the spoofing power varied from –163 dBW to –154 dBW. The code phase difference between each spoofing signal and their authentic counterpart was randomly chosen from 150 m to 600 m, and the Doppler frequency differences were all set as 10 Hz.

In each trial of Monte Carlo simulations, the test statistic was calculated and compared to the predefined threshold value, which satisfies $P_{fa} < 10^{-5}$. Figure 9 shows the probability of the spoofing detection as a function of the power ratio of spoofing to the authentic signal. It is observed that when the signal number is 4, 5, 6, the presence of spoofing signals starts to be detected as soon as the power ratio of spoofing to the authentic signal exceeds −3 dB, −4 dB, −5 dB, respectively. This is because the spoofing signals come from the same direction and the total power is higher than the power of each authentic signal. As the spoofing power increases, the detection performance of the proposed method increases as well. Notably, once the power of the spoofing signals exceeds the power of the authentic ones, the probability of spoofing detection in all scenarios exceeds 99%.

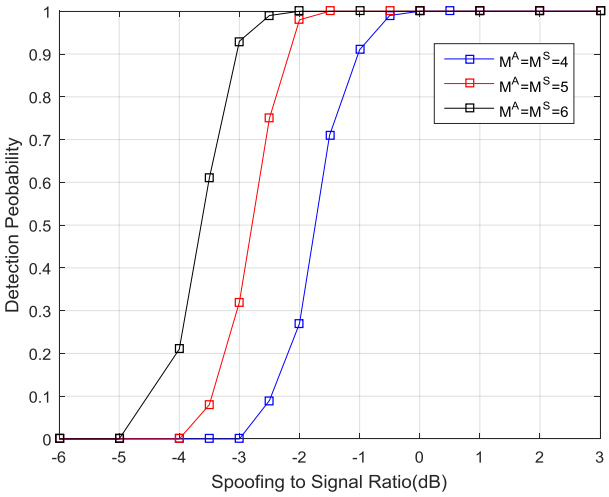


Figure 9. Spoofing detection probability with the power ratio of spoofing to the authentic signal.

5. Simulation Results

In this section, more simulation results have been provided to demonstrate the effectiveness of the proposed interference suppression scheme in different application scenarios.

- Scenario 1:

In the first experiment, a uniform linear array was used, in which ten omnidirectional antennas were arranged in a straight line and the spacing between adjacent elements was half of a GPS L1 wavelength. Five authentic satellite signals PRN2, PRN5, PRN8, PRN19 and PRN26 were transmitted from the direction at the azimuth of −50°, −30°, 0°, 20° and 70° with the power assumed to be −157 dBW. There were two interference sources. One source transmitted five spurious signals PRN2, PRN5, PRN8, PRN19 and PRN26 from the direction at azimuth of 50°. The power of each spoofing signal was 3 dB higher than the authentic signal. The code phase differences between the spoofing signals and their authentic counterparts were all set as 150 m (about 0.5 chips) and the Doppler frequency differences were set as 10 Hz. The other source emitted the jamming signal from the direction at the azimuth of −5°. The jamming-to-signal power ratio (J/S) was assumed to be 60 dB. The additive Gaussian noise on each antenna was assumed to be white with spectral density −204 dBW/Hz. The bandwidth of the receiver, as well as the I/Q sampling frequency, was set to be 5 MHz. The recorded data length was 120 s and the proposed interference suppression scheme was executed every 1 second. The relevant results are as follows.

After the subspace projection in the first stage, the output signal passed to the acquisition process of a GPS receiver to verify the jamming suppression effect. The acquisition result shows that five PRN signals are captured. For example, the correlation result for PRN2 is presented in Figure 10. It can be seen that there are two distinct correlation peaks, one for the authentic satellite signal and the other

for the spoofing signal. It means that jamming has been removed from the received signal. As the spoofing signal has a higher power, a normal GNSS receiver can track it instead of the right signal.

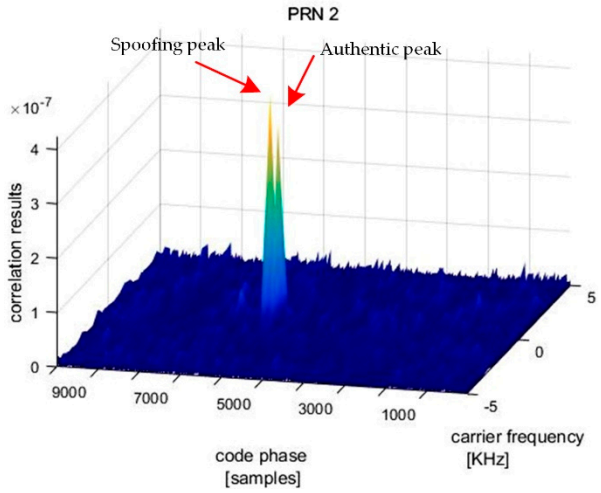


Figure 10. Correlation result of the receiver for PRN2 after jamming suppression.

In the spoofing detection and mitigation module, $G = 9$ data blocks were first selected, each of which contains $K = 1000$ samples, to estimate the cyclic correlation matrix. Then, the eigenvalues of this matrix are used to determine the number of signal sources based on the MDL criterion. For $d \in \{0, 1, \cdots, 9\}$, the resulting values of the *MDL(d)* are shown in Table 2. The minimum of the MDL is obtained, as expected, at $\hat{d} = 6$.

Table 2. The corresponding values of the *MDL* function for different d.

d	0	1	2	3	4	5	6	7	8	9
MDL(d)	801.3	673.7	553.7	424.1	356.8	314.1	298.7	320.8	335.5	345.3

Therefore, the first $\hat{d} = 6$ eigenvalues are used for spoofing detection. Then, the CCET algorithm is used to calculate the test statistic, which is shown in Figure 11. It illustrates that the spoofing attack is successfully detected every epoch. Then, the first $\hat{d} = 6$ eigenvectors construct the signal subspace to estimate the spatial power spectrum and the result is shown in Figure 12. The dashed lines represent the real DOAs of the authentic satellite signals, and the solid line represents the spoofing DOA. It shows that the Cyclic MUSIC algorithm can estimate the directions of all the signal sources effectively and the location of the maximum peak aligns with the spoofing DOA.

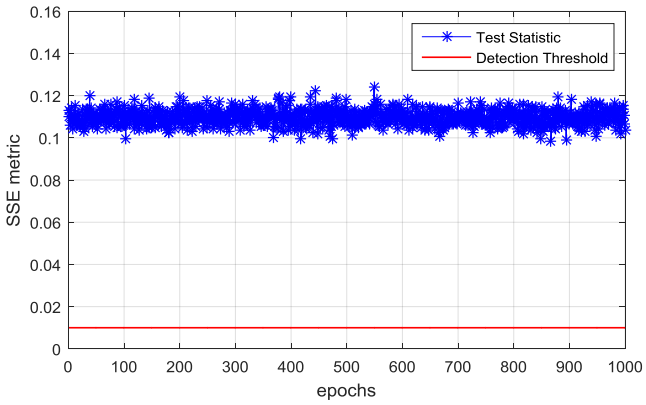


Figure 11. Comparison between the test statistic calculated by the cyclic correlation eigenvalue test (CCET) algorithm and the spoofing detection threshold.

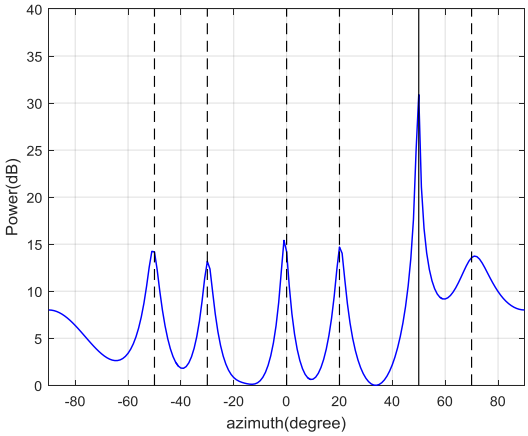


Figure 12. Estimated spatial spectrum of the jamming-free signal by Cyclic MUSIC algorithm.

Based on the above results, the final weight vector for each authentic satellite signal can be calculated by Equation (37) and the antenna beam patterns are shown in Figure 13. It demonstrates that the proposed interference suppression scheme can form nulls in the directions of spoofing and jamming, while the authentic satellite signal gets the maximum gain. Figure 14 shows the correlation result for PRN2 of the output signal, in which only the authentic peak is present.

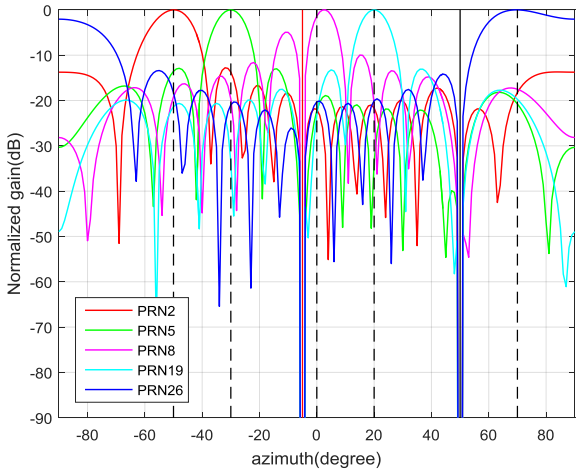


Figure 13. Beam pattern for each authentic satellite using obtained weight vectors.

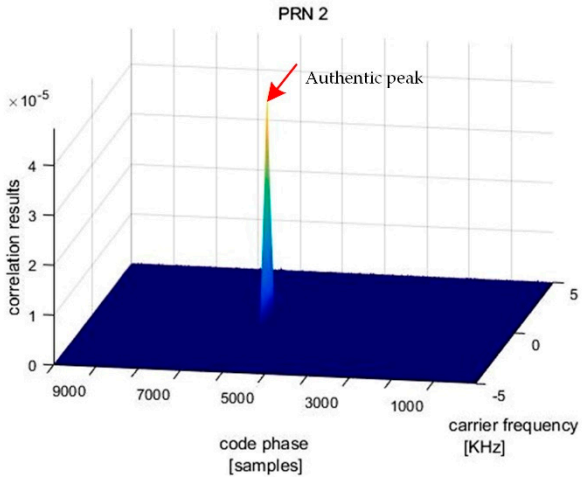


Figure 14. Correlation result for PRN2 after spoofing detection and mitigation.

- Scenario 2:

In Section 3, an alternative spoofing suppression scheme was provided when the number of array elements is less than the number of all the incoming signals (include jamming, spoofing and satellite signals). Herein, the feasibility of this method was verified by simulation. In this experiment, the ten-element ULA was still employed and the number of satellite signals was set to seven. Two jamming sources transmitted high power interferences from different directions. One spoofing source emitted seven spurious signals with the same PRNs as the authentic satellite. The PRN and DOA information of these signals are given in Table 3. The other parameters are the same as the values in Scenario 1.

Table 3. Simulation parameters of the signal sources.

	Sat1	**Sat2**	**Sat3**	**Sat4**	**Sat5**	**Sat6**	**Sat7**	**Spoofing**	**Jam1**	**Jam2**
PRN	2	5	8	19	21	26	29	[2,5,8,19,21,26,29]		
DOA	−50°	−30°	0°	20°	40°	70°	−70°	50°	−5°	5°

The simulation results show that, in this scenario, the jamming signals can be detected and eliminated successfully in the first stage. In the spoofing detection module, the values of the *MDL(d)* are shown in Table 4. It can be seen that the *MDL(d)* is a monotonically decreasing function so that the number of signal sources cannot be determined. In this case, the eigenvector corresponding to the largest eigenvalue is regarded as the spoofing subspace and projects the array signal onto its null space. Figure 15 shows the final beam pattern after two projections. It turned out that the proposed method can eliminate jamming and spoofing signals in the case of a small array. Since the beamforming for each satellite cannot be performed, the authentic signals may be attenuated more or less.

Table 4. The values of the *MDL(d)* in the case of a small array.

d	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
MDL(d)	1033.5	633.1	625.7	615.1	603.8	584.7	566.8	557.5	475.9

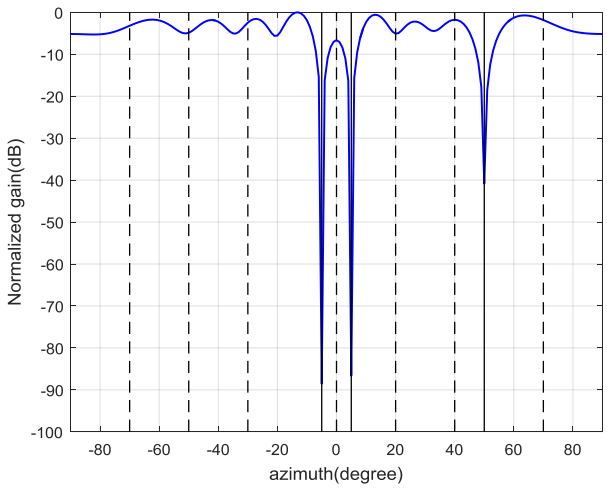


Figure 15. Quiescent beam pattern after jamming and spoofing mitigation.

- Scenario 3:

In the above two scenarios, a one-dimension line array was used to display the simulation results, such as the estimated spatial spectrum and the beam patterns, more intuitively. In order to verify that the proposed scheme is suitable for any arbitrary antenna array, in the next experiment, a 3×4 rectangular array was used, which consists of twelve omnidirectional antennas arranged as shown in Figure 2. Four authentic satellite signals were incident on the array from different directions.

One jamming source transmitted the jamming signal and one spoofing source emitted four spurious signals from the same direction. Table 5 presents the DOAs of these signals in the form of the elevation and azimuth angles. The other parameters are set as the values in Scenario 1 and Scenario 2.

Table 5. Simulation parameters of the signal sources.

	Sat1	Sat2	Sat3	Sat4	Spoofing	Jamming
PRN	2	5	8	19	[2,5,8,19]	
DOA	(20°,300°)	(30°,200°)	(40°,60°)	(50°,150°)	(50°,30°)	(60°,120°)

Figure 16 shows the spatial spectrum estimated by the Cyclic MUSIC algorithm in which the black dots denote the DOAs of all incident signals, S and A represent spoofing signal and authentic satellite signal, respectively. It indicates that the presence of spoofing interference can be detected and then mitigated through subspace projection and beamforming. Figure 17 shows the beam patterns for all the authentic satellites with respect to azimuth and elevation, in which J represents jamming. It can be seen that the weight vector calculated by the proposed method in this paper can suppress spoofing and jamming simultaneously and guarantee the gain of the authentic satellite signals. It can be concluded that the proposed interference suppression scheme is still valid when planar arrays are employed.

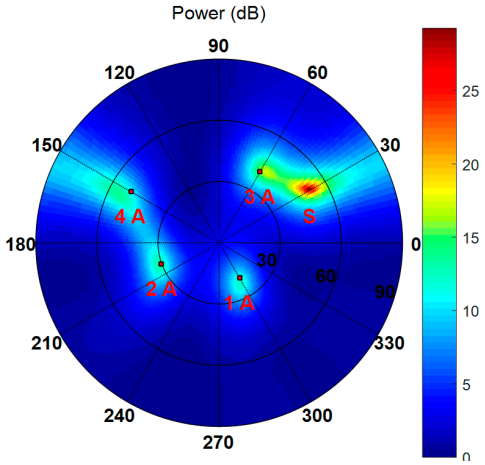
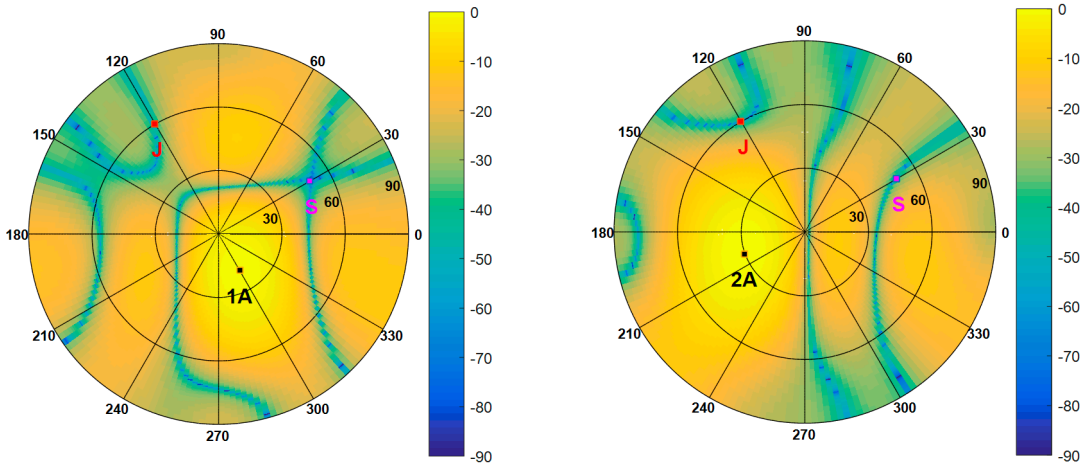
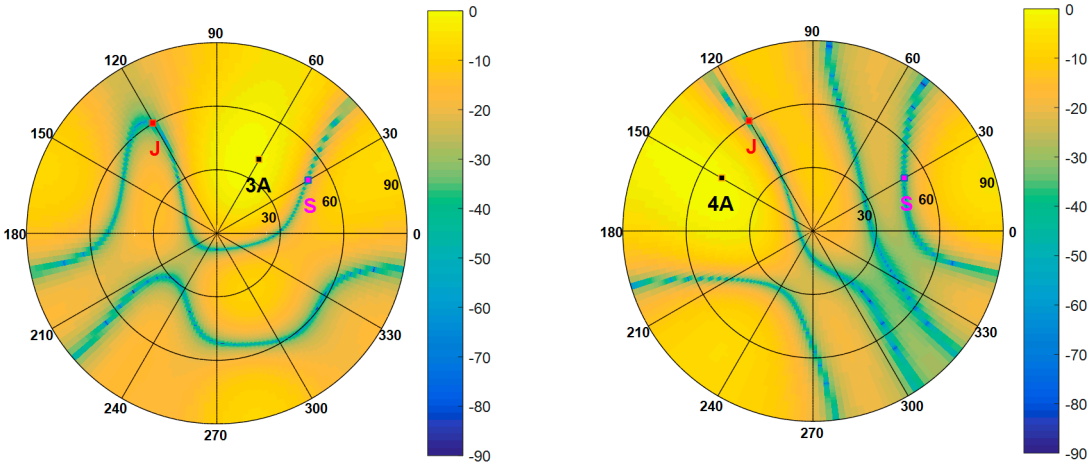


Figure 16. Spatial spectrum estimated by Cyclic MUSIC algorithm.



(**a**) PRN 2 (**b**) PRN 5

Figure 17. *Cont.*



(**c**) PRN 8 (**d**) PRN 19

Figure 17. Beam patterns for each authentic satellite.

6. Conclusions

As the use of GNSS is pervasive in military and civil fields, interference like jamming and spoofing has shown its potential threats to modern GNSS applications. This paper introduces a two-stage GNSS interference suppression scheme based on antenna arrays. In the first stage, the subspace projection was adopted to remove the strong jamming signals. The second stage dealt with low power spoofing signals, in which the cyclostationarity of navigation signals was fully excavated to detect spoofing signals and estimated the spatial power spectrum before the despreading process. Then, the subspace projection mitigated the spoofing signals and beamforming for each satellite which ensured that the power of the authentic signals was not attenuated.

The simulation results show that the proposed scheme can detect jamming signals and form deep nulls (more than −90 dB) in beam patterns to eliminate them. When the code phase differences between the authentic and spoofing signals are more than 0.5 code chips, the scheme can detect the spoofing attack successfully and estimate the DOAs of all the signals accurately. The spoofing signals can be attenuated by more than 50 dB while the main-beam points to the desired satellite. It should be noted that our method is to distinguish between interference and satellite signals based on their differences in the spatial-domain. When the DOA of a satellite signal is close to the jamming's or spoofing's DOA, this signal can be eliminated in interference nulls. Fortunately, according to the geometry distribution of the GPS satellites, there are not many authentic signals from the direction close to the interference DOA.

However, in the spoofing scenario of a small time-offset, the correlation between the authentic and spoofing signals may cause poor DOA estimation performance. Given this problem, the forward-backward spatial smoothing techniques for de-correlation can be used to improve the DOA estimation performance, but it may also result in the loss of array freedom. When both the satellites and receiver are moving, the calculation of the cyclic correlation matrix over a long data set may provide the necessary smoothing needed. The authors intend to make further investigations in future work.

Author Contributions: Conceptualization, J.Z.; Data curation, J.Z.; Formal analysis, J.Z.; Funding acquisition, M.L.; Investigation, J.Z.; Methodology, J.Z.; Project administration, X.C.; Resources, X.C. and M.L.; Software, J.Z.; Supervision, X.C.; Validation, J.Z.; Visualization, J.Z. and X.C.; Writing—original draft, J.Z.; Writing—review & editing, X.C. and H.X.

Funding: This research received no external funding.

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

References

1. Papadimitratos, P.; Jovanovic, A. Protection and fundamental vulnerability of GNSS. In Proceedings of the IEEE International Workshop on Satellite and Space Communications, Toulouse, France, 1–3 October 2008.
2. Ioannides, R.T.; Pany, T.; Gibbons, G. Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. *Proc. IEEE* **2016**, *104*, 1174–1194.
3. Katulski, R.; Magiera, J.; Stefanski, J.; Studanska, A. Research study on reception of GNSS signals in presence of intentional interference. In Proceedings of the IEEE International Conference on Telecommunications and Signal Processing, Budapest, Hungary, 18–20 August 2011.
4. Lijun, W.; Huichang, Z.; Gang, X.; Shuning, Z. AM-FM interference suppression for GPS receivers based on time-frequency analysis and synthesis. In Proceedings of the IEEE, International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, Beijing, China, 8–12 August 2015.
5. Chang, C.L. Novel multiplexing technique in anti-jamming GNSS receiver. In Proceedings of the 2011 American Control Conference, San Francisco, CA, USA, 29 June–1 July 2011.
6. Fante, R.L.; Vaccaro, J. Wideband cancellation of interference in a GPS receive array. *IEEE Trans. Aerosp. Electron. Syst.* **2000**, *36*, 549–564. [CrossRef]
7. Gupta, I.J.; Moore, T.D. Space-frequency adaptive processing (SFAP) for radio frequency interference mitigation in spread-spectrum receivers. *IEEE Trans. Antennas Propag.* **2004**, *52*, 1611–1615. [CrossRef]
8. Daneshmand, S.; Jahromi, A.J.; Broumandan, A.; Lachapelle, G. GNSS space-time interference mitigation and attitude determination in the presence of interference signals. *Sensors* **2015**, *15*, 12180–12204. [CrossRef] [PubMed]
9. Moore, T.D. Analytic Study of Space-Time and Space-Frequency Adaptive Processing for Radio Frequency Interference Suppression. Ph.D. Thesis, The Ohio State University, Columbus, OH, USA, 2002.
10. Jafarnia Jahromi, A. Gnss Signal Authenticity Verification in the Presence of Structural Interference. Ph.D. Thesis, University of Calgary, Calgary, AB, Cananda, 2013.
11. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270.
12. Broumandan, A.; Jafarnia-Jahromi, A.; Daneshmand, S.; Lachapelle, G. Overview of spatial processing approaches for GNSS structural interference detection and mitigation. *Proc. IEEE* **2016**, *4*, 1246–1257.
13. Jahromi, A.J.; Broumandan, A.; Nielsen, J. Gérard Lachapelle. Gps spoofer countermeasure effectiveness based on signal strength, noise power, and c/n0 measurements. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 81–191.
14. McMilin, E.; De Lorenzo, D.S.; Walter, T.; Lee, T.H.; Enge, P. Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications. In Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute OF Navigation (ION GNSS+ 2014), Tampa, FL, USA, 8–12 September 2014.
15. Cho, S.L.; Shin, M.Y.; Lim, S.; Hwang, D.H.; Lee, S.J.; Park, C. Design of a TOA-based anti-spoofing method for GPS civil signal. In Proceedings of the ION GNSS PNT Symposium 2008, Savannah, GA, USA, 16–19 September 2008.
16. Daneshmand, S.; Jafarnia-Jahromi, A.; Broumandan, A.; Lachapelle, G. A GNSS structural interference mitigation technique using antenna array processing. In Proceedings of the 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop, A Coruna, Spain, 22–25 June 2014.
17. Appel, M.; Konovaltsev, A.; Meurer, M. Robust spoofing detection and mitigation based on direction of arrival estimation. In Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Tampa, FL, USA, 14–18 September 2015.
18. Meurer, M.; Konovaltsev, A.; Cuntz, M.; Hättich, C. Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM. In Proceedings of the 25th Int. Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012.
19. Dreher, A.; Niklasch, N.; Klefenz, F.; Schroth, A. Antenna and receiver system with digital beamforming for satellite navigation and communications. *IEEE Trans. Microw. Theory Tech.* **2003**, *51*, 1815–1821. [CrossRef]
20. Wang, L.; Wu, R.; Zhang, Y. Multi-type interference suppression for GNSS based on despread-respread method. In Proceedings oF the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Tampa, FL, USA, 14–18 September 2015.

21. Rong, Z. Simulations of adaptive array algorithm for CDMA system. Blacksburg: Virginia echnology. In Proceedings of the 1997 IEEE 47th Vehicular Technology Conference. Technology in Motion, Phoenix, AZ, USA, 4–7 May 1997.
22. Dong, K.; Zhang, Z.; Xu, X. A hybrid interference suppression scheme for global navigation satellite systems. In Proceedings of the 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 11–13 October 2017.
23. Trees, V.; Harry, L. *Optimum Array Processing: Part IV of Detection, Estimation, and Modulation*; Wiley: New York, NY, USA, 2002.
24. Kaplan, E.; Hegarty, C. *Understanding GPS: Principles and Applications*; Artech House: Norwood, MA, USA, 2005.
25. Gardner, W.A. *Cyclostationarity in Communications and Signal Processing*; IEEE: New York, NY, USA, 1993.
26. Gardner, W.A. Simplification of MUSIC and ESPRIT by exploitation of cyclostationarity. *Proc. IEEE* **1988**, *76*, 845–847. [CrossRef]
27. Anderson, T.W. Asymptotic theory for principal component analysis. *Ann. Math. Stat.* **1963**, *34*, 122–148. [CrossRef]
28. Wax, M.; Kailath, T. Detection of signals by information theoretic criteria. *IEEE Trans. Acoust. Speech Signal Process.* **1985**, *ASSP-33*, 387–392.
29. Johnstone, I.M. On the Distribution of the Largest Eigenvalue in Principal Components Analysis. *Ann. Stat.* **2001**, *29*, 295–328. [CrossRef]
30. Amin, M.G.; Sun, W. A novel interference suppression scheme for global navigation satellite systems using antenna array. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 999–1012.