Hindawi
International Journal of Antennas and Propagation
Volume 2019, Article ID 8012569, 9 pages
https://doi.org/10.1155/2019/8012569

Research Article

A Combined Antijamming and Antispoofing Algorithm for GPS Arrays

Qiong Yang,[1,2] **Yi Zhang**,[1] **Chengkai Tang**,[1] **and Jie Lian**[3]

[1]*School of Electronic Information, Northwestern Polytechniacl University, Xi'an 710072, China*
[2]*School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China*
[3]*Department of Electrical and Computer Engineering, University of Virginia, VA 22904, USA*

Correspondence should be addressed to Qiong Yang; 821057095@qq.com

Received 9 August 2018; Revised 7 February 2019; Accepted 28 February 2019; Published 15 April 2019

Academic Editor: Xiulong Bao

The Global Positioning System (GPS), with its accurate positioning and timing information, has become a commonly used navigation instrument for many applications. However, it is susceptible to intentional interference such as jamming and spoofing. The conventional antijamming GPS receiver fails to work in a combined jamming and spoofing attack scenario. To solve the problem, a combined antijamming and antispoofing algorithm for a GPS receiver based on an antenna array is proposed. In this method, the jamming is eliminated by subspace projection, and then a compressed sensing framework is adopted to obtain the direction of arrival (DOA) of the despreading satellite navigation signal and detect the spoofing signal. According to the DOA of the authentic and spoofing signals, the receiver uses adaptive multibeamforming to concurrently achieve the undistorted reception of the authentic satellite signal and the suppression of the spoofing. We analyse three aspects of algorithmic performance: the antenna array direction diagram, the spoofing detection and the acquisition results. The simulation results and their analysis preliminarily show that the proposed method can detect and suppress GPS jamming and spoofing effectively.

1. Introduction

The Global Navigation Satellite System (GNSS) is widely used in modern military and civil navigation and positioning systems. However, the satellite signal power at the ground is very low (approximately -130 dBm), which makes it vulnerable to interference. Research on satellite navigation system interference suppression technology has important practical application value. GNSS interference can be divided into jamming and spoofing. Jamming can block the receiver by transmitting strong interference so that the useful GNSS signal cannot be detected and acquired normally. A jammer with a power of 1 W can disable the civil Global Positioning System (GPS) within 25 kilometres [1]. On the other hand, spoofing cheats the receiver by sending fake signals similar to authentic signal parameters and results in incorrect location or time information. In 2013, Todd Humpherys from the University of Texas demonstrated that the use of a civilian spoofer can control and dominate the movement path of a UAV [2] and a deluxe yacht [3]. Baziar designed a novel GPS spoofing generation method based on a combination of authentic and delayed signals, without expensive hardware equipment and reduced the cost and complexity of spoofing implementation [4].

With the development of antijamming technology, a new generation of satellite navigation receivers has adopted a series of interference suppression measures, including the use of the Wavelet packet transform (WPT) [5], neural network cancellation [6], and the adaptive notch filter [7, 8] to suppress narrowband interferences, but these methods are not suitable for wideband interference suppression. Many antijamming receivers make use of the antenna array power inversion (PI) [9, 10] algorithm to nullify the wideband interference or the adaptive beamforming algorithm to improve the output signal-to-noise ratio (SNR) of the array by nullifying the interference directions while forming the useful GNSS signal directional beam [11]. However, the degrees of freedom of antennas are limited by the number of antenna elements, and the space-time adaptive processing (STAP) method increases the degrees of freedom without increasing the array elements.

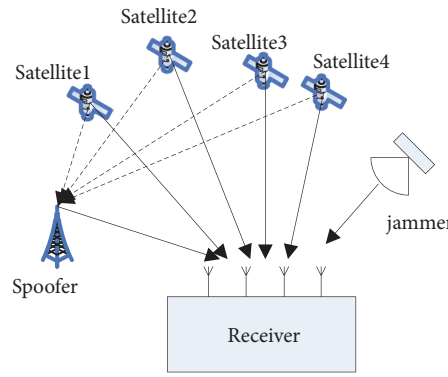

Figure 1: Severe environment with the spoofing and jamming model.

The method also has better antijamming performance in a highly dynamic environment [12–14]. Although spoofing is highly concealable and creates confusion, many scholars have proposed spoofing detection and suppression algorithms. The monitoring automatic gain control (AGC) proposed by [15] is the simplest and most effective spoofing detection method. However, this method can not suppress the spoofing, and the jamming will cause AGC value alteration. Todd proposed a power-distortion detection algorithm based on the received power and the correlated peak distortion monitoring, which can distinguish multipath fading, spoofing, and jamming [16, 17]. A comprehensive spoofing detection method based on Dempster-Shafer theory was proposed by Mingquan Lu; this method fuses the power, tracking error, C/N0, and Doppler frequency shift and reduces the detection error rate [18]. Psiaki assumed that the spoofing signals come from the same direction and detected the existence of spoofing by the carrier phase difference characteristics of a dual antenna [19, 20]. Similarly, HK Chang detected the spoofing direction of arrival (DOA) through the extended Kalman filter [21]. LuWen Zhao proposed a tracking phase spoofing detection method in which spectrum analysis of the PLL loop phase output is conducted, and the low-frequency residual signal in the spectrum can be used to identify the characteristics of spoofing [22]. Li and Mosavi took advantage of a multichannel correlator to filter the correlation results, thereby protecting GPS receivers from spoofing [23, 24]. The hypothesis test theory was applied to the open spoofing dataset TEXBAT to verify the detection correctness by Gamba [25]. Some researchers [26–28] proposed a spatial correlation detection algorithm under the motion of a single-antenna receiver to reduce the possibility of spoofing by dynamic receivers and proposed the spoofing cancellation algorithm. However, while the above methods based on single-antenna focus on spoofing detection, little work has been done on spoofing suppression.

With the wide application of adaptive antenna array technology in antijamming receivers, it is currently very difficult to interfere with the receiver via only jamming or spoofing. However, in actual combat, the combination of jamming and spoofing makes the existing independent antijamming algorithms and antispoofing algorithms invalid. A combined GNSS jamming and spoofing suppression algorithm based on multiple antennas in [29] suffers from high calculation costs. To solve these problems, this paper presents a computationally nonintensive method for an antijamming and antispoofing algorithm for a GPS receiver. It first suppresses jamming by projecting the received signals in the orthogonal subspace of the jamming. Then, the receiver estimates the DOAs of satellites based on compressed sensing and detects spoofing via DOA information. Finally, the receiver uses multibeamforming to nullify the spoofing. We analyse the interference suppression performance of the receiver under combined attacks.

2. System Model

The received signal $\mathbf{r}(t)$ $(M\times1)$ is composed of m authentic GPS signals, k jamming, n spoofing GPS signals, and noise:

$$\mathbf{r}(t) = \sum_{i=1}^{m} \mathbf{a}(\theta_i)\, \mathbf{s}_i^a(t) + \mathbf{a}(\varphi) \sum_{i=1}^{n} \mathbf{s}_i^s(t) + \sum_{q=1}^{k} \mathbf{a}(\kappa_q)\, J_q(t) + \mathbf{n}(t) \tag{1}$$

where $\mathbf{a}(\theta_i)$ is the $M \times 1$ steering matrix of the i-th authentic GPS signal, $\mathbf{a}(\varphi)$ is the $M \times 1$ steering matrix of the spoofing GPS signal, $\mathbf{a}(\kappa_q)$ is the $M \times 1$ steering matrix of the jamming, and $\mathbf{s}_i^a(t)$ $(M\times1)$ is time domain waves of the i-th authentic signal. $J_q(t)$ $(M \times 1)$ is the time domain waves of the jamming signal. The i-th authentic GPS signal can be expressed as $s_i^a(t) = A_i^a C_i^a(t) D_i^a(t) \sin(\omega_{L1}(t) + \varphi_i^a)$ and the i-th spoofing signal can be expressed as $s_i^s(t) = A_i^s C_i^s(t) D_i^s(t) \sin(\omega_{L1}(t) + \varphi_i^s)$, where A_i is i-th C/A code amplitude, $C_i(t)$ is the i-th pseudorandom noise (PRN) code, $D_i(t)$ is the i-th PRN navigation message, ω_{L1} is the angular frequency of L1 signal, φ_i is the signal phase [4], and the subscripts a and s, respectively, represent the authentic and spoofing signals. $\mathbf{n}(t)$ $(M \times 1)$ is the Gaussian noise with zero mean and the variance σ^2. The spoofing in this paper is the single-antenna repeater spoofing. Specifically, the spoofer first receives several authentic satellite signals, and it then increases the power of the signals by approximately 3 dB, delays the signal, and broadcasts the spoofed signals in one direction. The power of spoofing is higher than that of an authentic satellite signal, but it is still far below the noise level. Figure 1 shows the severe environment with the spoofing and jamming model.

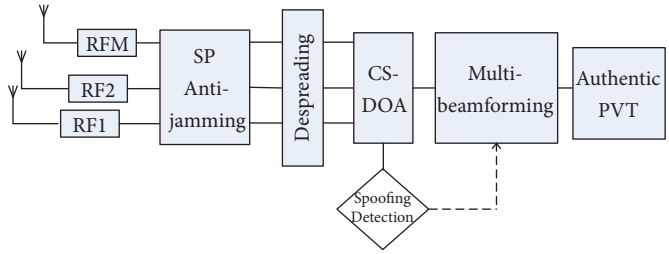

Figure 2: GPS receiver antijamming and antispoofing system.

3. Combined Antijamming and Antispoofing Algorithm (AJ-AS)

Jamming and spoofing are two major threats to satellite navigation system safety. The current single type interference suppression methods become invalid when jamming and spoofing are jointly used to attack the receivers. The strong jamming reduces the SNR and makes the receiver unable to work, and the spoofing misleads the receiver to get the wrong positioning results. An antijamming receiver is easily misled by spoofing, and an antispoofing receiver will not be able to obtain the characteristics of the spoofing during the joint attack unless it removes the jamming first. Here, we propose a combined antijamming and antispoofing algorithm for a GPS receiver with antenna arrays. The details are presented in the following subsections.

3.1. Antijamming Based on Subspace Projection. Figure 2 shows the GPS receiver antijamming and antispoofing system, which suppresses the jamming based on subspace projection and detects the spoofing by the compressed sensing DOA estimation. If spoofing exists, the receiver uses multibeamforming to eliminate the spoofing and get the authentic position, velocity, and time (PVT).

The self-correlation matrix of the received signal can be depicted as follows [30]:

$$\mathbf{R}_{\mathrm{r}} = E\left\{\mathbf{r}(t)\,\mathbf{r}^{H}(t)\right\} = \mathbf{R}_a + \mathbf{R}_s + \mathbf{R}_J + \sigma^2\mathbf{I} \tag{2}$$

where $\mathbf{R}_a$, $\mathbf{R}_s$, $\mathbf{R}_J$ denote the self-correlation matrix of authentic signals, spoofing and jamming, respectively, and $\mathbf{I}$ is the identity matrix. The spoofing power is 3 dB higher than the authentic signal, the power of the authentic signal is 20 dB below the noise, and the power of jamming is far higher than the noise. Thus, formula (2) can be approximated as

$$\mathbf{R}_r \approx \mathbf{R}_J + \sigma^2\mathbf{I} \tag{3}$$

In case that the jamming and noise are independent of each other, we can estimate the jamming and noise subspaces with the eigen-decomposition of the correlation matrix.

$$\mathbf{R}_r = \mathbf{U}_j\mathbf{\Lambda}_j\mathbf{U}_j^H + \mathbf{U}_N\mathbf{\Lambda}_N\mathbf{U}_N^H \tag{4}$$

where λ_j $(j = 1, \sim, M)$ are the eigenvalues of the array covariance matrix, $\lambda_1 \geq \lambda_2 \cdots \geq \lambda_k \gg \lambda_{k+1} \cdots > \lambda_M = \sigma^2$, and $\mathbf{u}_j$ is the eigenvector corresponding to the eigenvalue λ_j. Determining the k jammers based on the eigenvalues and the jamming subspace $\mathbf{U}_j$ is defined by the eigenvectors corresponding to the k largest eigenvalues and the M-k smallest eigenvectors are defined as the noise subspace $\mathbf{U}_N$.

$$\begin{aligned} \mathbf{U}_N^H\mathbf{U}_j &= 0 \\ \mathbf{U}_N\mathbf{U}_N^H + \mathbf{U}_j\mathbf{U}_j^H &= \mathbf{I} \end{aligned} \tag{5}$$

Through the projection of the received signal vector of the arrays to the noise subspace, the jamming component can be effectively suppressed. The orthogonal complement space of jamming $\mathbf{P}_\perp$ can be defined as follows:

$$\mathbf{P}_\perp = \mathbf{I} - \frac{\mathbf{U}_j\mathbf{U}_j^H}{\left\|\mathbf{U}_j\mathbf{U}_j^H\right\|} \tag{6}$$

$$\begin{aligned} \overline{\mathbf{r}}(t) = \mathbf{P}_\perp^H\mathbf{r}(t) = \mathbf{P}_\perp^H\Bigg(&\sum_{i=1}^{m}\mathbf{a}(\theta_i)\,\mathbf{s}_i^a(t) + \mathbf{a}(\varphi)\sum_{i=1}^{n}\mathbf{s}_i^s(t) \\ &+ \sum_{q=1}^{k}\mathbf{a}(\kappa_q)\,J_q(t) + \mathbf{n}(t)\Bigg) = \mathbf{P}_\perp^H\sum_{i=1}^{m}\mathbf{a}(\theta_i)\,\mathbf{s}_i^a(t) \\ &+ \mathbf{P}_\perp^H\mathbf{a}(\varphi)\sum_{i=1}^{n}\mathbf{s}_i^s(t) + \tilde{\mathbf{n}}(t) \end{aligned} \tag{7}$$

As a result, the output vector $\overline{\mathbf{r}}(t)$ does not contain jamming, but it may still contain spoofing. The power of an authentic signal and spoofing are still far below that of the noise. The receivers never know the DOA of the spoofing. The conventional DOA algorithm, such as multiple signal classification (MUSIC) [31], estimates the signal parameters via the rotation invariant technique (ESPRIT) [31], which results in incorrect estimates in very low SNRs. In addition, the spoofing is confusing. The spoofing DOA is easy to be regarded as the authentic DOA, which will mislead beamforming to form a main lobe in the direction of spoofing.

3.2. Spoofing Detection and Suppression. The current spoofers mostly use single-antenna transmission spoofing. This use makes the directions of the multiple spoofed signals arriving at the receiver antenna exactly the same, while the authentic signals arrive from totally different directions. The principle of the detection of spoofing involves using high-precision DOA estimation based on the compressed sensing

theory to obtain the incoming information. The antijamming output is sent to the acquisition module, which applies correlation integral despreading to improve the SNR. Then, the compressed sensing theory can be used to solve the DOA estimation problem for the despreading signal. The advantages of compressed sensing theory are small snapshots, low SNR, and high resolution. There are numerous possible signal DOAs in space, but only a very limited proportion is in the direction of the actual signal coverage in the whole airspace. Therefore, it is considered that the signal has spatial sparsity. The compressed sensing theory can be used to reconstruct the source signal, and the support sets of the reconstructed signals correspond to the arrival angles of the source signals. A spoofing detection method based on the compressed sensing DOA is feasible.

Since the authentic satellite and spoofing share the same PRN, there are P far-field narrowband signals for the i-th satellite that arrive at the uniform linear array of M elements. Generally speaking, P=2 in one spoofing and authentic satellite coexistence environment. Using them, we can get the antijamming and despreading received signal model.

$$\tilde{\mathbf{r}}_i(t) = \mathbf{\Phi}\mathbf{s}_i(t) + \tilde{\mathbf{n}}(t) \tag{8}$$

where $\tilde{\mathbf{n}}(t)$ is the despreading noise, $\mathbf{\Phi} = [\mathbf{a}_1 \ \mathbf{a}_2 \ \cdots \mathbf{a}_N]$ is the $M \times N$ sparsity manifold matrix, $\mathbf{a}_k = \left[1 \mathrm{e}^{-j2\pi f_0((d\sin\theta_k)/c)} \ \cdots \mathrm{e}^{-j2\pi f_0((M-1)d\sin\theta_k/c)}\right]^T$ is the steering vector of uniform linear array, f_0 is the carrier frequency, c is the speed of light, d is the array spacing, and θ_p is the DOA of the p-th signal. The space is divided into N parts on average as $\{\theta_1, \theta_2, \cdots, \theta_N\}$. Suppose that each θ_n corresponds to a potential signal s_i^n. Since $N \gg P$, $\mathbf{s}_i = \left[s_i^1 \ s_i^2 \ \cdots s_i^N\right]^T$ is the $N \times 1$ vector with P sparsity. That is to say, there are only P elements of signal locations that are nonzero; the rest of the N-P elements are zero. Let $\boldsymbol{\theta}$ be the information vector and $\boldsymbol{\psi}$ be the orthogonal basis sparse dictionary. The compressed sensing theory points out that when the signal is compressible or sparse, it can be projected into a low dimensional space via a measurement matrix, and then a certain reconstruction algorithm is used to recover the signal. The compression observation of $\mathbf{s}_i$ can be expressed as [31]

$$\tilde{\mathbf{r}}_i = \Phi\mathbf{s}_i + \tilde{\mathbf{n}} = \Phi\boldsymbol{\psi}\boldsymbol{\theta} + \tilde{\mathbf{n}} = \mathbf{A}_{cs}\boldsymbol{\theta} + \tilde{\mathbf{n}} \tag{9}$$

where $\mathbf{A}_{\mathrm{cs}} = \mathbf{\Phi}\boldsymbol{\psi}$ is $M \times P$ sensing matrix. The information vector $\boldsymbol{\theta}$ can be reconstructed accurately from using the despread received data $\tilde{\mathbf{r}}_\mathbf{i}$ and the l_1 norm optimization. The corresponding sparse reconstruction model can be written as follows:

$$\begin{aligned} \arg\min \quad & \|\boldsymbol{\theta}\|_1, \\ \text{s.t.} \quad & \left\|\tilde{\mathbf{r}}_i - \mathbf{A}_{cs}\boldsymbol{\theta}\right\|_2 \le \varepsilon \end{aligned} \tag{10}$$

where ε is a parameter related to the noise level and $\|\bullet\|_1$ denotes the l_1 norm. Since formula (10) is a convex optimization problem, it can be solved directly by the CVX toolbox [32]. The solutions of formula (10) are the DOAs of the P target signal sources.

Assuming that the DOAs of spoofing and the authentic satellite are different, the proposed method can not recognize the spoofing and the real signal when their DOAs are the same. However, the case of the same DOA is a small probability event; even if the two DOAs are exactly the same, the real satellite is moving at all times; the authentic DOA is also changing over time; this method can restore normal work quickly.

Because the spoofer transmits multiple spoofing signals through a single antenna, multiple satellite signals from the same direction can be used as evidence of spoofing. If there is spoofing, the next step is to suppress the spoofing by using adaptive multibeamforming. The adaptive multibeamforming can form main lobes in multiple satellite directions at the same time. The linear constrained minimum variance (LCMV) criterion minimizes the contribution power of noise and any interference from undesired directions, but it can keep the signal in the expected directions. The constrained equation is as follows:

$$\begin{aligned} \min_{\mathbf{w}} \quad & \mathbf{w}^H\mathbf{R}_{\tilde{r}\tilde{r}}\mathbf{w}, \\ \text{s.t.} \quad & \mathbf{G}\mathbf{w} = \mathbf{F} \end{aligned} \tag{11}$$

w is the beamforming weighted vector, $\mathbf{R}_{\tilde{r}\tilde{r}}$ is the covariance matrix after the antijamming, $\mathbf{G}$ is the steering vector constrained matrix, and $\mathbf{F}$ responds to the spatial filter in each constraint direction. The optimal weighting is

$$\mathbf{w} = \mathbf{R}_{\tilde{r}\tilde{r}}^{-1}\mathbf{G}\left(\mathbf{G}^H\mathbf{R}_{\tilde{r}\tilde{r}}^{-1}\mathbf{G}\right)^{-1}\mathbf{F} \tag{12}$$

At this point, since the received signals first have gone through the antijamming unit and then the spoofing detection and suppression unit, the GPS receiver can work under a combined jamming and spoofing attack.

4. Simulation Results

To evaluate the performance of the method proposed in this paper, some simulation results are provided in this section. We take a uniform linear array with 9 elements as the multiantenna model. The array space is half of the GPS L1 wavelength, the jamming is wideband interference, the jamming-to-signal ratio (JSR) is 40 dB, and the direction of the jamming is 20°. The GPS receiver needs at least four satellites to calculate a position. Therefore, four authentic and four spoofing PRNs are simulated. For example, receiver A receives 4 strong authentic PRNs, which are 18, 22, 24, and 25. The satellite simulator generates the spoofing with the same PRNs and transmits it through a single antenna. The power of the spoofing is 3 dB higher than that of the authentic PRNs. The spoofing PRNs are from the same direction 0°, and the receiver does not know the directions of the authentic and spoofing PRNs. The primary simulation parameters are shown in Table 1.

4.1. Adaptive Array Direction Diagram. As is shown in Figure 3, the red line is the adaptive array direction diagram of the proposed AJ-AS algorithm, the black line is the adaptive

Table 1: Parameters of satellite and interference.

Symbol	PRN	DOA/degree	Doppler/Hz	JSR/dB
Authentic(A1)	18	50	-3572	/
(A2)	22	80	-2561	/
(A3)	24	-45	-711	/
(A4)	25	-10	-358	/
Spoofing(S1)	18	0	-3429	3
(S2)	22	0	-2656	3
(S3)	24	0	-1102	3
(S4)	25	0	14	3
Jamming(J1)	/	20	/	40

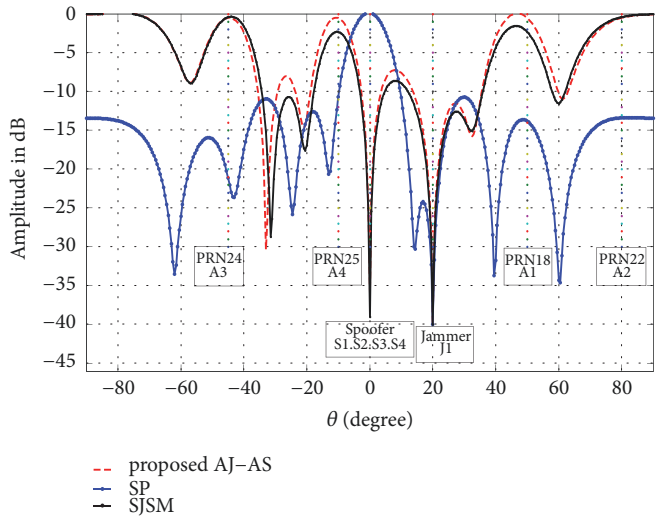

Figure 3: Adaptive array direction diagram.

array direction diagram of the spoofing and jamming suppression method (SJSM) [28], and the blue line is the adaptive array direction diagram of the SP [30] antijamming algorithm. The coloured lines show the directions of the authentic PRNs, the spoofer, and the jammer. Since the four spoofing signals come from the same direction, the spoofing degree of freedom is one, the degree of freedom of jamming is one, and the four authentic satellites represent four degrees of freedom; thus, a total of six degrees of freedom are required. Therefore, it is theoretically feasible to use nine element arrays to process six degrees of freedom beamforming in the simulation. Both the AJ-AS and the SJSM can form a deep null steering beam in the directions of the jammer (approximately -40 dB) and the spoofer (approximately -36 dB) and multibeamform to the four authentic PRNs' directions, but the SJSM has a small attenuation (approximately -2 dB) in the directions of PRN18 and PRN25 [28]. This attenuation occurs because the SJSM approximates the cross-correlation matrix of the current signal and the delay signal and ignores the effects of navigation data bit jump. Fortunately, the AJ-AS does not have these shortcomings. Figure 3 shows that both the AJ-AS and the SJSM can suppress the combined jamming and spoofing attack, but the interference performance of the AJ-AS is better than that of the SJSM. The SP only has deep null steering in the direction of the jammer (approximately -41 dB), but its beam is in the spoofing direction. The SP can mitigate jamming, but it cannot detect the spoofing.

4.2. Spoofing Detection. Figure 4 shows the DOA estimates for PRN18, PRN22, PRN24, and PRN25 using the compressed sensing theory. The X-axis represents the whole space, and the Y-axis represents the probability of the existence of signals in the space. Due to the highly similar navigation message structure between the spoofing and the authentic satellite signal, conventional receivers have difficulty detecting the spoofing. However, the receiver with the proposed AJ-AS algorithm in this paper detects two PRN18 satellites at 0° and 50°, two PRN22 satellites at 0° and −80°, two PRN24 satellites at 0° and −45°, and two PRN25 satellites at 0° and −45°. Since the spoofings come from the same direction and the directions of the authentic satellite signals are different, we can choose the number of signals at a direction as the spoofing detection threshold; if there are more than two signals at a direction, the receiver can detect the spoofing successfully. Moreover, it is deduced that the DOA of the spoofer is 0°, the DOA of the authentic PRN18 is 50°, the DOA of the authentic PRN22 is 80°, the DOA of the authentic PRN24 is −45°, and the DOA of the authentic PRN25 is −10°.

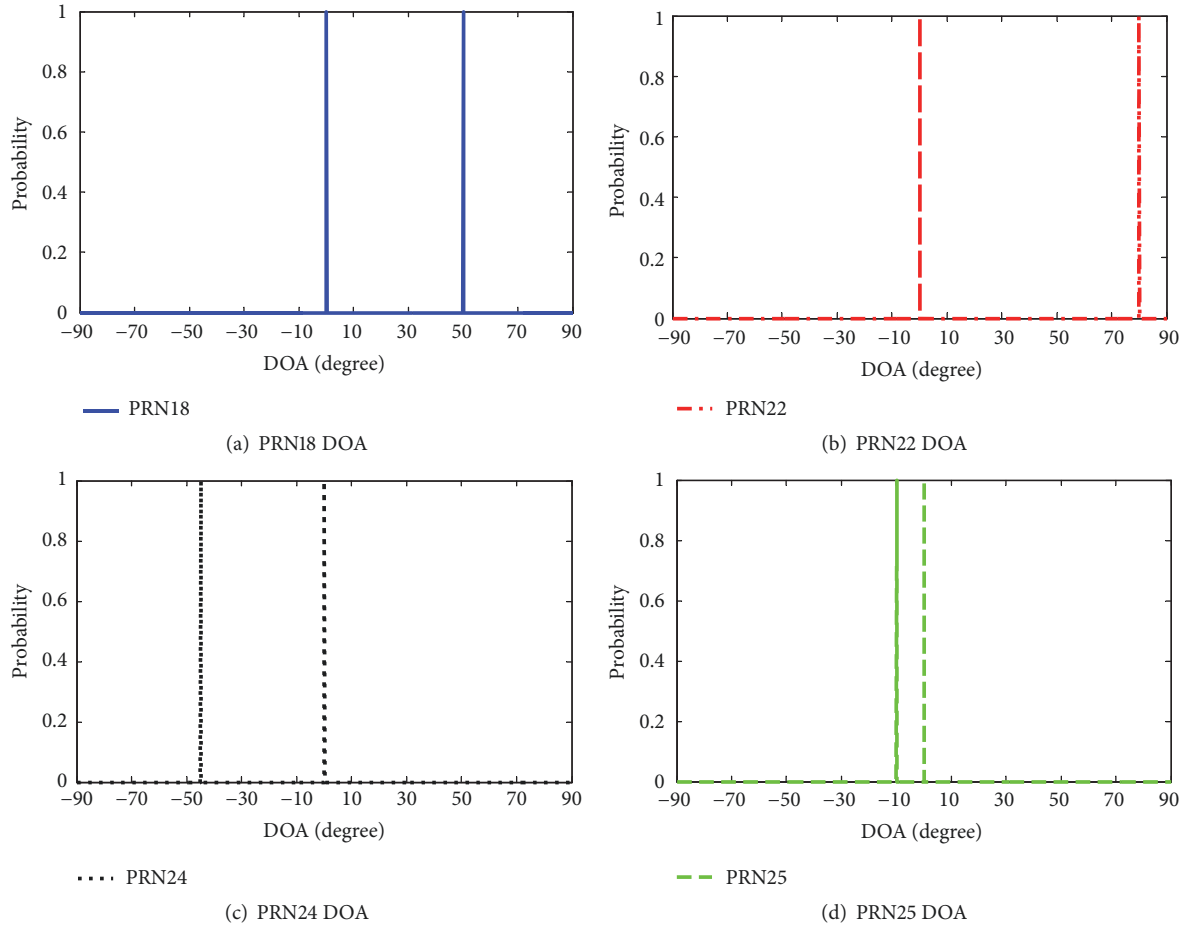

Figure 4: DOA estimation of satellite (a) DOA of PRN18; (b) DOA of PRN22; (c) DOA of PRN24; (d) DOA of PRN25.

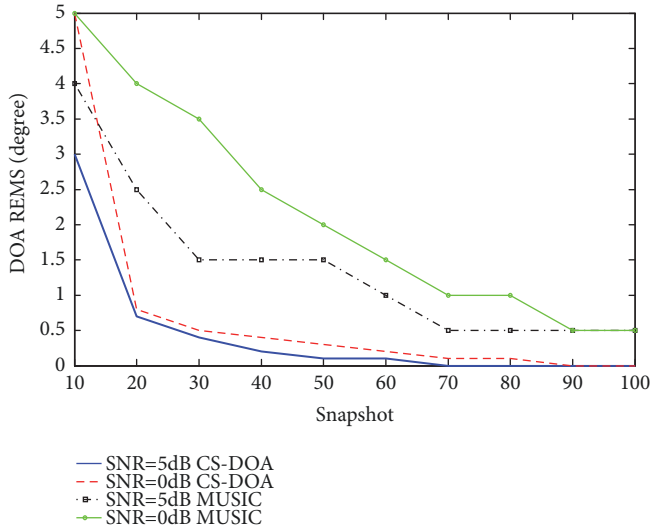

Figure 5: DOA RAMES versus snapshot.

The DOA estimates of the satellites are consistent with the parameters in Table 1, which validates the effectiveness of the DOA algorithm based on compressed sensing.

As shown in Figure 5, both the DOA REMS of compressed sensing and MUSIC decrease with increases in the snapshot and the SNR. The DOA accuracy of the compressed sensing is at least 0.5° better than that of MUSIC at the same SNR and snapshot, which directly affects the spoofing detection and the adaptive array direction diagram. The DOA method based on compressed sensing has the advantages of

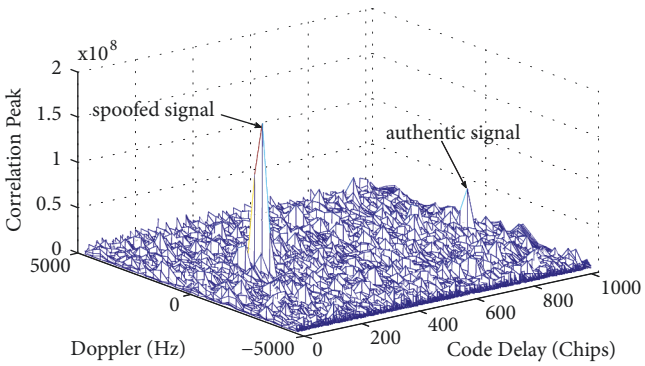

Figure 6: Acquisition of PRN25 with SP.

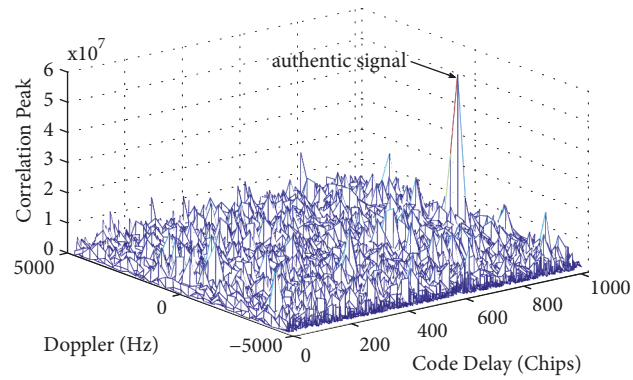

Figure 8: Acquisition of PRN25 with the proposed AJ-AS.

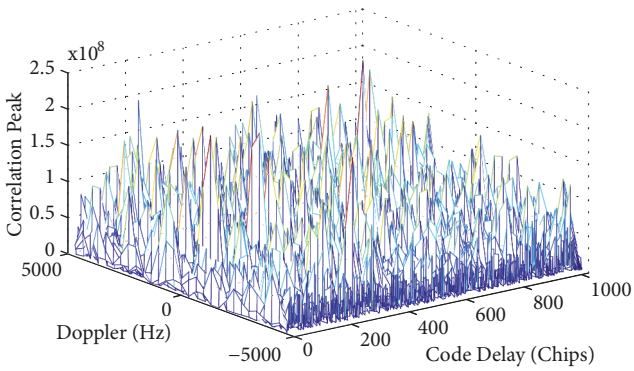

Figure 7: Acquisition of PRN25 with antispoofing based on tracking loop.

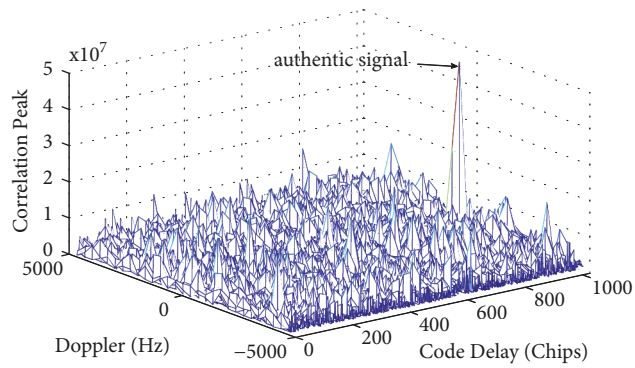

Figure 9: Acquisition of PRN25 with SJSM.

low computational costs and high accuracy. The complexity of the proposed AJ-AS algorithm increases more than that of the SP algorithm at a rate of $O(ML)^3$, where M denotes the array number and L denotes the snapshot. The snapshot is generally 100, and the estimated error is less than 0.1 degree in the experiment. Therefore, the additional computation cost of spoofing detection in AJ-AS is not high.

However, the SJSM does not mention how to detect the spoofing. It takes the DOA of spoofing as a priori information, which is not suitable for practical application scenario. In contrast, the proposed AJ-AS uses the compressed sensing method to estimate the DOAs and detect the spoofing. This method is simple, and the detection success rate is high.

4.3. Acquisition Results. Figures 6, 7, 8, and 9 show the two-dimensional correlation accumulation acquisitions for PRN25. Figure 6 is the SP antijamming algorithm, Figure 7 is the antispoofing algorithm based on the tracking loop [24], Figure 8 is the proposed AJ-AS algorithm, and Figure 9 is the SJSM. As shown in Table 1, the Doppler of the spoofing PRN25 is 14 Hz, and the Doppler of the authentic PRN25 is -358 Hz. There are two clear correlation peaks in Figure 6, where the higher peak is spoofed and the other is an authentic signal according to the Doppler. The SP suppresses the jamming but cannot mitigate the spoofing. However, there is no obvious peak in Figure 7, which shows that the receiver only with antispoofing ability cannot capture the satellite under the combined attack of jamming and spoofing because the jamming dominates the correlation peaks. There is only one authentic peak in Figures 8 and 9, but the correlation peak of the AJ-AS (5.413×10^7) is higher than that of the SJSM (4.564×10^7), which means that the proposed AJ-AS algorithm can suppress the jamming and spoofing better than the SJSM.

Synthesizing the above analysis, we reach the following conclusions:

(I) The proposed AJ-AS algorithm can nullify the directions of spoofing and jamming and can beam the main lobe at the authentic directions at the same time. A class of algorithms that only suppress jamming (represented by the SP antijamming algorithm) will be spoofed by the spoofing. Other algorithms that can only suppress spoofing (represented by the antispoofing method based on tracking loop) will be dominated by the jamming;

(II) Comparing the proposed AJ-AS algorithm with the current spoofing and jamming suppression method (SJSM), a method of spoofing detection based on compressed sensing DOA estimation is proposed. The detection is convenient and accurate and has better interference suppression performance.

5. Conclusion

We propose a combined antijamming and antispoofing algorithm for a GPS receiver that can intelligently suppress jamming and spoofing and receive the authentic signal distortion free. The proposed method has convenient, accurate spoofing detection and has better interference suppression performance. It can be integrated into the software program of an adaptive array without the need to adjust the antijamming receiver hardware. Moreover, it does not rely on the attitude information provided by the attitude measuring elements, such as the IMU. The software update increases the low computational costs, but the conventional antijamming GPS receiver becomes an antijamming and antispoofing receiver.

Data Availability

The data used to support the findings of this study are currently under embargo while the research findings are commercialized. Requests for data, 6 months after publication of this article, will be considered by the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants 61571370 and 61202394.

References

[1] X. Chen, G. Zhang, C. Jiang, and S. Wu, "GNSS augmentation by FM radio symbiosis," *IEEE Access*, vol. 6, no. 99, pp. 5162–5169, 2018.

[2] M. L. Psiaki and T. E. Humphreys, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," *IEEE Spectrum*, vol. 53, no. 8, pp. 26–53, 2016.

[3] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[4] A. R. Baziar, M. Moazedi, and M. R. Mosavi, "Analysis of single frequency GPS receiver under delay and combining spoofing algorithm," *Wireless Personal Communications*, vol. 83, no. 3, pp. 1955–1970, 2015.

[5] M. R. Mosavi, M. J. Rezaei, M. Pashaian, and M. S. Moghaddasi, "A fast and accurate anti-jamming system based on wavelet packet transform for GPS receivers," *GPS Solutions*, vol. 21, no. 2, pp. 415–426, 2017.

[6] M. R. Mosavi and F. Shafiee, "Narrowband interference suppression for GPS navigation using neural networks," *GPS Solutions*, vol. 20, no. 3, pp. 341–351, 2016.

[7] C. H. Kang, S. Y. Kim, and C. G. Park, "A GNSS interference identification using an adaptive cascading IIR notch filter," *GPS Solutions*, vol. 18, no. 4, pp. 605–613, 2014.

[8] Y.-R. Chien, "Design of GPS anti-jamming systems using adaptive notch filters," *IEEE Systems Journal*, vol. 9, no. 2, pp. 451–460, 2015.

[9] S. Daneshmand, T. Marathe, and G. Lachapelle, "Millimetre level accuracy GNSS positioning with the blind adaptive beamforming method in interference environments," *Sensors*, vol. 16, no. 11, pp. 1824–1842, 2016.

[10] Y. Wan, F. Chen, J. Nie, and G. Sun, "Optimum reference element selection for GNSS power-inversion adaptive arrays," *IEEE Electronics Letters*, vol. 52, no. 20, pp. 1723–1725, 2016.

[11] J. Arribas, C. F. Prades, and P. Closas, "Multi-antenna techniques for interference mitigation in GSS signal acquisition," *Eurasip Journal on Advances in Signal Processing*, vol. 1, no. 1, pp. 143–152, 2013.

[12] L.-W. Chen and J.-S. Zheng, "A broadened and deepened antijamming technology for high-dynamic GNSS array receivers," *IEICE Transactions on Communications*, vol. E99B, no. 9, pp. 2055–2061, 2016.

[13] B. Zhang, H. Ma, X.-L. Sun, Q. Tan, and H. Pan, "Robust antijamming method for high dynamic global positioning system receiver," *IET Signal Processing*, vol. 10, no. 4, pp. 342–350, 2016.

[14] F. Chen, J. Nie, B. Li, and F. Wang, "Distortionless space-time adaptive processor for global navigation satellite system receiver," *IEEE Electronics Letters*, vol. 51, no. 25, pp. 2138-2139, 2015.

[15] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *NAVIGATION: Journal of the Institute of Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[16] K. D. Wesson, J. N. Gross, and T. E. Humphreys, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace & Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2017.

[17] T. E. Humphreys, "Detection strategy for cryptographic gnss anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.

[18] H. Tao, H. Li, and M. Lu, "A method of detections' fusion for GNSS anti-spoofing," *Sensors*, vol. 16, no. 12, pp. 883–904, 2016.

[19] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection: Correlating carrier phase with rapid antenna motion," *GPS World*, vol. 24, no. 1, pp. 53–58, 2013.

[20] M. L. Psiaki, B. W. OHanlon, S. P. Powell et al., "GNSS spoofing detection using two-antenna differential carrier phase," in *Proceedings of the 27th ITM ION*, pp. 2776–2800, Florida, USA, 2014.

[21] C. H. Kang, S. Y. Kim, and C. G. Park, "Adaptive complex-EKF-based DOA estimation for GPS spoofing detection," *IET Signal Processing*, vol. 12, no. 2, pp. 174–181, 2018.

[22] L. W. Zhao, Z. M. Miao, and B. J. Zhang, "A novel spoofing attack detection method in satellite navigation tracking phase," *The Journal of Astronautics*, vol. 36, no. 10, pp. 1172–1177, 2015.

[23] J. Li, J. Zhang, S. Chang, and M. Zhou, "Performance evaluation of multimodal detection method for GNSS intermediate spoofing," *IEEE Access*, vol. 4, pp. 9459–9468, 2016.

[24] M. R. Mosavi, Z. Nasrpooya, and M. Moazedi, "Advanced anti-spoofing methods in tracking loop," *Journal of Navigation*, vol. 69, no. 4, pp. 883–904, 2016.

[25] M. Troglia Gamba, M. D. Truong, B. Motella, E. Falletti, and T. H. Ta, "Hypothesis testing methods to detect spoofing attacks: a test against the TEXBAT datasets," *GPS Solutions*, vol. 21, no. 2, pp. 1–13, 2017.

[26] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," *GPS Solutions*, vol. 19, no. 3, pp. 1–13, 2015.

[27] F. Wang, H. Li, and M. Lu, "GNSS spoofing countermeasure with a single rotating antenna," *IEEE Access*, vol. 5, no. 99, pp. 8039–8047, 2017.

[28] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for GNSS receiver," *IEEE Sensors Journal*, vol. 18, no. 7, pp. 2952–2958, 2018.

[29] S. Han, L. Chen, W. Meng, and C. Li, "Improve the security of GNSS receivers through spoofing mitigation," *IEEE Access*, vol. 5, no. 99, pp. 21057–21069, 2017.

[30] L. Wang, R. Wu, W. Wang, D. Lu, and Q. Jia, "Joint GNSS interference mitigation approach for jamming and spoofing based on multi-antenna array," *Journal of Electronics and Information Technology*, vol. 38, no. 9, pp. 2344–2350, 2016.

[31] Q. Shen, W. Liu, W. Cui, and S. Wu, "Underdetermined DOA estimation under the compressive sensing framework: a review," *IEEE Access*, vol. 4, no. 99, pp. 8865–8878, 2016.

[32] H. Li, C. Wang, and X. Zhu, "Compressive sensing for high-resolution direction-of-arrival estimation via iterative optimization on sensing matrix," *International Journal of Antennas and Propagation*, vol. 2015, Article ID 713930, 5 pages, 2015.