IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 13, 2017, accepted September 10, 2017, date of publication September 19, 2017,
date of current version October 25, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2754414

Improve the Security of GNSS Receivers Through Spoofing Mitigation

SHUAI HAN[1,2], (Senior Member, IEEE), LEI CHEN[1], (Student Member, IEEE), WEIXIAO MENG[1,2], (Senior Member, IEEE), AND CHENG LI[3], (Senior Member, IEEE)
[1]Communication Research Center, Harbin Institute of Technology, Harbin 150001, China
[2]State Key Laboratory of Satellite Navigation System and Equipment Technology, Shijiazhuang 050081, China
[3]Electrical and Computer Engineering Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, A1B 3X5, Canada

Corresponding author: Weixiao Meng (wxmeng@hit.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 91438205 and in part by the 54th Research Institute of CETC under Grant KX162600037.

ABSTRACT Spoofing attacks are one of the most dangerous threats for the application of the global navigation satellite system (GNSS), especially for autonomous driving and unmanned aerial vehicles. In this paper, we present a more robust spoofing mitigation algorithm based on subspace projection that is independent of the number of antennas and that can be utilized in single-antenna GNSS receivers. During a spoofing attack, authentic signals are contaminated by spoofing signals. We demonstrate that all spoofing signals can be eliminated by projecting the received signal onto the orthogonal null space of the spoofing signals. Moreover, two types of receiver structures are designed: a centralized structure that has the ability to suppress cross-correlation interference and a distributed structure with lower computational complexity and lower projection power losses. The proposed algorithm is verified by the Beidou B1I signals for improving the security of the receiver.

INDEX TERMS Security, spoofing attack, subspace projection, spoofing mitigation, GNSS.

I. INTRODUCTION

By regenerating counterfeit satellite signals, a spoofing attack can intentionally mislead a receiver to obtain fake positioning/navigation results or incorrect time information [1]–[3]. Since the development of chips and software-defined radio, the cost of spoofing attacks has greatly decreased, and their flexibility has vastly improved. In comparison with jamming, spoofing attacks are more difficult to detect and suppress. Consequently, to avoid being deceived, effective anti-spoofing module is an indispensable component in a GNSS receiver.

Typical anti-spoofing schemes can be categorized into three types: encrypting the signal in the space segment [4]–[6], redesigning the receivers in the user segment [7]–[18], and anti-spoofing assisted by external facilities [19], [20]. Encrypting the signal is an effective but subversive scheme for avoiding spoofing attacks. In the literature [4], an anti-spoofing method based on spread spectrum security codes (SSSCs) was proposed. By interleaving the normal pseudo-random code with the cryptographic SSSCs, signal authentication is achieved. Additionally, a navigation message authentication (NMA) method was also investigated in [5] and [6]. The basic principle of NMA embeds the signature information into the navigation message frame to provide a defense against spoofing attacks. Methods for encrypting signals are highly immune to spoofing attacks. However, the penalty is the modification of the conventional signal design in the space segment and the decryption of the decoded message in the user segment.

Different from adding anti-spoofing mechanisms in the space segment, redesigning anti-spoofing receivers to resist spoofing attacks is a more flexible and implementable solution. Generally, the anti-spoofing schemes implemented in GNSS receivers can be classified into two categories. The first category is composed of spoofing detection schemes that have the ability to detect and identify spoofing attacks. The majority of spoofing detection methods are built on the different characteristics between spoofing signals and genuine signals [7]–[14]. As reported in [7] and [8], it is possible to identify spoofing signals by monitoring C/N_0 and the absolute power. Spoofing signals also can be detected in the acquisition procedure, as in the work in [9]. The results in [10] have shown that spoofing signals can be determined by the cross-correlation characteristics of the P(Y) codes received by two geographically separated receivers. Carrier phase measurements are important features in identifying a spoofing attack. [11] proposed a spoofing detection method based on the carrier phase data received by a moving patch antenna, and [12] improved this method by introducing two antennas to replace the process of movement. In [13], the power measurements from a static rotating antenna were exploited to counter spoofing attacks. Moreover, the decoded baseband data also can be utilized to distinguish spoofing signals. For example, a particle-filter-based anti-spoofing algorithm employing the variations in decoded pseudorange data was reported by [14]. For the anti-spoofing schemes based on spoofing detection, when a spoofing attack is detected, the corresponding spoofing signal will be ignored; however, the spoofed authentic satellite signal corresponding to the spoofing signal will also be ignored, thereby decreasing the number of available satellites.

The second type of anti-spoofing scheme implemented in GNSS receivers is primarily based on spoofing mitigation, which eliminates spoofing signals and ensures that the spoofed authentic satellite signals are still available. Exploiting the spatial independence property between spoofing signals and genuine signals is an effective approach to mitigate spoofing signals. [15] proposed that using the DOA (Direction of Arrival) information of authentic signals and spoofing signals estimated from a miniaturized adaptive antenna array can effectively mitigate spoofing attacks. In [16] and [17], digital spatial nulls were introduced in the direction of the spoofing signals to achieve spoofing mitigation. [18] also investigated a null steering-based spoofing mitigation algorithm, in which the dominant spatial power property of the spoofing signals is utilized and low computational complexity is achieved by pre-despreading processing. However, most of the effective spoofing mitigation methods are based on antenna arrays and cannot be extended to single-antenna receivers.

In this paper, we propose a subspace projection-based spoofing mitigation algorithm, in which a spoofing countermeasure is achieved in the pseudo-random noise (PRN) code domain rather than the spatial domain. Therefore, the proposed spoofing mitigation algorithm is independent of the antenna array and can be realized in a typical single-antenna receiver. Although the successive spoofing cancellation (SSC) algorithm presented in [21] can also be implemented in single-antenna receivers, it presupposes that all parameters of spoofing signals are accurately estimated, including amplitudes, code delays, navigation data-bits, carrier frequencies and carrier phases. However, the proposed anti-spoofing algorithm in this paper only requires the code delays and carrier frequency information, which can be easily extracted from the tracking loop.

Subspace projection is a classic signal-processing method [22]–[27]. The most essential aspect of subspace projection is to construct the subspace by specific elements or characteristics. Beamforming, whose subspace is constructed using channel information, is a common form of subspace projection [23]–[26]. Because GNSS signals are direct spread-spectrum signals, the approximate orthogonal PRN codes are the ideal elements to construct the desired subspace [27], [28]. Thus, we develop the subspace projection method to mitigate spoofing attacks. First, we demonstrate that the projection of input signals onto the spoofing signals' subspace is approximated as the sum of the spoofing signals and the projection of the noise. Then, we use the projection as the estimation of the spoofing signals. After subtracting this estimation from the input signals, the result essentially consists of the desired authentic signals and noise. Next, the theoretical relationships between the performance of the proposed anti-spoofing algorithm and the estimated parameters of the spoofing signals are described in detail. We show that the performance of the proposed method is independent of the carrier phases and navigation data-bits of the spoofing signals, which indicates that only the code delays and carrier frequencies are indispensable. In addition, two types of receiver structures are designed in this paper. Finally, the validity of the subspace projection method is tested on Beidou B1I signals.

The remainder of this paper is organized as follows. Section II introduces the mathematical model of the proposed spoofing mitigation algorithm. Section III presents the theoretical performance analysis and proves that carrier phases and data-bit information are unnecessary. In Section IV, the receiver structures with both centralized and distributed spoofing mitigation modules are designed. Then, the simulation results are presented in Section V to confirm the validity of the proposed anti-spoofing scheme.

Notation: We use $\mathbf{X}^T$, $\mathbf{X}^H$, and $\mathbf{X}^{-1}$ to denote the transpose, conjugate transpose, and inverse of a matrix $\mathbf{X}$, respectively. For a vector $\mathbf{x} \in \mathbb{C}^{M\times 1}$, we use diag($\mathbf{x}$) to denote the diagonal matrix whose diagonal entries are constructed by $\mathbf{x}$, $\|\mathbf{x}\|_2$ to indicate the Euclidean norm of a vector $\mathbf{x}$, and $(\mathbf{x})_i$ to represent the ith element of a vector $\mathbf{x}$. Finally, the identity matrix and zero vector are represented by $\mathbf{I}$ and $\mathbf{0}$, respectively.

II. SPOOFING MITIGATION BASED ON SUBSPACE PROJECTION

Assuming that there are N authentic signals and M spoofing signals, the received IF signal can be expressed as

$$\mathbf{r}_{IF} = \mathbf{r}_A + \mathbf{r}_S + \mathbf{n}, \tag{1}$$

where $\mathbf{r}_{IF} = [r(t_1), \ldots, r(t_l), \ldots, r(t_L)]^T$ denotes the IF signal, $\mathbf{n} = [n(t_1), \ldots, n(t_l), \ldots, n(t_L)]^T$ is the additive white Gaussian noise, t_l is the lth sampling time, and L is the total number of samples.

The N authentic signals $\mathbf{r}_A$, which are composed of $N-M$ unspoofed authentic signals and M spoofed authentic signals, are given by

$$\mathbf{r}_A = \sum_{i=1}^{N} \mathbf{r}_A^i = \mathbf{Q}_A \mathbf{a}_A. \tag{2}$$

In equation (2), $\mathbf{Q}_A$ is the basis matrix of the N authentic signals and is defined as

$$\mathbf{Q}_A = [\mathbf{q}_A^1, \ldots, \mathbf{q}_A^i, \ldots, \mathbf{q}_A^N]_{L\times N}, \tag{3}$$

where

$$\mathbf{q}_A^i = \begin{bmatrix} d_A^i(t_1)C_A^i(t_1)e^{j(2\pi f_A^i t_1+\theta_A^i)} \\ \vdots \\ d_A^i(t_l)C_A^i(t_l)e^{j(2\pi f_A^i t_l+\theta_A^i)} \\ \vdots \\ d_A^i(t_L)C_A^i(t_L)e^{j(2\pi f_A^i t_L+\theta_A^i)} \end{bmatrix}, \tag{4}$$

and the parameters $d_A^i(t_l)$, $C_A^i(t_l)$,f_A^i and θ_A^i denote the navigation data, the PRN code, the carrier frequency (intermediate frequency) and the carrier phase of the ith authentic signal, respectively. Additionally, in equation (2), the amplitude vector $\mathbf{a}_A$ of the N authentic signals is defined as

$$\mathbf{a}_A = [a_A^1, \ldots, a_A^i, \ldots, a_A^N]^T, \tag{5}$$

where a_A^i is the amplitude of the ith authentic signal.

Similarly, the M spoofing signals are also given by

$$\mathbf{r}_S = \sum_{i=1}^{M} \mathbf{r}_S^i = \mathbf{Q}_S\mathbf{a}_S. \tag{6}$$

The matrix $\mathbf{Q}_S$ is the basis matrix of the M spoofing signals and can also be expressed as

$$\mathbf{Q}_S = [\mathbf{q}_S^1, \ldots, \mathbf{q}_S^i, \ldots, \mathbf{q}_S^M]_{L\times M}, \tag{7}$$

where

$$\mathbf{q}_S^i = \begin{bmatrix} d_S^i(t_1)C_S^i(t_1)e^{j(2\pi f_S^i t_1+\theta_S^i)} \\ \vdots \\ d_S^i(t_l)C_S^i(t_l)e^{j(2\pi f_S^i t_l+\theta_S^i)} \\ \vdots \\ d_S^i(t_L)C_S^i(t_L)e^{j(2\pi f_S^i t_L+\theta_S^i)} \end{bmatrix}. \tag{8}$$

Likewise, the parameters $d_S^i(t_l)$, $C_S^i(t_l)$, f_S^i and θ_S^i denote the navigation data, the PRN code, the carrier frequency (intermediate frequency) and the carrier phase of the ith spoofing signal, respectively. The amplitude vector of the M spoofing signals $\mathbf{a}_S$ is written as

$$\mathbf{a}_S = [a_S^1, \ldots, a_S^i, \ldots, a_S^M]^T, \tag{9}$$

where a_S^i is the amplitude of the ith spoofing signal.

If the spoofing signals have been successfully detected, after the acquisition, tracking, and decoding processes, the PRN code delays, navigation data, carrier frequencies and carrier phases of the spoofing signals can be completely determined. Then, the basis matrix $\mathbf{Q}_S$ of the spoofing signals can be reconstructed as equation (7). Consequently, the subspace projection matrix of the spoofing signals is known as

$$\mathbf{H} = \mathbf{Q}_S\left(\mathbf{Q}_S^H\mathbf{Q}_S\right)^{-1}\mathbf{Q}_S^H. \tag{10}$$

Next, the null space of the spoofing signals is obtained as

$$\mathbf{H}_C = \mathbf{I} - \mathbf{H}. \tag{11}$$

Because the projection of the spoofing signals $\mathbf{r}_S$ onto the null space $\mathbf{H}_C$ is $\mathbf{0}$:

$$\begin{aligned} \mathbf{H}_C\mathbf{r}_S &= (\mathbf{I}-\mathbf{H})\mathbf{r}_S = (\mathbf{I}-\mathbf{H})\mathbf{Q}_S\mathbf{a}_S \\ &= \mathbf{Q}_S\mathbf{a}_S - \mathbf{Q}_S\left(\mathbf{Q}_S^H\mathbf{Q}_S\right)^{-1}\mathbf{Q}_S^H\mathbf{Q}_S\mathbf{a}_S \\ &= \mathbf{Q}_S\mathbf{a}_S - \mathbf{Q}_S\left[\left(\mathbf{Q}_S^H\mathbf{Q}_S\right)^{-1}\mathbf{Q}_S^H\mathbf{Q}_S\right]\mathbf{a}_S \\ &= \mathbf{Q}_S\mathbf{a}_S - \mathbf{Q}_S\mathbf{a}_S \\ &= \mathbf{0}, \end{aligned} \tag{12}$$

by projecting the received signal $\mathbf{r}_{IF}$ onto the complementary space $\mathbf{H}_C$, we have

$$\begin{aligned} \mathbf{r} &= \mathbf{H}_C\mathbf{r}_{IF} = (\mathbf{I}-\mathbf{H})\mathbf{r}_{IF} \\ &= \underbrace{\mathbf{r}_{IF}}_{\text{received IF signal}} - \underbrace{\mathbf{H}\mathbf{r}_{IF}}_{\text{projection}} \\ &= \underbrace{(\mathbf{I}-\mathbf{H})\mathbf{r}_A}_{\text{authentic signals}} + \underbrace{(\mathbf{I}-\mathbf{H})\mathbf{r}_S}_{\text{spoofing signals}} + \underbrace{(\mathbf{I}-\mathbf{H})\mathbf{n}}_{\text{noise}} \\ &= \underbrace{(\mathbf{I}-\mathbf{H})\mathbf{r}_A}_{\text{authentic signals}} + \underbrace{\mathbf{0}}_{\text{spoofing signals}} + \underbrace{(\mathbf{I}-\mathbf{H})\mathbf{n}}_{\text{noise}} \\ &= \underbrace{(\mathbf{I}-\mathbf{H})\mathbf{r}_A}_{\text{authentic signals}} + \underbrace{(\mathbf{I}-\mathbf{H})\mathbf{n}}_{\text{noise}}, \end{aligned} \tag{13}$$

in which the spoofing signals have been successfully mitigated after the projection operation.

Since both the self-correlation of the same PRN code with different delays and the cross-correlation of different PRN codes are very small, the above projection result is approximated as

$$\begin{aligned} \mathbf{r} &= (\mathbf{I}-\mathbf{H})\mathbf{r}_A + (\mathbf{I}-\mathbf{H})\mathbf{n} \\ &\approx \mathbf{r}_A + (\mathbf{I}-\mathbf{H})\mathbf{n}, \end{aligned} \tag{14}$$

The detailed proof is presented in Appendix A. Note that, the proposed spoofing mitigation method is based on subspace projection in PRN code domain and is achieved by digital IF signal processing. So, it is independent with the number of antennas and can be deployed in both single antenna receiver and multiple antenna receivers.

III. PERFORMANCE ANALYSIS

As discussed in the previous sections, when reconstructing the the basis matrix $\mathbf{Q}_S$, the PRN code delays, navigation data, carrier frequencies, and carrier phases of the spoofing signals are required. However, in this section, we will prove that the carrier phases and navigation data information are unnecessary. Thus, only utilizing carrier frequencies and PRN code delays can achieve spoofing mitigation. Additionally, the influence of the Doppler frequency estimation error and the length of each projection operation are also evaluated.

A. CARRIER PHASE

According to the construction of the basis matrix, equation (7) can be rewritten as

$$\mathbf{Q}_S = [\tilde{\mathbf{q}}_S^1, \ldots, \tilde{\mathbf{q}}_S^i, \ldots, \tilde{\mathbf{q}}_S^M]\Theta = \tilde{\mathbf{Q}}_S\Theta, \tag{15}$$

where

$$\tilde{\mathbf{q}}_S^i = \begin{bmatrix} d_S^i(t_1)C_S^i(t_1)e^{j(2\pi f_S^i t_1)} \\ \vdots \\ d_S^i(t_l)C_S^i(t_l)e^{j(2\pi f_S^i t_l)} \\ \vdots \\ d_S^i(t_L)C_S^i(t_L)e^{j(2\pi f_S^i t_L)} \end{bmatrix}. \tag{16}$$

The matrix Θ is the carrier phase matrix, which denotes the initial carrier phases of the spoofing signals and is given by

$$\Theta = \mathrm{diag}\{e^{j\theta_S^1}, \ldots, e^{j\theta_S^i}, \ldots, e^{j\theta_S^M}\}. \tag{17}$$

Thus, the spoofing space projection matrix $\mathbf{H}$ can be rearranged as

$$\begin{aligned} \mathbf{H} &= \mathbf{Q}_S\left(\mathbf{Q}_S^H\mathbf{Q}_S\right)^{-1}\mathbf{Q}_S^H \\ &= \left(\tilde{\mathbf{Q}}_S\Theta\right)\left[\left(\tilde{\mathbf{Q}}_S\Theta\right)^H\left(\tilde{\mathbf{Q}}_S\Theta\right)\right]^{-1}\left(\tilde{\mathbf{Q}}_S\Theta\right)^H \\ &= \left(\tilde{\mathbf{Q}}_S\Theta\right)\left[\Theta^{-1}\left(\tilde{\mathbf{Q}}_S^H\tilde{\mathbf{Q}}_S\right)^{-1}\left(\Theta^H\right)^{-1}\right]\left(\Theta^H\tilde{\mathbf{Q}}_S^H\right) \\ &= \tilde{\mathbf{Q}}_S\left(\Theta\Theta^{-1}\right)\left(\tilde{\mathbf{Q}}_S^H\tilde{\mathbf{Q}}_S\right)^{-1}\left[\left(\Theta^H\right)^{-1}\Theta^H\right]\tilde{\mathbf{Q}}_S^H \\ &= \tilde{\mathbf{Q}}_S\left(\tilde{\mathbf{Q}}_S^H\tilde{\mathbf{Q}}_S\right)^{-1}\tilde{\mathbf{Q}}_S^H, \end{aligned} \tag{18}$$

where $\Theta\Theta^{-1} = \mathbf{I}_M$ and $\left(\Theta^H\right)^{-1}\Theta^H = \mathbf{I}_M$.

The above result shows that the carrier phase matrix Θ is independent of the spoofing space projection matrix $\mathbf{H}$. Therefore, the carrier phases of the spoofing signals can be neglected when acquiring the parameters of the spoofing signals.

B. NAVIGATION DATA

By choosing the appropriate sample length L to ensure that the navigation data of the spoofing signals are constant in each projection operation,

$$d_S^i(t_1) = \ldots = d_S^i(t_l) = \ldots = d_S^i(t_L) = D_S^i, \tag{19}$$

the basis matrix can be constructed as

$$\mathbf{Q}_S = [\hat{\mathbf{q}}_S^1, \ldots, \hat{\mathbf{q}}_S^i, \ldots, \hat{\mathbf{q}}_S^M]\mathbf{D} = \hat{\mathbf{Q}}_S\mathbf{D}, \tag{20}$$

where

$$\hat{\mathbf{q}}_S^i = \begin{bmatrix} C_S^i(t_1)e^{j(2\pi f_S^i t_1 + \theta_S^i)} \\ \vdots \\ C_S^i(t_l)e^{j(2\pi f_S^i t_l + \theta_S^i)} \\ \vdots \\ C_S^i(t_L)e^{j(2\pi f_S^i t_L + \theta_S^i)} \end{bmatrix}. \tag{21}$$

The matrix $\mathbf{D}$ is the navigation data matrix that represents the navigation data of the spoofing signals and is given by

$$\mathbf{D} = \mathrm{diag}\{D_S^1, \ldots, D_S^i, \ldots, D_S^M\}. \tag{22}$$

Thus, the spoofing space projection matrix $\mathbf{H}$ is presented as

$$\begin{aligned} \mathbf{H} &= \mathbf{Q}_S\left(\mathbf{Q}_S^H\mathbf{Q}_S\right)^{-1}\mathbf{Q}_S^H \\ &= \left(\hat{\mathbf{Q}}_S\mathbf{D}\right)\left[\left(\hat{\mathbf{Q}}_S\mathbf{D}\right)^H\left(\hat{\mathbf{Q}}_S\mathbf{D}\right)\right]^{-1}\left(\hat{\mathbf{Q}}_S\mathbf{D}\right)^H \\ &= \left(\hat{\mathbf{Q}}_S\mathbf{D}\right)\left[\mathbf{D}^{-1}\left(\hat{\mathbf{Q}}_S^H\hat{\mathbf{Q}}_S\right)^{-1}\left(\mathbf{D}^H\right)^{-1}\right]\left(\mathbf{D}^H\hat{\mathbf{Q}}_S^H\right) \\ &= \hat{\mathbf{Q}}_S\left(\mathbf{D}\mathbf{D}^{-1}\right)\left(\hat{\mathbf{Q}}_S^H\hat{\mathbf{Q}}_S\right)^{-1}\left[\left(\mathbf{D}^H\right)^{-1}\mathbf{D}^H\right]\hat{\mathbf{Q}}_S^H \\ &= \hat{\mathbf{Q}}_S\left(\hat{\mathbf{Q}}_S^H\hat{\mathbf{Q}}_S\right)^{-1}\hat{\mathbf{Q}}_S^H, \end{aligned} \tag{23}$$

where $\mathbf{D}\mathbf{D}^{-1} = \mathbf{I}_M$ and $\left(\mathbf{D}^H\right)^{-1}\mathbf{D}^H = \mathbf{I}_M$.

Thus, the navigation data matrix $\mathbf{D}$ is demonstrated to be independent of the spoofing space projection matrix $\mathbf{H}$ when the appropriate L is chosen to ensure that the navigation data of the spoofing signals are constant in each projection operation. In this context, the navigation data of the spoofing signals are not required for the subspace projection algorithm. Moreover, because the period of the navigation data is considerably longer than that of the projection operation, the constraint can be easily achieved.

C. ESTIMATION ERROR OF THE DOPPLER FREQUENCY

The Doppler frequency of a spoofing signal is extracted from the corresponding tracking loop. Because of the existence of loop noise, the estimation error of the Doppler frequency will be introduced, which will generate a bias in the basis matrix and reduce the performance of the proposed anti-spoofing algorithm. In this subsection, we will deduce the relationship between the anti-spoofing ability and the estimation error of the Doppler frequency. To obtain the closed-form expressions, we assume that there is only one spoofing signal.[1] Thus, the basis matrix $\mathbf{Q}_S$ is simplified to a basis vector $\mathbf{q}_S$.

Let Δf denote the estimation error of the Doppler frequency; then, the constructed basis vector $\mathbf{q}_S$ is written as

$$\mathbf{q}_S = \Phi\hat{\mathbf{q}}_S, \tag{24}$$

where the phase bias matrix Φ, which is induced by the estimation error of the Doppler frequency, is given by

$$\Phi = \mathrm{diag}\{e^{j2\pi\Delta f t_1}, \ldots, e^{j2\pi\Delta f t_l}, \ldots, e^{j2\pi\Delta f t_L}\}, \tag{25}$$

and the actual basis vector $\hat{\mathbf{q}}_S$ is presented as

$$\hat{\mathbf{q}}_S = \begin{bmatrix} d_S(t_1)C_S(t_1)e^{j(2\pi f_S t_1 + \theta_S)} \\ \vdots \\ d_S(t_l)C_S(t_l)e^{j(2\pi f_S t_l + \theta_S)} \\ \vdots \\ d_S(t_L)C_S(t_L)e^{j(2\pi f_S t_L + \theta_S)} \end{bmatrix}. \tag{26}$$

[1] This hypothesis is corresponding to the distributed anti-spoofing structure shown in Fig. 2(b) and Fig. 3.

Considering $\Phi^H\Phi = \mathbf{I}_L$ and $\left(\hat{\mathbf{q}}_S^H\hat{\mathbf{q}}_S\right)^{-1} = \frac{1}{L}$ and substituting equation (24) into equation (10), the projection matrix is transformed as

$$\begin{aligned}\mathbf{H} &= \mathbf{q}_S\left(\mathbf{q}_S^H\mathbf{q}_S\right)^{-1}\mathbf{q}_S^H \\ &= \left(\Phi\hat{\mathbf{q}}_S\right)\left[\left(\Phi\hat{\mathbf{q}}_S\right)^H\left(\Phi\hat{\mathbf{q}}_S\right)\right]^{-1}\left(\Phi\hat{\mathbf{q}}_S\right)^H \\ &= \left(\Phi\hat{\mathbf{q}}_S\right)\left(\hat{\mathbf{q}}_S^H\Phi^H\Phi\hat{\mathbf{q}}_S\right)^{-1}\left(\Phi\hat{\mathbf{q}}_S\right)^H \\ &= \left(\Phi\hat{\mathbf{q}}_S\right)\left[\hat{\mathbf{q}}_S^H\left(\Phi^H\Phi\right)\hat{\mathbf{q}}_S\right]^{-1}\left(\Phi\hat{\mathbf{q}}_S\right)^H \\ &= \left(\Phi\hat{\mathbf{q}}_S\right)\left(\hat{\mathbf{q}}_S^H\hat{\mathbf{q}}_S\right)^{-1}\left(\Phi\hat{\mathbf{q}}_S\right)^H \\ &= \frac{1}{L}\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H. \qquad (27)\end{aligned}$$

Let $\Delta\mathbf{r}_S$ denote the residual spoofing signal, and we can obtain

$$\Delta\mathbf{r}_S = \mathbf{r}_S - \mathbf{H}\mathbf{r}_S = \hat{\mathbf{q}}_S a_s - \mathbf{H}\hat{\mathbf{q}}_S a_s. \qquad (28)$$

Thus, the power of the residual spoofing signal can be defined as

$$\begin{aligned}\Delta P_S &= \frac{1}{L}\|\Delta\mathbf{r}_S\|_2^2 \\ &= a_S^2\left[1 - \frac{1}{L^2}\left(\frac{\sin\left(\frac{\pi\Delta fL}{F_S}\right)}{\sin\left(\frac{\pi\Delta f}{F_S}\right)}\right)^2\right]. \qquad (29)\end{aligned}$$

where F_S is the sampling frequency. The detailed calculation is provided in Appendix B.

Because the sampling frequency F_S is much larger than the estimation error of the Doppler frequency Δf, the power of the residual spoofing signal can be approximated as

$$\Delta P_S \approx a_S^2\left[1 - \text{sinc}^2\left(\frac{\Delta fL}{F_S}\right)\right], \qquad (30)$$

where $\text{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$.

Therefore, the output SIR (Signal-to-Interference Ratio) of the spoofing mitigator can be expressed as

$$\begin{aligned}SIR_{out} &= \frac{P_A^{out}}{\Delta P_S} = \frac{\frac{1}{L}\|(\mathbf{I}-\mathbf{H})\mathbf{r}_A\|_2^2}{\Delta P_S} \\ &\approx \frac{\|\mathbf{r}_A\|_2^2}{L\Delta P_S} = \frac{a_A^2}{a_S^2\left[1 - \text{sinc}^2\left(\frac{\Delta fL}{F_S}\right)\right]}. \qquad (31)\end{aligned}$$

After transforming the output SIR into decibel form, we have

$$SIR_{out}(\text{dB}) = SIR_{in}(\text{dB}) + \mu, \qquad (32)$$

where $SIR_{in}(\text{dB})$ is the input SIR of the spoofing mitigator, which is given by

$$SIR_{in}(\text{dB}) = 10\lg\left(\frac{a_A^2}{a_S^2}\right), \qquad (33)$$

and μ is defined as the anti-spoofing gain, expressed as

$$\mu = -10\lg\left[1 - \text{sinc}^2\left(\frac{\Delta fL}{F_S}\right)\right]. \qquad (34)$$

In this way, the relationship between the anti-spoofing performance and the estimation error of the Doppler frequency Δf is constructed. In real receivers, the estimation error of the Doppler frequency of the track loop is on the order of 10^0 or 10^1 Hz, whereas the sampling frequency is always on the order of 10^6 Hz. Thus, the anti-spoofing gain will decrease as the estimation error of the Doppler frequency increases.

D. LENGTH OF THE PROJECTION OPERATION

The derived anti-spoofing gain μ is a function of the estimation error of the Doppler frequency and the length of the projection operation. When the estimation error of the Doppler frequency is set to be Δf, for a desired anti-spoofing gain μ, the maximum length of the projection operation L_{max} is the solution of the following transcendental equation:

$$\text{sinc}\left(\frac{\Delta fL_{max}}{F_S}\right) = \sqrt{1 - 10^{\frac{SIR_{in}(\text{dB}) - SIR_{out}(\text{dB})}{10}}}, \qquad (35)$$

which can be solved using a numerical method. It can be clearly observed that for the given anti-spoofing gain μ, the maximum length of the projection operation L_{max} is inversely proportional to the estimation error of the Doppler frequency Δf.

Additionally, because the PRN codes are not perfectly orthogonal, after spoofing-mitigation processing, the authentic signal will also exhibit a power loss resulting from the projection operation. Let ΔP_A denote the power loss. Then, the ratio between the power loss and the total input power can be presented as

$$\begin{aligned}\frac{\Delta P_A}{P_A} &= \frac{\frac{1}{L}\|\mathbf{H}\mathbf{r}_A\|_2^2}{\frac{1}{L}\|\mathbf{r}_A\|_2^2} = \frac{\|a_A\mathbf{H}\mathbf{q}_A\|_2^2}{La_A^2} \\ &= \frac{1}{L}\|\mathbf{H}\mathbf{q}_A\|_2^2 = \frac{1}{L}\|\mathbf{q}_S(\mathbf{q}_S^H\mathbf{q}_S)^{-1}\mathbf{q}_S^H\mathbf{q}_A\|_2^2 \\ &= \frac{1}{L^3}\|\mathbf{q}_S\mathbf{q}_S^H\mathbf{q}_A\|_2^2 = \frac{1}{L^3}\|\mathbf{q}_S\|_2^2|\mathbf{q}_S^H\mathbf{q}_A|^2 \\ &= \frac{1}{L^2}|\mathbf{q}_S^H\mathbf{q}_A|^2, \qquad (36)\end{aligned}$$

where $|\mathbf{q}_S^H\mathbf{q}_A|$ is the correlation between the spoofing signal and the spoofed authentic signal. This correlation result represents the self-correlation of the specific PRN code, which is determined by the code design and relative code delay. When the spoofing signal and the spoofed authentic signal have different code delays, the value of $|\mathbf{q}_S^H\mathbf{q}_A|$ will be considerably smaller than L, which means that the power loss is inversely proportional to L^2.

However, when the code delays of the spoofing signal and spoofed authentic signal are identical, the correlation result will be approximately equal to L, which indicates that the loss is almost equal to the total input power. Therefore, if the spoofing signal and the spoofed authentic signal have the same code delay, both will be eliminated simultaneously. The experimental results in Section V will verify this conclusion. Fortunately, the probability of two received signals sharing

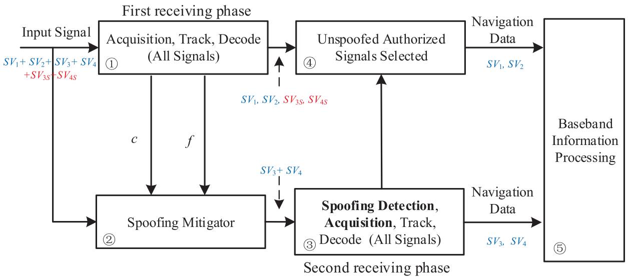

First receiving phase
Input Signal
$SV_1+SV_2+SV_3+SV_4$
$+SV_{3S}+SV_{4S}$
Acquisition, Track, Decode (All Signals)
①
Unspoofed Authorized Signals Selected
④
Navigation Data
SV_1, SV_2
SV_1, SV_2, SV_{3S}, SV_{4S}
c
f
SV_3+SV_4
Spoofing Mitigator
②
Spoofing Detection, Acquisition, Track, Decode (All Signals)
③
Navigation Data
SV_3, SV_4
Baseband Information Processing
⑤
Second receiving phase

FIGURE 1. An anti-spoofing receiver with a centralized spoofing-mitigation module.

the same code delay is negligible. Because all accessed signals are independent, especially for the common spoofing signals generated by the open loop signal simulator [3], the probability that two received signals will have an identical code delay is $\frac{1}{L_C}$, where L_C is the length of the PRN code. For a GPS system, the length of the C/A code is 1023, and the probability is approximately 0.001. Therefore, although the proposed anti-spoofing scheme will be ineffective when the spoofing signal and the spoofed authentic signal have the same code delay, because the probability of this scenario is quite small, the proposed spoofing-mitigation algorithm can still be utilized in GNSS receivers.

IV. RECEIVER STRUCTURE

We have theoretically described and demonstrated the validity of the proposed spoofing-mitigation algorithm in the previous two sections. In this section, the anti-spoofing receiver structure will be presented in detail, and both centralized and distributed anti-spoofing schemes are discussed. Note that to successfully deceive target GNSS receivers, the power of spoofing signal is always higher than the power of the corresponding spoofed authentic signal [2], [16]; therefore, the receiver will acquire the spoofing signal first.

A. ANTI-SPOOFING RECEIVER WITH A CENTRALIZED SPOOFING-MITIGATION MODULE

Fig. 1 shows the structure of an anti-spoofing receiver with a centralized spoofing-mitigation module. For this type of anti-spoofing receiver, only one subspace projection operation is required during each anti-spoofing process, and the basis matrix $\mathbf{Q}_S$ is constructed by the parameters of all the acquired and tracked signals at the first receiving phase. To better explain the anti-spoofing mechanism, a scenario containing four authentic signals and two spoofing signals is utilized. We assume that the input signal consists of four authentic signals, SV_1, SV_2, SV_3, and SV_4, and two spoofing signals, SV_{3S} and SV_{4S}.[2] Then, the following steps describe the anti-spoofing processing procedure in detail:

Step 1: At the first receiving phase, SV_1, SV_2, SV_{3S} and SV_{4S} will be acquired and tracked; the PRN code delays and carrier frequencies of SV_1, SV_2, SV_{3S} and SV_{4S} will be obtained and input into the spoofing mitigator. At this point, the receiver cannot identify that SV_{3S} and SV_{4S} are spoofing signals.

Step 2: The original received IF signal will be processed by the spoofing mitigator depicted in Fig. 2(a). First, construct the basis matrix $\mathbf{Q}_S$ with the obtained parameters in *Step 1*; then, calculate the subspace projection matrix $\mathbf{H}$, project the input signals onto the subspace, and subtract the projection result from the input signal. At this step, SV_1, SV_2, SV_{3S} and SV_{4S} will be treated as spoofing signals and will be canceled, whereas SV_3 and SV_4 will be maintained.

Step 3: At the second receiving phase, the output of the spoofing mitigator will go through acquisition, tracking and decoding again; SV_3 and SV_4, which are the spoofed authentic signals, will be acquired and tracked, which means that the received SV_{3S} and SV_{4S} at the first receiving phase are spoofing signals.

Step 4: Select the unspoofed authentic signals SV_1 and SV_2 from the output of *Step 1*.

Step 5: The anti-spoofing is achieved, and the receiver continues to process the navigation data.

B. ANTI-SPOOFING RECEIVER WITH A DISTRIBUTED SPOOFING-MITIGATION MODULE

An anti-spoofing receiver with a distributed spoofing-mitigation module is presented in Fig. 3. For this type of anti-spoofing receiver, multiple subspace projection operations are required. Using the same example in the centralized structure, the processing of the distributed structure consists of the following steps:

Step 1: As with the centralized receiver structure, at the first receiving phase, SV_1, SV_2, SV_{3S} and SV_{4S} will be acquired and tracked; the PRN code delays and carrier frequencies of SV_1, SV_2, SV_{3S} and SV_{4S} will be obtained and delivered to the spoofing mitigators.

Step 2: Because four signals are detected at the first receiving phase, four spoofing mitigators will be deployed to process the original received IF signal. First, in each mitigator, construct each basis vector $\mathbf{q}_S$ with the obtained parameters of each acquired and tracked signal in the first receiving phase. The ith mitigator is shown in Fig. 2(b), and the ith basis vector $\mathbf{q}_S^i$ is constructed by the acquired parameters of the ith signal. Then, calculate the subspace projection matrix $\mathbf{H}$ of each spoofing mitigator. Next, the original IF signal will pass through each mitigator in parallel, and the ith signal component of the IF signal will be canceled at the ith spoofing mitigator; for example, the SV_{3S} component of the original IF signal will be mitigated by the spoofing mitigator that is constructed by the parameters of SV_{3S}.

Step 3: There are multiple (four) receiving modules in the second receiving phase, and each receiving module can only acquire and track one signal. The output of each spoofing mitigator will be injected into the corresponding

[2] SV_{3S} is the spoofing signal corresponding to the authentic signal SV_3, which means that SV_{3S} and SV_3 share the same PRN code, and SV_{3S} has a higher power than SV_3. Similarly, SV_{4S} is the spoofing signal corresponding to the authentic signal SV_4, they share the same PRN code, and SV_{4S} has a higher power than SV_4.

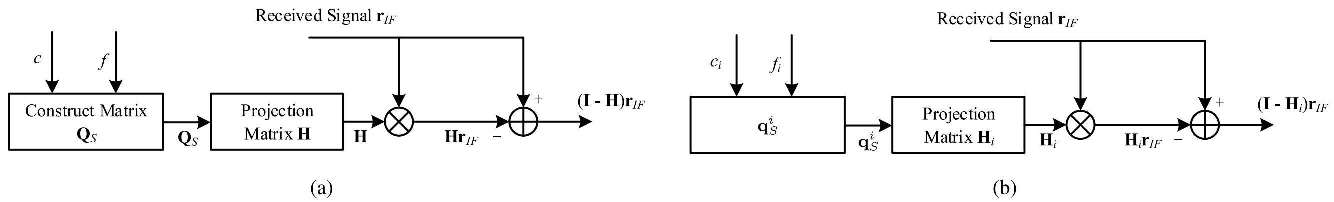

Received Signal $\mathbf{r}_{IF}$
c
f
Construct Matrix $\mathbf{Q}_S$
$\mathbf{Q}_S$
Projection Matrix $\mathbf{H}$
$\mathbf{H}$
$\mathbf{Hr}_{IF}$
+
−
$(\mathbf{I}-\mathbf{H})\mathbf{r}_{IF}$
(a)
Received Signal $\mathbf{r}_{IF}$
c_i
f_i
$\mathbf{q}_S^i$
$\mathbf{q}_S^i$
Projection Matrix $\mathbf{H}_i$
$\mathbf{H}_i$
$\mathbf{H}_i\mathbf{r}_{IF}$
+
−
$(\mathbf{I}-\mathbf{H}_i)\mathbf{r}_{IF}$
(b)

FIGURE 2. The structure of the spoofing mitigator. (a) Type I. (b) Type II.

TABLE 1. Computational complexity.

	Multiplication	Addition	Inverse
Centralized	$L(N^2+2N)+N^2$	$L(N^2+2N-1)-2N$	one $N \times N$ matrix
Distributed	$3LN+N$	$2LN-2N$	N 1×1 matrices

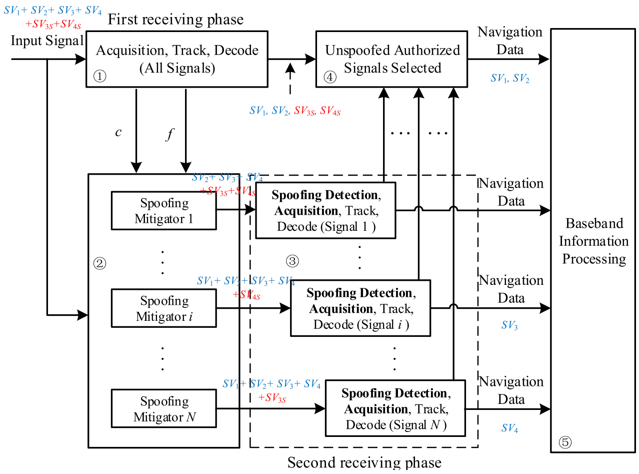


FIGURE 3. An anti-spoofing receiver with a distributed spoofing-mitigation module.

receiving module and will complete the acquisition, tracking and decoding procedures. For example, the first receiving module will acquire and track SV_1 again; however, the SV_1 has been removed by the first spoofing mitigator in *Step 2*, and thus, no signal will be detected by this receiving module. For the experimental scenario utilized in this section, the first and second receiving module will show that no signal is detected, and only the third and fourth receiving module will show that SV_3 and SV_4 are detected, respectively, which means that the received SV_{3S} and SV_{4S} at the first receiving phase are spoofing signals.

Step 4: Select the unspoofed authentic signals SV_1 and SV_2 from the output of *Step 1*;

Step 5: The anti-spoofing is achieved, and the receiver continues to process the navigation data.

Because spoofing signals are stronger than authentic signals, except in spoofing attacks, cross-correlation interference will also be introduced, which will severely reduce the acquisition probability and degrade the tracking loop performance. For the centralized anti-spoofing structure, all spoofing signals are mitigated in the spoofing mitigator prior to the acquisition of the spoofed authentic signals, which means that all the cross-correlation interference between the spoofing signals and spoofed authentic signals will also be eliminated. However, for the distributed anti-spoofing structure, only the ith spoofing signal is suppressed by the ith spoofing mitigator, and another $M-1$ spoofing signals remain in this channel. Thus, the remaining $M-1$ spoofing signals will introduce cross-correlation interference to the ith spoofed authentic signal.

The computational complexities of the two types of receiver structures are presented in Table 1. This table shows that the distributed spoofing mitigation module has a lower computational complexity. Thus, when the spoofing signals are not too strong, utilizing the distributed structure, which has low computational complexity, will conserve hardware resources. On the other hand, when the spoofing signals are very strong, the centralized structure should be used to simultaneously mitigate both spoofing attacks and cross-correlation interference.

According to the actual spoofing generator, we assume that the the power of spoofing signal is higher than the power of the corresponding spoofed authentic signal, so the receiver will acquire the spoofing signal first. However, when the power of spoofing signal is lower or similar with the power of the corresponding spoofed authentic signal, with the assistance of other spoofing detection methods, spoofing mitigation can still achieve by subspace projection processing; if no other spoofing detection methods in this scenario, the proposed anti-spoofing receiver can still detect the existence of spoofing signal, but can not distinguish which one of the signals acquired by the first and the second receiving phase[3] is spoofing signal.

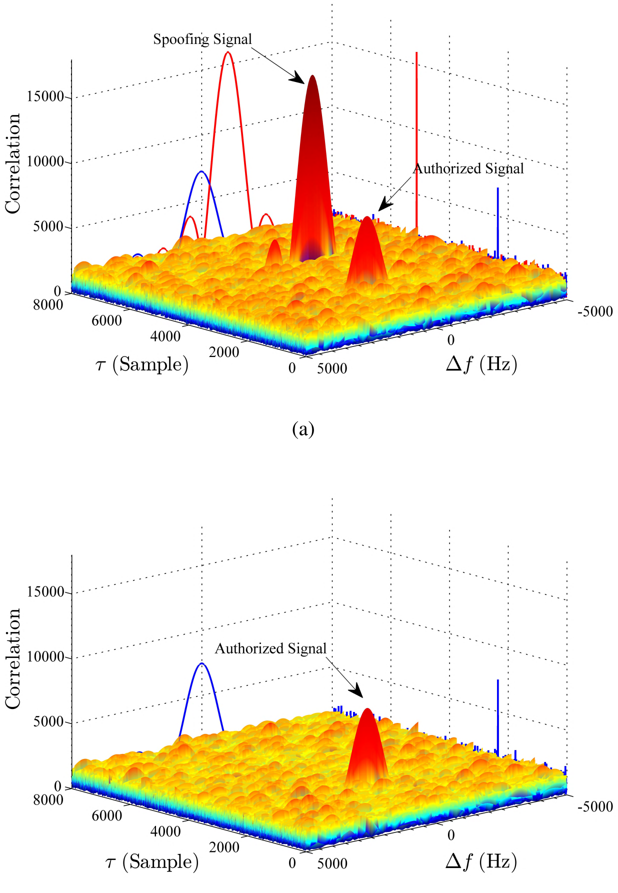
V. SIMULATION AND NUMERICAL RESULTS

We have theoretically investigated the spoofing-mitigation algorithm based on subspace projection. In this section, the acquisition of a Beidou B1I signal will be tested to verify

[3] Both of two receiving phase will acquire a signal with same PRN code, so the signal with this PRN code is spoofed.

TABLE 2. Simulation parameters.

Parameter	Value
PRN	4, 5, 6
IF	3.25 MHz
Sample Frequency	8 MHz
Integration time	1 ms
C/N_0 for authentic signal	44 dB-Hz
C/N_0 for spoofing signal	50 dB-Hz



(a)

(b)

FIGURE 4. Acquisition results for PRN 4 (different code delays). (a) Before spoofing mitigation. (b) After spoofing mitigation.

the validity of the proposed algorithm. The simulation parameters are listed in Table 2. In the simulation, the received IF signals consist of 3 spoofing signals and 3 spoofed authentic signals.

The acquisition results before and after spoofing mitigation for PRN 4 are presented in Fig. 4(a) and Fig. 4(b), respectively. In the simulation, for the spoofing PRN 4 signal, the Doppler frequency bias and the code delay are −1 kHz and 5120 samples, respectively, whereas those of the authentic PRN 4 signal are 0 Hz and 2354 samples, respectively. Before spoofing mitigation, as shown in Fig. 4(a), the results consist of two correlation peaks. Because the spoofing signal is 6 dB stronger than the authentic signal, the receiver will generally acquire the former. However, after mitigating the spoofing signal, only the correlation peak of the authentic signal is detected, which confirms the validity of the spoofing-mitigation algorithm based on subspace projection.

According to our analysis, spoofing signals will be completely eliminated if the corresponding basis matrix can be precisely reconstructed. We have demonstrated that the carrier phase and the navigation data are independent of the basis matrix of the spoofing signals. However, because of the existence of track loop noise, the Doppler frequency of the spoofing signals cannot be accurately estimated. Consequently, the constructed basis matrix of the spoofing signals will contain errors. Fig. 5 shows that the output SIR after mitigation processing decreases with increasing Doppler frequency estimation error when the input SIR is −6 dB. The theoretical results coincide with the simulation results, thus confirming the validity of equation (31). Because the error of the constructed basis matrix increases as the Doppler frequency estimation error increases, the constructed subspace will eventually no longer be the spoofing subspace, and the proposed anti-spoofing scheme will be invalid. The simulation results also show that the output SIR is almost equal to the input SIR when the Doppler frequency estimation error is on the order of 10^4 Hz.

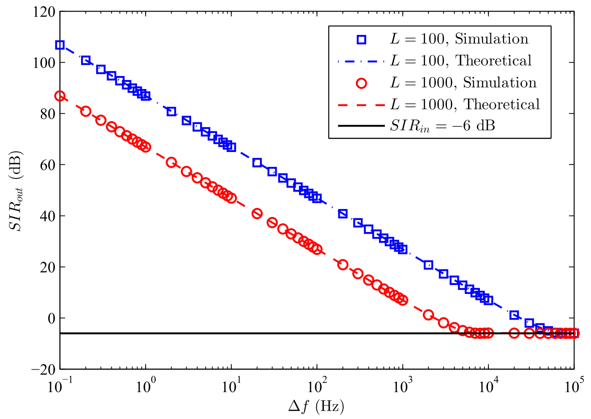


FIGURE 5. Output SIR vs. estimation error of the Doppler frequency.

Moreover, two lengths of the projection operation, $L = 100$ and $L = 1000$, are tested in Fig. 5. When the Doppler frequency estimation error is fixed, the shorter operation length results in a higher output SIR. Furthermore, Fig. 6 also shows the inversely proportional relationship between the projection operation length and the tolerable maximum estimation error of the Doppler frequency for a given anti-spoofing gain. The shorter operation length results in a larger tolerable maximum Doppler frequency estimation error. Therefore, from the perspective of spoofing signals, a shorter projection operation length should be chosen.

However, we have stated that the authentic signal also undergoes a power loss caused by the projection operation

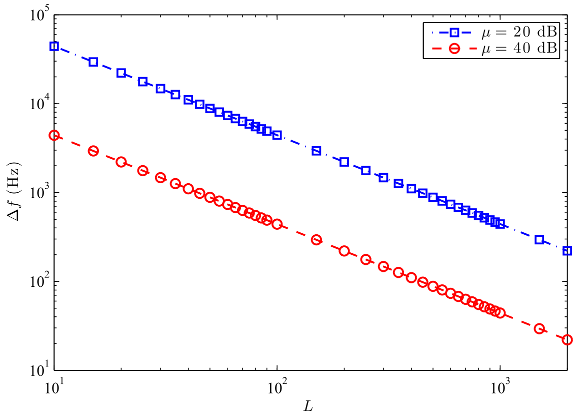


FIGURE 6. Estimation error of the Doppler frequency vs. the projection operation length.

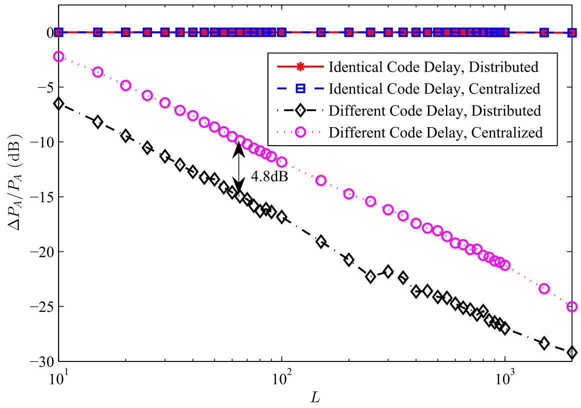


FIGURE 7. The ratio between the power loss and the total input power.

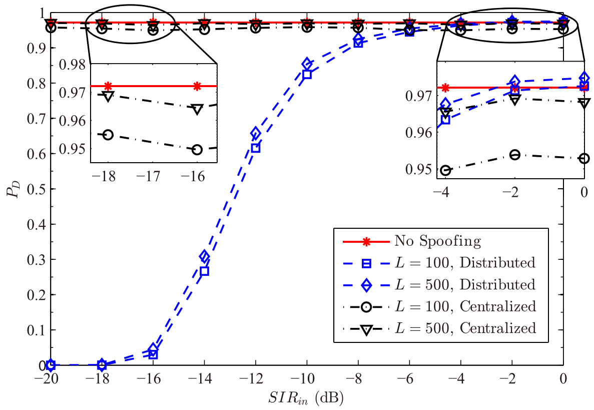


FIGURE 8. Acquisition probability for authentic PRN 4 (different code delays).

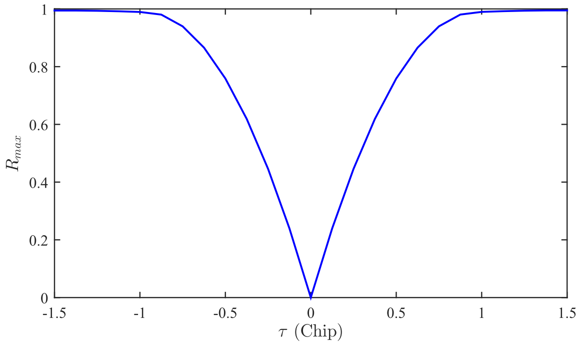


FIGURE 9. Normalized correlation peak vs. code delay bias.

after spoofing-mitigation processing. The ratio between the power loss and the total input power of the authentic signal is given by equation (36). The simulation results in Fig. 7 show the power loss caused by the projection operation. During the simulation, PRN 4 is chosen. When the authentic PRN 4 signal and the spoofing PRN 4 signal have different code delays, the ratio between the power loss and the total input power will decrease as the projection operation length increases. Thus, when the operation length is longer, less power will be lost. This is also confirmed by the acquisition probability in Fig. 8. For both the centralized and distributed structures, the acquisition probability for $L = 500$ is larger than that for $L = 100$. Thus, from the perspective of the authentic signal, a longer projection operation length should be chosen to minimize the power loss caused by the projection operation.

The simulation in Fig. 7 also shows that the distributed structure involves less power loss than the centralized structure. This is because there are three spoofing signals (PRN 4, PRN 5, and PRN 6), which means that one centralized projection is approximately equivalent to three distributed projections. For this reason, the centralized structure has approximately three times more power loss (4.8 dB) than the distributed structure. Theoretically, the power loss of the authentic signal will produce a reduction in the acquisition probability. Thus, the distributed structure should achieve a higher acquisition probability than the centralized structure. However, as shown by 8, only the acquisition probability in the low-SIR region gives this conclusion. In the high-SIR region, the achieved acquisition probability by the centralized structure is much higher than the value under the distributed receiver. For this condition, the main factor that determines the severe reduction in the acquisition probability under distributed processing is the strong cross-correlation generated by the other two spoofing signals (PRN 5 and PRN 6). Because the centralized structure can eliminate all cross-correlation during anti-spoofing processing, the achieved acquisition probability remains almost constant.

We have analyzed the Doppler frequency error and the projection length. Next, we will present the effect of the code delay bias between the spoofing signal and the corresponding authentic signal. Let τ denote the code delay bias, and Fig. 9 presents the acquired normalized correlation peak of authentic signal after subspace projection. When the bias is larger than 0.5 chip, the projection operation is effective. When the code delay bias is small (for example, $\tau < \frac{1}{4}Chip$), the residual authentic signal will be very weak and the projection operation is inoperative.

When the authentic signal and the spoofing signal have an identical code delay (bias $\tau = 0$), shown as Fig. 7, the power loss of the authentic signal is almost equal to the total input

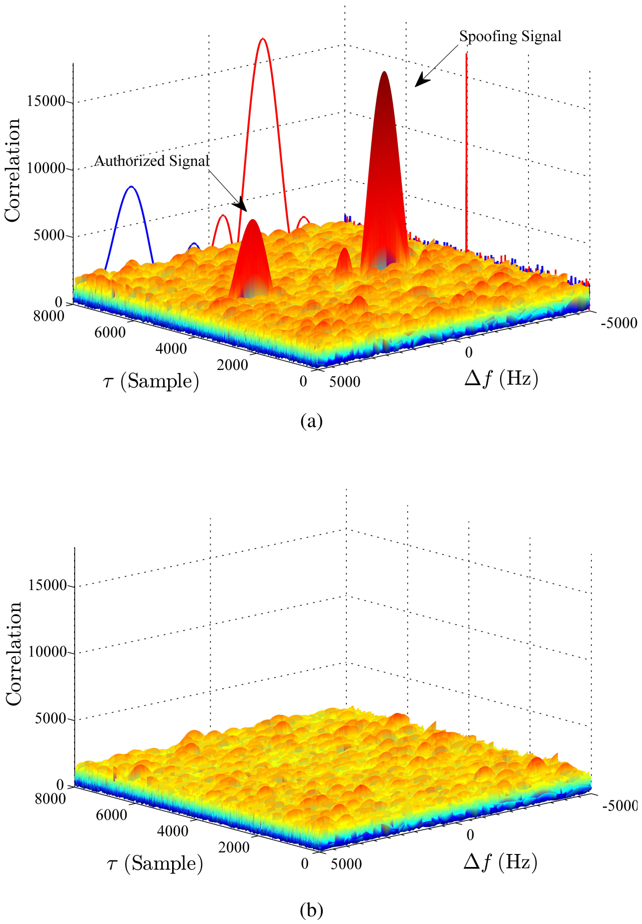


FIGURE 10. Acquisition results for PRN 4 (identical code delays). (a) Before spoofing mitigation. (b) After spoofing mitigation.

power for both distributed and centralized processing. This experimental result means that the authentic signal is also eliminated in this condition. The subspace (or the null space) is constructed based on the correlation property of the PRN code. So, when the authentic and the corresponding spoofing signal have the same code delay, they will have same correlation property and same subspace, thus, the authentic signal will be eliminated too by the subspace projection processing. The simulation in Fig. 10 confirms this deduction. In this simulation, for the spoofing signal (PRN 4), the Doppler frequency bias and the code delay are −2 kHz and 4032 samples, whereas for the authentic signal (PRN 4), the Doppler frequency bias and the code delay are 3 kHz and 4032 samples, respectively. Comparing the acquisition results in Figs. 10(a) and 10(b), it can be observed that after being processed by the proposed method, both the spoofing signal and the authentic signal are eliminated. So, for the scenario that the spoofing signal and the corresponding spoofed authentic signal share same code delay (for example, the intermediate spoofing attack), the subspace projection based spoofing mitigation algorithm will be meaningless. But for the common open loop spoofing attack, because the length of the GNSS PRN code is very large and because the code delays for the signals accessed by the receiver are independent, the probability that the spoofing signal and the authentic signal share the same code delay is negligible in a practical scenario. For example, for the Beidou B1I signal, this probability is 1/2046.

VI. CONCLUSION

In this paper, an anti-spoofing method based on subspace projection is developed. The proposed anti-spoofing technique can provide both spoofing detection and spoofing mitigation, and it can even be implemented in typical single-antenna receivers. Because only the Doppler frequency and code delay information are required, the proposed anti-spoofing method is more robust. However, almost all anti-spoofing schemes have limitations and can only counter a specific type of spoofing attack [1]–[3]. The precondition of the proposed anti-spoofing method in this paper is that the spoofing signal is stronger than the authentic signal. If this precondition is not met, the spoofing detection function will lose its effectiveness. However, when combined with other spoofing detection schemes, the spoofing signals can still be mitigated by the subspace projection algorithm to improve the security of the receiver.

APPENDIX A
PROOF OF EQUATION (14)

The element in the ith row and jth column of the matrix $\mathbf{Q}_S^H\mathbf{Q}_S$ is given by

$$\left(\mathbf{Q}_S^H\mathbf{Q}_S\right)_{i,j} = \begin{cases} L & i=j \\ \sum_{l=1}^{L}(\mathbf{q}_S^i)_l(\mathbf{q}_S^j)_l & i\neq j, \end{cases} \tag{A.1}$$

where $\sum_{l=1}^{L}(\mathbf{q}_S^i)_l(\mathbf{q}_S^j)_l = (\mathbf{q}_S^i)^H\mathbf{q}_S^j$ is the cross-correlation between the ith spoofing signal and the jth spoofing signal when $i\neq j$. For the case $i=j$, $\sum_{l=1}^{L}(\mathbf{q}_S^i)_l(\mathbf{q}_S^j)_l = (\mathbf{q}_S^i)^H\mathbf{q}_S^j = L$ is the self-correlation of the ith spoofing signal. Let C denote the maximum cross-correlation of two GNSS signals. Then, we have $C \ll L$. Therefore, the matrix $\mathbf{Q}_S^H\mathbf{Q}_S$ is approximately equal to the identity matrix, and we have

$$\mathbf{Q}_S^H\mathbf{Q}_S \approx L\mathbf{I}_M \text{ and } \left(\mathbf{Q}_S^H\mathbf{Q}_S\right)^{-1} \approx \frac{1}{L}\mathbf{I}_M. \tag{A.2}$$

Next, the lth entry of the vector $\frac{1}{L}\mathbf{Q}_S\mathbf{Q}_S^H\mathbf{q}_A^i$ is expressed as

$$\left(\frac{1}{L}\mathbf{Q}_S\mathbf{Q}_S^H\mathbf{q}_A^i\right)_l = \frac{1}{L}\sum_{m=1}^{M}(\mathbf{q}_S^m)_l\sum_{j=1}^{L}(\mathbf{q}_S^m)_j(\mathbf{q}_A^i)_j, \tag{A.3}$$

where $\sum_{j=1}^{L}(\mathbf{q}_S^m)_j(\mathbf{q}_A^i)_j = (\mathbf{q}_S^m)^H\mathbf{q}_A^i$ is the cross-correlation between the mth spoofing signal and the ith spoofed authentic signal. The maximum cross-correlation is also C, and as a result, the modulus is given by

$$\begin{aligned}\left|\frac{1}{L}(\mathbf{Q}_S\mathbf{Q}_S^H\mathbf{q}_A^i)_l\right| &= \frac{1}{L}\left|\sum_{m=1}^{M}(\mathbf{q}_S^m)_l\sum_{j=1}^{L}(\mathbf{q}_S^m)_j(\mathbf{q}_A^i)_j\right| \\ &\leq \frac{1}{L}\sum_{m=1}^{M}\left|(\mathbf{q}_S^m)_l\sum_{j=1}^{L}(\mathbf{q}_S^m)_j(\mathbf{q}_A^i)_j\right|\end{aligned}$$

$$= \frac{1}{L}\sum_{m=1}^{M}\left|(\mathbf{q}_S^m)_l\right|\left|\sum_{j=1}^{L}(\mathbf{q}_S^m)_j(\mathbf{q}_A^i)_j\right|$$

$$= \frac{1}{L}\sum_{m=1}^{M}\left|\sum_{j=1}^{L}(\mathbf{q}_S^m)_j(\mathbf{q}_A^i)_j\right| \tag{A.4}$$

Because the number of spoofing signals M is very small (less than 8) and because the ratio between the maximum cross-correlation C and the maximum self-correlation L is on the order of 10^{-2}, we can make the following approximations:

$$\left|\frac{1}{L}(\mathbf{Q}_S\mathbf{Q}_S^H\mathbf{q}_A^i)_l\right| \le \frac{MC}{L} \approx 0, \tag{A.5}$$

which can be further simplified to

$$\frac{1}{L}\mathbf{Q}_S\mathbf{Q}_S^H\mathbf{q}_A^i \approx \mathbf{0}_{L\times 1}. \tag{A.6}$$

To prove equation (14), first, substitute equation (2) into equation (13) and obtain

$$\begin{aligned}\mathbf{r} &= (\mathbf{I}-\mathbf{H})\mathbf{r}_A + (\mathbf{I}-\mathbf{H})\mathbf{n}\\ &= \sum_{i=1}^{N}(\mathbf{I}-\mathbf{H})\mathbf{r}_A^i + (\mathbf{I}-\mathbf{H})\mathbf{n}.\end{aligned} \tag{A.7}$$

By substituting equations (A.2) and (A.6) into equation (A.7), the ith entry of the summation can be presented as

$$\begin{aligned}(\mathbf{I}-\mathbf{H})\mathbf{r}_A^i &= a_A^i(\mathbf{I}-\mathbf{H})\mathbf{q}_A^i\\ &= a_A^i(\mathbf{q}_A^i - \mathbf{Q}_S\left(\mathbf{Q}_S^H\mathbf{Q}_S\right)^{-1}\mathbf{Q}_S^H\mathbf{q}_A^i)\\ &\approx a_A^i(\mathbf{q}_A^i - \frac{1}{L}\mathbf{Q}_S\mathbf{Q}_S^H\mathbf{q}_A^i)\\ &\approx a_A^i\mathbf{q}_A^i\\ &= \mathbf{r}_A^i,\end{aligned} \tag{A.8}$$

Finally, combining equations (A.8) and (A.7), equation (14) can be written as

$$\begin{aligned}\mathbf{r} &\approx \sum_{i=1}^{N}\mathbf{r}_A^i + (\mathbf{I}-\mathbf{H})\mathbf{n}\\ &= \mathbf{r}_A + (\mathbf{I}-\mathbf{H})\mathbf{n}.\end{aligned} \tag{A.9}$$

Note that the precondition of this proof is that the spoofing signal and the corresponding spoofed authentic signal share different code delay. When the code delay bias between ith spoofing signal and the corresponding spoofed authentic signal is very small (for example less than 1/4 chip), $\mathbf{H}\mathbf{q}_A^i$ can not be approximated to zero vector.

APPENDIX B
PROOF OF EQUATION (29)

We assume that the distributed anti-spoofing structure is used in the receiver as described by equation (27). Therefore, the constructed projection matrix $\mathbf{H}$ is written as $\mathbf{H} = \frac{1}{L}\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H$. Then, the power of the residual spoofing signal is calculated as

$$\begin{aligned}\Delta P_S &= \frac{1}{L}\|\Delta\mathbf{r}_S\|_2^2 = \frac{1}{L}\Delta\mathbf{r}_S^H\Delta\mathbf{r}_S\\ &= \frac{1}{L}(\mathbf{r}_S - \mathbf{H}\mathbf{r}_S)^H(\mathbf{r}_S - \mathbf{H}\mathbf{r}_S)\\ &= \frac{1}{L}\left(\mathbf{r}_S^H\mathbf{r}_S - \mathbf{r}_S^H\mathbf{H}\mathbf{r}_S - \mathbf{r}_S^H\mathbf{H}^H\mathbf{r}_S + \mathbf{r}_S^H\mathbf{H}^H\mathbf{H}\mathbf{r}_S\right)\\ &= \frac{a_S^2}{L}\left(\hat{\mathbf{q}}_S^H\hat{\mathbf{q}}_S - \hat{\mathbf{q}}_S^H\mathbf{H}\hat{\mathbf{q}}_S - \hat{\mathbf{q}}_S^H\mathbf{H}^H\hat{\mathbf{q}}_S + \hat{\mathbf{q}}_S^H\mathbf{H}^H\mathbf{H}\hat{\mathbf{q}}_S\right),\end{aligned} \tag{B.1}$$

where the four terms are respectively calculated as

$$\hat{\mathbf{q}}_S^H\hat{\mathbf{q}}_S = L, \tag{B.2}$$

$$\hat{\mathbf{q}}_S^H\mathbf{H}\hat{\mathbf{q}}_S = \frac{1}{L}\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S, \tag{B.3}$$

$$\hat{\mathbf{q}}_S^H\mathbf{H}^H\hat{\mathbf{q}}_S = \frac{1}{L}\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S, \tag{B.4}$$

$$\begin{aligned}\hat{\mathbf{q}}_S^H\mathbf{H}^H\mathbf{H}\hat{\mathbf{q}}_S &= \frac{1}{L^2}\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S\\ &= \frac{1}{L^2}\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H(\Phi^H\Phi)\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S\\ &= \frac{1}{L^2}\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S(\hat{\mathbf{q}}_S^H\hat{\mathbf{q}}_S)\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S\\ &= \frac{1}{L}\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S.\end{aligned} \tag{B.5}$$

Then, the residual power is simplified as

$$\Delta P_S = \frac{a_S^2}{L}\left(L - \frac{1}{L}\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S\right). \tag{B.6}$$

Let F_S denote the sampling frequency, which gives

$$\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S = \sum_{l=1}^{L}e^{j2\pi\Delta f_S t_l}, \tag{B.7}$$

and

$$\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S = \sum_{l=1}^{L}e^{-j2\pi\Delta f_S t_l}. \tag{B.8}$$

Thus, for the second term of equation (B.6), we have

$$\begin{aligned}\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S &= \left(\hat{\mathbf{q}}_S^H\Phi\hat{\mathbf{q}}_S\right)\left(\hat{\mathbf{q}}_S^H\Phi^H\hat{\mathbf{q}}_S\right)\\ &= \left(\sum_{l=1}^{L}e^{j2\pi\frac{\Delta f_S l}{F_S}}\right)\left(\sum_{l=1}^{L}e^{-j2\pi\frac{\Delta f_S l}{F_S}}\right)\\ &= \frac{2-2\cos\left(2\pi\frac{\Delta f_S L}{F_S}\right)}{2-2\cos\left(2\pi\frac{\Delta f_S}{F_S}\right)}\\ &= \left(\frac{\sin\left(\frac{\pi\Delta f L}{F_S}\right)}{\sin\left(\frac{\pi\Delta f}{F_S}\right)}\right)^2.\end{aligned} \tag{B.9}$$

Finally, the residual power is written as

$$\Delta P_S = a_S^2 \left[1 - \frac{1}{L^2} \left(\frac{\sin\left(\frac{\pi \Delta f L}{F_S}\right)}{\sin\left(\frac{\pi \Delta f}{F_S}\right)} \right)^2 \right]. \tag{B.10}$$

REFERENCES

[1] C. Günther, "A survey of spoofing and counter-measures," *Navigation*, vol. 61, no. 3, pp. 159–177, Sep. 2013.

[2] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navigat. Observat.*, vol. 2012, May 2012, Art. no. 127072.

[3] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[4] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proc. ION GPS/GNSS*, Portland, OR, USA, Sep. 2003, pp. 1543–1552.

[5] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

[6] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation*, vol. 59, no. 3, pp. 177–193, Sep. 2012.

[7] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N$_0$ measurements," *Int. J. Satellite Commun. Netw.*, vol. 30, no. 4, pp. 181–191, Jul./Aug. 2012.

[8] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. ION GNSS*, Long Beach, CA, USA, Sep. 2005, pp. 1285–1290.

[9] 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.

[10] B. W. O'Hanlon and M. L. Psiaki, "Real-time spoofing detection using correlation between two civil GPS receiver," in *Proc. ION GNSS*, Nashville, TN, USA, Sep. 2012, pp. 3584–3590.

[11] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in *Proc. ION GNSS*, Nashville, TN, USA, Sep. 2013, pp. 2949–2991.

[12] M. L. Psiaki *et al.*, "GNSS spoofing detection using two-antenna differential carrier phase," in *Proc. ION GNSS*, Tampa, FL, USA, Sep. 2014, pp. 2776–2800.

[13] F. Wang, H. Li, and M. Lu, "GNSS spoofing countermeasure with a single rotating antenna," *IEEE Access*, vol. 5, pp. 8039–8047, 2017.

[14] S. Han, D. Luo, W. Meng, and C. Li, "A novel anti-spoofing method based on particle filter for GNSS," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 5413–5418.

[15] A. Konovaltsev, S. Caizzone, M. Cuntz, and M. Meurer, "Autonomous spoofing detection and mitigation with a miniaturized adaptive antenna array," in *Proc. ION GNSS*, Tampa, FL, USA, Sep. 2014, pp. 2853–2861.

[16] C. E. McDowell, "GPS spoofer and repeater mitigation system using digital spatial nulling," U.S. Patent 7 250 903 B1, Jul. 31, 2007.

[17] J. Magiera and R. Katulski, "Applicability of null-steering for spoofing mitigation in civilian GPS," in *Proc. IEEE 79th Veh. Technol. Conf. (VTC Spring)*, May 2014, pp. 1–5.

[18] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," in *Proc. ION GNSS*, Nashville, TN, USA, Sep. 2012, pp. 1233–1243.

[19] P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals, and R. J. Hartnett, "GNSS spoof detection using shipboard IMU measurements," in *Proc. ION GNSS*, Tampa, FL, USA, Sep. 2014, pp. 745–758.

[20] N. I. Ziedan, "Investigating and utilizing the limitations of spoofing in a map-matching anti-spoofing algorithm," in *Proc. ION GNSS*, Tampa, FL, USA, Sep. 2014, pp. 2843–2852.

[21] 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. 475–487, Jul. 2015.

[22] L. L. Scharf and B. Friedlander, "Matched subspace detectors," *IEEE Trans. Signal Process.*, vol. 42, no. 8, pp. 2146–2157, Aug. 1994.

[23] J. Landon, B. D. Jeffs, and K. F. Warnick, "Model-based subspace projection beamforming for deep interference nulling," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1215–1228, Mar. 2012.

[24] W. S. Youn and C. Un, "Robust adaptive beamforming based on the eigenstructure method," *IEEE Trans. Signal Process.*, vol. 42, no. 6, pp. 1543–1547, Jun. 1994.

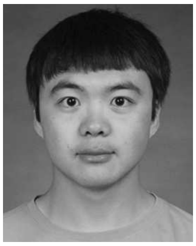
[25] B. D. Jeffs and K. F. Warnick, "Spectral bias in adaptive beamforming with narrowband interference," *IEEE Trans. Signal Process.*, vol. 57, no. 4, pp. 1373–1382, Apr. 2009.

[26] A. Pezeshki, B. D. V. Veen, L. L. Scharf, H. Cox, and M. L. Nordenvaad, "Eigenvalue beamforming using a multirank MVDR beamformer and subspace selection," *IEEE Trans. Signal Process.*, vol. 56, no. 5, pp. 1954–1967, May 2008.

[27] L. Chen, W. Meng, S. Han, and E. Liu, "A cross-correlation mitigation method based on subspace projection for GPS receiver," in *Proc. ION GNSS*, Nashville, TN, USA, Sep. 2012, pp. 1428–1434.

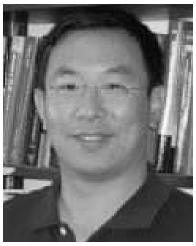
[28] Y. T. Morton, M. Miller, J. Tsui, D. Lin, and Q. Zhou, "GPS civil signal self-interference mitigation during weak signal acquisition," *IEEE Trans. Signal Process.*, vol. 55, no. 12, pp. 5859–5863, Dec. 2007.

SHUAI HAN (M'11–SM'17) received the degree in the communication engineering from the Harbin Institute of Technology in 2000, M.E. and Ph.D. degrees in information and communication engineering from the Harbin Institute of Technology in 2007 and 2011, respectively, and the Ph.D. degree in electrical and computer engineering from Memorial University of Newfoundland, Canada, in 2012. He is currently an Associate Professor with the Department of Electronics and Communication Engineering, Harbin Institute of Technology. His research interests include wireless sensor networks, wireless communications, the global navigation satellite system and indoor location. He is Senior Member of the IEEE Communication Society, Vice Chair of the IEEE Harbin ComSoc Chapter and a Vice Chair of the IEEE Harbin VTS Chapter. He has served as a Co-Chair for technical symposia of international conference ICC 2018, VTC FALL 2016, IWCMC 2017 IWCMC 2016, IWCMC 2015, ComComAp 2012 Workshop. He has also served as the TPC member for many international conferences, including the IEEE ICC, IEEE GLOBECOM, VTC, IEEE COMNETSAT, APCC. He is an Associate Editor of IEEE ACCESS.



LEI CHEN (S'13) received the B.S. and M.E. degrees in communication engineering from the Harbin Institute of Technology, Harbin, China, in 2010 and 2012, where he is currently pursuing the Ph.D. degree with the Communications Research Center. From 2015 to 2017, he was a Visiting Student with the Laboratory of Signals, Systems and Networks, University of California, Riverside, CA, USA. His research interests include power allocation, transmitting beamforming and GNSS signal processing.

WEIXIAO MENG (M'02–SM'10) received the B.Eng., M. Eng., and Ph.D. degrees from the Harbin Institute of Technology (HIT), Harbin, China, in 1990, 1995, and 2000, respectively. From 1998 to 1999, he was with NTT DoCoMo on adaptive array antenna and dynamic resource allocation for beyond 3G as a Senior Visiting Researcher. He is currently a Full Professor and the Vice Dean with the School of Electronics and Information Engineering, HIT. His research interests include broadband wireless communications and networking, MIMO, GNSS receiver, and wireless localization technologies. He has published 3 books and over 220 papers on journals and international conferences. He is the Chair of the IEEE Communications Society Harbin Chapter, a Fellow of the China Institute of Electronics, a Senior Member of the IEEE ComSoc and the China Institute of Communication. He has been an Editorial Board Member for Wileys WCMC Journal since 2010, an Area Editor for PHYCOM journal since 2014, an editorial board for IEEE Communications Surveys and Tutorials since 2014 and the IEEE Wireless Communications since 2015. He acted as leading TPC co-chair of ChinaCom2011 and ChinaCom2016, leading Services and Applications Track Co-Chair of IEEE WCNC2013, Awards Co-Chair of IEEE ICC2015 and Wireless Networking Symposia Co-Chair of IEEE Globecom2015. In 2005, he was honored provincial excellent returnee and selected into New Century Excellent Talents plan by Ministry of Education, China, in 2008, and the Distinguished Academic Leadership of Harbin.



CHENG LI (M'04–SM'07) received the B.Eng. and M.Eng. degrees from the Harbin Institute of Technology, Harbin, China, in 1992 and 1995, respectively, and the Ph.D. degree in electrical and computer engineering from Memorial University, St. Johns, NL, Canada, in 2004. He is currently a Full Professor with the Department of Electrical and Computer Engineering, Faculty of Engineering and Applied Science, Memorial University, St. Johns, NL, Canada. His research interests include mobile *ad hoc* and wireless sensor networks, wireless communications, and mobile computing, switching and routing, and broadband communication networks. He is a registered Professional Engineer in Canada and is a member of the IEEE Communication Society, Computer Society, Vehicular Technology Society, and Ocean Engineering Society He was a recipient of the Best Paper Award at the 2010 IEEE International Conference on Communications, Cape Town, 2010. He is an Editorial Board Member of Wiley Wireless Communications and Mobile Computing, an Associate Editor of Wiley Security and Communication Networks, and an Editorial Board Member of Journal of Networks, International Journal of E-Health and Medical Communications, and KSII Transactions on Internet and Information Systems. He has served a Technical Program Committee Co-Chair for the ACM MSWIM14, MSWIM13, IEEE WiMob11 and QBSC10. He has served as a Co-Chair for various technical symposia of many international conferences, including the IEEE GLOBECOM, ICC, WCNC, and IWCMC. He has also served as the TPC Member for many international conferences, including the IEEE ICC, GLOBECOM, and WCNC.