Robust Spoofing Detection for GNSS Array Instrumentation Based on C/N_0 Difference Measurements

Jinyuan Liu, Feiqiang Chen, Yuchen Xie, Beibei Ge, Zukun Lu, and Guangfu Sun

***Abstract*— In recent years, Global Navigation Satellite System (GNSS) spoofing detection techniques have attracted wide attention. Spoofing attacks have posed a greater security threat than jamming and are more difficult to detect due to their strong concealment. One of the key measurements of GNSS instruments is the carrier-to-noise ratio (C/N_0), which may be affected by spoofing. However, the variations in C/N_0 are always uncertainty especially for the array instruments under the attack. This article proposes a method for GNSS array instruments to detect the spoofing after anti-jamming. A theoretically model of the effective C/N_0 in array receiver is deduced. The C/N_0 single difference (CSD) between satellites is further proposed as a testing statistic for spoofing detection. Simulation results demonstrate that the proposed method can effectively detect the abnormal C/N_0 feature of counterfeit signals after anti-jamming by the antenna array. The detection performance of the proposed metrics is verified in the jamming and spoofing scenarios using the real data collected by an antenna array instrument. This method does not require modifications to the hardware configuration of conventional array receivers and can provide an effective defense in the combination of jamming and spoofing attacks.**

***Index Terms*— Antenna array, anti-jamming, C/N_0, Global Navigation Satellite System (GNSS), spoofing detection.**

I. Introduction

GLOBAL Navigation Satellite System (GNSS) has become a key infrastructure for positioning, navigation, and timing synchronization worldwide [1]. With the rapid development of Internet of Things (IoT), unmanned vehicles, and other GNSS-dependent systems, more and more devices further rely on GNSS to provide accurate position and precise timing information [2].

However, GNSS instruments are vulnerable to intentional or unintentional interference, since the signal power is very low and the details of civilian signals are publicly available [3]. Jamming and spoofing are the most common forms of intentional interference [4]. Moreover, spoofing significantly poses more threats than jamming as victims are always unaware of being in such an attack [5]. The spoofer will replay some recorded genuine GNSS signals or generate fake signals imitating the authentic signal's structure, which will mislead the victim instrument to deduce a false position and/or timing solution [6]. In recent years, the attack incidents of spoofing have aroused wide concern, and the spoofer seriously threatened the security and integrity of GNSS [7], [8]. In particular, with the rapid development of software-defined radio (SDR) technology, the cost and complexity of implementing a spoofing attack will be greatly reduced by combining relevant RF platforms with the open-source software of the signal simulator [9], [10].

Therefore, the development of anti-spoofing has generated a great deal of interest in the community [11]. A review of the state of the art for spoofing detection and mitigation techniques proposed in the last decade can be found in [12] and [13]. Spoofing detection has always been a key issue and a field of active research, while it is also a prerequisite for spoofing mitigation. There have been many techniques developed to detect spoofing attacks including: signal strength monitoring [14], spatial processing [15], [16], [17], consistency cross-check [18], [19], signal-quality monitoring [20], [21], and cryptographic authentication [22], [23].

Among all these families of the above methods, signal strength monitoring such as carrier-to-noise ratio (C/N_0) is the simplest and most effective way to identify abnormal energy levels of signals [24]. In an open area with good visibility, C/N_0 measurements generally vary smoothly and are only affected by platform dynamics and ionospheric errors. Obtaining C/N_0 measurements for the defender is easy and the method is simple. On the other hand, it is difficult for the spoofing attacker to precisely control the signal power reaching the defender's antenna.

In [24], a joint detection method of C/N_0 and automatic gain control (AGC) is proposed to give the C/N_0 and AGC characteristics of the receiver under authentic signals and spoofing, respectively. This method requires the receiver to have an additional AGC. In [25], a method based on C/N_0 difference is utilized for spoofing detection, which requires two antennas with different patterns, such as a monopole antenna and a patch antenna. However, this method requires a significant difference between the two antenna patterns, while the difference between common GNSS antennas is small, resulting in a high false alarm rate. Jahromi et al. [26]

Manuscript received 31 March 2023; revised 23 August 2023; accepted 14 October 2023. Date of publication 30 October 2023; date of current version 8 November 2023. This work was supported in part by the National Nature Science Foundation of China under Grant 62303475 and in part by the Science-Technology Foundation Hunan Province, China, under Grant 2021RC3073. The Associate Editor coordinating the review process was Dr. Jingyu Hua. *(Corresponding author: Feiqiang Chen.)*

The authors are with the College of Electronic Science and Engineering, National University of Defense Technology, Changsha, Hunan 410073, China (e-mail: gongkenan23@163.com; matlabfly@hotmail.com; olien_x@163.com; gbb950222@163.com; luzukun@nudt.edu.cn; gfsunmail@163.com).

Digital Object Identifier 10.1109/TIM.2023.3328684

proposed a method based on the prior power information of GNSS signals. Since the C/N_0 of the real signals in a certain area is usually known in advance within a certain range, any inconsistency with this prior information could indicate the presence of spoofing. However, the performance of spoofing detection is heavily dependent on the prior threshold, making it susceptible to missed alarms if the spoofer modulates the signal power.

Another approach, as presented in [27], exploits the difference in correlation coefficients between the real and spoofed signals when the receiver or antenna is in motion. This method essentially uses spatial movement to introduce the variation of received power, which is always small. However, the performance is influenced by the distance and velocity of the moving antenna, resulting in limited practical application.

The conventional signal strength monitoring methods generally monitor the C/N_0 and look for any abnormal changes that can be an indication of a spoofing attack. The unusual variations include a sudden change or disagreement with prior information. However, the main problem with the above methods is challenging to implement when dealing with scenarios involving both jamming and spoofing. For a single-antenna receiver, spoofing signals elevate the power of the GNSS signals while the jamming increases the background noise level, causing the C/N_0 measurements to remain within the expected range. For receivers employing the anti-jamming adaptive array, it is well known that the C/N_0 of the antenna array receiver depends on the processing gain, which depends on the relative power spectral densities of the signal of interest (SOI), interference, and noise [28]. The unpredictable variation of C/N_0 in the presence of jamming and spoofing attack raise the uncertainty of the prior threshold and further introduce degradation in the performance of spoofing detection by monitoring raw C/N_0 values.

Hence, the main purpose of this article is to develop a spoofing detection method for GNSS instrumentation following the interference mitigation by the adaptive antenna array. The novelty and contribution of this article are as follows. First, we provide a feasible path for array instruments to detect spoofing after anti-jamming. The second original contribution of this article is that we propose a new metric based on the differential C/N_0 measurements between available satellites and prove that this metric can distinguish the spoofing signals from the authentic ones during the process of anti-jamming. In this way, the antenna array can retain to act as an adaptive processor mitigating the high-power interference. Therefore, the proposed method only requires the GNSS instruments' own measurements and needs no extensive hardware modifications to the conventional GNSS array receivers. Third, we consider the impact of the element factor to the metric by modeling the non-isotropic pattern of the antenna element accurately.

The rest of this article is organized in the following order. Section II introduces the signal model and effective C/N_0 model in the antenna array. In Section III, we derive the C/N_0 single difference (CSD) metrics and design the spoofing detection algorithm. In Section IV, a simulation platform is utilized to verify the ability of the proposed method in Section IV and a mean scheme is developed to boost the performance. To validate the performance of the proposed method in real-world scenarios, we arranged a system including the data collector based on hardware equipment and a post-processing array instrument based on the SDR. The experiment results are given in Section V. Finally, Section VI concludes this article.

II. Signal Model

A. Array Signal Model

To evaluate the performance of each array under study as a controlled reception pattern antenna (CRPA), we assume that it is connected to a multichannel adaptive processor and study its steady-state adapted pattern in the presence of desired signals and interfering signals, all of which are assumed to be stationary. Accounting for the time required for the signal to propagate along the array usually much smaller than the inverse of the bandwidth of GNSS signals, we assume GNSS signals satisfy the narrowband array assumption [29].

We consider the space-time adaptive processing (STAP) in this article, which is the most widely used in GNSS array receivers [30]. Assuming the adaptive array is composed of M elements and each element is followed by K-tap finite-impulse response (FIR) filters. GNSS satellites that can be tracked in the channels likely come from the real satellites or the same spoofer which is assumed to locate at a fix position in this article. The received signal vector of each snapshot $\mathbf{x} \in \mathbb{C}^{MK\times 1}$ can be defined as

$$\mathbf{x}(t) = \sum_{p=1}^{N^{\mathrm{au}}} \mathbf{a}_{st}(\theta_p^{\mathrm{au}}, \varphi_p^{\mathrm{au}}, f) s_p(t) + \mathbf{a}_{st}(\theta^{sp}, \varphi^{sp}, f) \sum_{q=1}^{N^{sp}} s_q(t) + \sum_{j=1}^{N^{i}} \mathbf{a}_{st}(\theta_j^{i}, \varphi_j^{i}, f) i_j(t) + \mathbf{n}(t) \tag{1}$$

where $s_p(t)$, $s_q(t)$, and $i_j(t)$ represents the complex waveform of the pth ($p = 1, \ldots, N^{\mathrm{au}}$) authentic signal, qth ($q = 1, \ldots, N^{sp}$) spoofed signal, and jth ($j = 1, \ldots, N^{i}$) jamming, of which the incident angle are $(\theta_p^{\mathrm{au}}, \varphi_p^{\mathrm{au}})$, $(\theta^{sp}, \varphi^{sp})$, and $(\theta_j^{i}, \varphi_j^{i})$, respectively. And the superscript au, sp, and i denote the authentic signals, spoofing, and jamming, respectively, of which N^{au}, N^{sp}, and N^{i} are the corresponding number. $\mathbf{n}(t)$ denote the white Gaussian noise, and $\mathbf{a}_{st}$ represents the spatial-temporal steering vector as

$$\mathbf{a}_{st}(\theta, \varphi, f) = \mathbf{a}_{s}(\theta, \varphi) \otimes \mathbf{a}_{t}(f) \tag{2}$$

where $\mathbf{a}_{s}(\theta, \varphi)$ and $\mathbf{a}_{t}(f)$ denote the spatial steering vector and the temporal steering vector, respectively. Notice that $\otimes$ stands for Kronecker product.

The digital signals after sampling can be denoted as $\mathbf{x}[n]$. The signal snapshot at time n is defined to a $MK \times 1$ vector as

$$\begin{aligned}\mathbf{x}[n] = [&x_1[n], x_1[n-1], \ldots, x_1[n-K+1],\\ &x_2[n], x_2[n-1], \ldots, x_2[n-K+1], \ldots,\\ &x_M[n], x_M[n-1], \ldots, x_M[n-K+1]]^{\mathrm{T}}.\end{aligned} \tag{3}$$

Typically, $w_{m,k}$ is the weight at the kth tap of the mth element, and the weight vector will be defined as

$$\mathbf{w} = [w_{1,1}, \ldots, w_{1,K}, w_{2,1}, \ldots, w_{2,K}, \ldots, w_{M,1}, \ldots, w_{M,K}]^{\mathrm{T}}. \tag{4}$$

The digital signals will enter an adaptive filter at the output of each channel to suppress the jamming. After filtering by the adaptive processor, the STAP output reads

$$y[n] = \mathbf{w}^H \mathbf{x}[n]. \tag{5}$$

A number of adaptive filtering algorithms have been proposed to determine the adaptive weights based on the received signals. It should be pointed out that the beamformer design for anti-jamming is not the purpose of this article, but to find the characteristic of measurements induced by the process of anti-jamming, so as to identify the presence of spoofing. Therefore, we consider to choose the power inversion (PI), which is the most popular and effective criterion used in modern GNSS array receivers based on minimizing the total output power [31], [32]. The PI algorithm require no prior information of the received signal and adapt to form the nulling toward the strong interfering signals [33]. Mathematically, the complex weight vector can be calculated as

$$\mathbf{w}_{\mathrm{PI}} = \frac{\mathbf{R}_x^{-1}\mathbf{b}_n}{\mathbf{b}_n^H \mathbf{R}_x^{-1}\mathbf{b}_n} = \mu \mathbf{R}_x^{-1}\mathbf{b}_n \tag{6}$$

where μ is an inconsequential scalar, which can be ignored later in this article. $\mathbf{b}_n = [0, 0, \ldots 1, \ldots, 0, 0]^{\mathrm{T}} \in \mathbb{C}^{MK\times 1}$ is a constraint vector with zeros except for 1 corresponding to the reference tap. It can be assuming that either the power of authentic signals or the power of spoofed signals is far below the noise. Thus, the covariance matrix of the received signals $\mathbf{R}_x \in \mathbb{C}^{MK\times MK}$ can be simplified as

$$\begin{aligned}\mathbf{R}_x &= E[\mathbf{x}(t)\mathbf{x}^H(t)] \\ &\approx \mathbf{R}_i + \mathbf{R}_n \\ &\approx \sum_{j=1}^{N^i} P_j \mathbf{a}_{st}\left(\theta_j^i, \varphi_j^i, f\right)\left(\mathbf{a}_{st}\left(\theta_j^i, \varphi_j^i, f\right)\right)^H + \sigma^2 \mathbf{I}\end{aligned} \tag{7}$$

where P_j denotes the power of jth jamming and σ^2 represents the variance of noise $\mathbf{n}(t)$ which are modeled as a Gaussian variable, and $\mathbf{I}$ is an $MK \times MK$ identity matrix.

B. Effective C/N$_0$ Model

This section deduces the effective C/N_0 derived based on the model of the adaptive antenna array. If a receiver is at risk of being spoofed, the key issue for anti-spoofing is to determine whether the signal currently in the tracking loop is authentic or not, and to give an alert in the case of spoofing. It should be noted that the conditions for spoofing to be successful are limited due to the defender's strategies, such as adaptive antenna arrays and possible signal processing. Instead of discussing the specific spoofing implementation method, this article focuses on the feature of C/N_0 in the case that the fake signals have captured the victim's tracking loop and are used for navigation solutions.

The adaptive antenna array can be considered as a digital filtering system consisting of M individual antenna elements that have a total frequency response as [28]

$$H_{\mathrm{sys}}(f, \theta, \varphi) = \sum_{m=1}^{M} A_m(f, \theta, \varphi) F_m(f) W_m(f) \tag{8}$$

where $A_m(f, \theta, \varphi)$, $F_m(f)$, and $W_m(f)$ denote the response of the mth antenna element for the signal incident from the (θ, φ), the response of the RF front-end-channel behind the element, and the response of each adaptive filter determined by the calculation in (6), respectively. Since $F_m(f)$ is independent of the incidence angle, the effect of the RF-front ends will be ignored in this article, i.e., $F_m(f) = 1$. Furtherly, the response of the adaptive antenna array can be derived on (8), expressed as

$$H_{\mathrm{sys}}(f, \theta, \varphi) = \sum_{m=1}^{M}\sum_{k=1}^{K} A_m(f, \theta, \varphi) w_{mk}^{*} e^{-j2\pi(k-1)fT_s}. \tag{9}$$

According to (1), the output of the adaptive antenna array includes several parts: authentic signals, counterfeit signals, the residual part of jamming after nulling by STAP, and the noise part. It is assumed that the normalized power spectral density of authentic signals is $G_s(f)$ satisfying $\int G_s(f)df = 1$ with incident power C_s. Then the power spectrum of the pth authentic signal component at the output of the adaptive antenna array takes the form as

$$S_p^{\mathrm{au}}(f) = C_s \left| H_{\mathrm{sys}}\left(f, \theta_p^{\mathrm{au}}, \varphi_p^{\mathrm{au}}\right)\right|^2 G_s(f) \tag{10}$$

where $(\theta_p^{\mathrm{au}}, \varphi_p^{\mathrm{au}})$ denotes the direction of the pth authentic signal. Since the spoofing generally approximates the structure of the real signal, we suppose that the power spectral density of spoofing is also $G_s(f)$. If the signal power corresponding to different pseudorandom noise (PRN) codes is consistent, namely, the attacker does not perform power regulation and thus the power of spoofing can be given as C_{sp}. It is assumed that all spoofing signals are incident from the same direction $(\theta^{sp}, \varphi^{sp})$, then the power spectrum of the spoofing component at the output of the adaptive antenna array is

$$S^{sp}(f) = N^{sp} C_{sp} \left| H_{\mathrm{sys}}(f, \theta^{sp}, \varphi^{sp})\right|^2 G_s(f). \tag{11}$$

Given that the power of the jth jamming incident from $(\theta_j^i, \varphi_j^i)$ is C_j, the normalized power spectral density is $G_j^i(f)$ satisfying $\int G_j^i(f)df = 1$. The power spectrum of the jamming component at the output of the adaptive antenna array can be written as

$$S^i(f) = \sum_{j=1}^{N^J} C_j^i \left| H_{\mathrm{sys}}\left(f, \theta_j^i, \varphi_j^i\right)\right|^2 G_j^i(f). \tag{12}$$

The noise component is modeled as zero-mean Gaussian noise, and its power spectral density at the output of the array is

$$S_n(f) = C_n \sum_{m=1}^{M} |W_m(f)|^2 \tag{13}$$

where C_n is the total power of the thermal noise before filtering by the RF front-end. Based on the output of the adaptive antenna array, the effective C/N_0 of the receiver can be estimated under the interference. It can be divided into two cases: unsuccessful spoofing and successful spoofing, and a theoretical model of effective C/N_0 will be derived for each of these two cases.

First, we consider that the receiver still processes the authentic signals under the attack, which spoofing does not distort the real correlation peak, nor does it successfully capture the tracking loop. At this point, the spoofing is equivalent to the matched-spectrum interference for the victim receiver. Since there is a mutual nonzero cross correlation of the PRN codes, the spoofing energy after STAP may further improve the noise floor [26]. Referring to the literature [34], [35] and combining with previous derivation, the theoretical model of the effective C/N_0 under the attack of both jamming and spoofing can be given as

$$\left(\frac{C_s}{N_0}\right)_{\text{eff}} = \frac{C_s\left|\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} H_{\text{sys}}\left(f, \theta_p^{\text{au}}, \varphi_p^{\text{au}}\right) G_s(f) df\right|^2}{\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} G_w(f) G_s(f) df} \tag{14}$$

where β_r represents the two-sided bandwidth of the front-end centered at zero frequency. $G_w(f)$ is the sum of the interference power and the noise power at the output of the adaptive antenna, which can be stated as

$$\begin{aligned} G_w(f) = {} & N^{sp} C_{sp}\left|H_{\text{sys}}(f, \theta^{sp}, \varphi^{sp})\right|^2 G_s(f) \\ & + \sum_{j=1}^{N^J} C_j^i \left|H_{\text{sys}}\left(f, \theta_j^i, \varphi_j^i\right)\right|^2 G_j^i(f) + S_n(f). \end{aligned} \tag{15}$$

The above equation comprises three terms: the contribution due to spoofing effects which can be modeled as the matched interference, the contribution due to jamming effects, and the contribution due to thermal noise effects. Accordingly, the noise floor in the receiver is bound to increase in the presence of interference. Note that, as shown in (9) and (10), the array gain toward the direction of the authentic signal will vary with the spatial relationship between the real satellite and the jamming. Therefore, the effective C/N_0 under this circumstance may be raised or decreased compared to that without spoofing, proving that it is difficult to provide robust spoofing detection merely by observing the variation of C/N_0.

Second, we consider the case that tracking loops have been captured by the counterfeit signals. In this case, it is obvious that the actual C/N_0 estimated by the receiver is determined by the power of spoofing arriving at the array aperture. Similarly, the theoretical model of the effective C/N_0 can be calculated as

$$\left(\frac{C_s}{N_0}\right)_{\text{eff}} = \frac{C_{sp}\left|\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} H_{\text{sys}}(f, \theta^{sp}, \varphi^{sp}) G_s(f) df\right|^2}{\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} G'_w(f) G_s(f) df}. \tag{16}$$

Under the premise that the spoofing attack has been successful, the power of spoofing is generally higher than that of the authentic signals. Therefore, at this time, the multiaccess interference introduced by the real satellite signals can be neglected, then the interference component and the noise component at the output of the adaptive antenna sum up to

$$G'_w(f) = \sum_{j=1}^{N^J} C_j^i \left|H_{\text{sys}}\left(f, \theta_j^i, \varphi_j^i\right)\right|^2 G_j^i(f) + S_n(f). \tag{17}$$

III. Spoofing Detection

In Section II, theoretical formulas for the effective C/N_0 are given for the two cases of successful and unsuccessful spoofing, respectively. This section further gives the single difference measurement on which we design the spoofing detection algorithm based.

A. CSD Metrics

The CSD is defined as the difference between the C/N_0 estimated from two different satellites. Assuming that the set of satellites that can be stably tracked during the observation time is Λ, the value of C/N_0 of the hth and the lth ($h, l \in \Lambda, h \neq l$) satellite is C_h and C_l, respectively. By definition, the CSD of the two satellites can be expressed as

$$\Delta C_{h,l} = |C_h - C_l|. \tag{18}$$

In the spoofing-absent condition, the hth and the lth satellites are both authentic, then the CSD of two authentic signals can be derived from (14) as follows:

$$\begin{aligned} \Delta C_{h,l}^{\text{au}} = C_s & \left| \frac{\left|\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} H_{\text{sys}}\left(f, \theta_h^{\text{au}}, \varphi_h^{\text{au}}\right) G_s(f) df\right|^2}{\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} G'_w(f) G_s(f) df} \right. \\ & \left. - \frac{\left|\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} H_{\text{sys}}\left(f, \theta_l^{\text{au}}, \varphi_l^{\text{au}}\right) G_s(f) df\right|^2}{\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} G'_w(f) G_s(f) df} \right|. \end{aligned} \tag{19}$$

We assume that the response of the mth antenna element can ignore the impact of broadband characteristics, i.e., the gain and the phase pattern of the antenna are the same under each frequency point. Thus, $A_m(f, \theta, \varphi)$ $(m = 1, 2, \ldots M)$ can be simplified as $A_m(\theta, \varphi)$. Furthermore, we assume that the elements of the array have equal patterns ignoring the mutual coupling and other non-ideal factors in the array, that is $A_m(\theta, \varphi) = A(\theta, \varphi), \forall m \in (m = 1, 2, \ldots M)$. Equation (8) can be further simplified as

$$H_{\text{sys}}(f, \theta, \varphi) \approx A(\theta, \varphi) \sum_{m=1}^{M} W_m(f) \tag{20}$$

where $H_{\text{sys}}(f, \theta, \varphi)$ represents the array response which is a function of the pattern of the elements in the array and the weights used. Inserting (20) into (19) yields

$$\begin{aligned} & \Delta C_{h,l}^{\text{au}} \\ & = \frac{C_s\left|A(\theta_l^{\text{au}}, \varphi_l^{\text{au}})\right|^2 (b-1)\left|\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} \sum_{m=1}^{M} W_m(f) G_s(f) df\right|^2}{\int_{-\frac{\beta_r}{2}}^{\frac{\beta_r}{2}} G'_w(f) G_s(f) df} \end{aligned} \tag{21}$$

where $b = (|A(\theta_h^{\text{au}}, \varphi_h^{\text{au}})|^2 / |A(\theta_l^{\text{au}}, \varphi_l^{\text{au}})|^2)$ implies the difference of element patterns toward the different directions of the two satellites. Therefore, the CSD metric in the spoofing-absent condition is related to the pattern of antenna element and the array factor which is determined by the effects of interference.

It can be derived from (21) that if the signals belonging to different PRNs are incident from the same direction, the value of b will be 1. That is to say, in the case that the receiver has been spoofed successfully, the CSD of two counterfeit signals which are both incident from $(\theta^{sp}, \varphi^{sp})$ can be derived as follows:

$$\Delta C_{h,l}^{sp} = 0. \tag{22}$$

It can be seen in (22) that in the presence of spoofing, since the signals belonging to different PRNs are incident from the same direction, the CSD between the two different satellites is theoretically zero as long as they can be tracked normally. It is clear that CSD in this case is mainly affected by the measurement noise of C/N_0, which is related to the specific estimation method of C/N_0 used by the receiver.

B. Statistical Analysis

As mentioned earlier, spoofing detection is essentially discriminating the counterfeit signals from the authentic signals by the anomalous characteristics at each stage in the receiver. The proposed CSD metric will exhibit a significant discrepancy between the two cases of authentic and counterfeit signals, thus spoofing can be detected by comparing the value of CSD metrics with a preset threshold. Note that the prerequisite for the CSD metric to be effective is that the victim receiver is not denial-of-service under the jamming attacks and the tracking loop is able to provide C/N_0 measurements for different satellites.

Let H_0 represents the hypothesis that the receiver has been spoofed successfully and H_1 be the hypothesis for the spoofing-absent condition. Therefore, the hypothesis test based on the statistics of CSD can be established as

$$\begin{cases} H_0 : \Delta C_{h,l} = \Delta n_{h,l}^{sp} \\ H_1 : \Delta C_{h,l} = \Delta C_{h,l}^{\text{au}} + \Delta n_{h,l}^{\text{au}} \end{cases} \tag{23}$$

where $\Delta n_{h,l}$ denotes the measurement noise of CSD and under H_0 hypothesis the detection statistic satisfies the distribution as

$$\Delta C_{h,l} \sim N\left(0, 2\sigma_n^2\right) \tag{24}$$

where σ_n^2 is the variance of the C/N_0 measurement error, that is, in the presence of spoofing, the CSD approximately satisfies a Gaussian distribution with a zero mean, and the probability density function (pdf) of CSD under H_0 hypothesis can be obtained as

$$f_N(\Delta C|H_0) = \frac{1}{\sqrt{4\pi}\sigma_n} \exp\left[-\frac{(\Delta C)^2}{4\sigma_n^2}\right]. \tag{25}$$

Furthermore, the CSD under H_1 hypothesis can be described as a Gaussian with mean $\mu_{\Delta C}$ and variance σ_n^2, of which pdf can be described

$$f(\Delta C|H_1) = \frac{1}{\sqrt{4\pi}\sigma_n} \exp\left[-\frac{(\Delta C - \mu_{\Delta C})^2}{4\sigma_n^2}\right]. \tag{26}$$

It is worth noticing that $\mu_{\Delta C}$ will be time-variant, which is dependent on the received power of satellite signals and the geometry conditions between jamming and authentic signals.

It is obvious that if two signals are tracked by the receiver incident from the same direction, the distribution of CSD is only related to the measurement noise of C/N_0, which is generally much smaller than that under the authentic signal. Therefore, by setting a reasonable detection threshold γ, it is feasible to distinguish any two signals that are stably tracked in the channel. When $\Delta C_{h,l} > \gamma$, H_1 can be judged to be valid, and at least one signal is authentic between the two signals; otherwise, both two signals are definitely spoofing and a spoofing-presence decision should be made. From the above derivation, the detection probability and false alarm probability can be written, respectively, as

$$P_D = \int_0^\gamma f_N(\Delta C|H_0)dt \tag{27}$$

$$P_{\text{FA}} = \int_0^\gamma f(\Delta C|H_1)dt. \tag{28}$$

The spoofing detection threshold can be set at a fixed value in advance empirically or adaptively determined by some criterion such as the constant false-alarm rate (CFAR) detection technique and so on. As shown in (28), the false alarm probability is determined by the pdf of CSD under H_1 hypothesis which is challenging to obtain, mainly owing to the fact that the pdf is mainly related to the spatial distribution of all signal components.

On the other hand, the performance of C/N_0 estimation algorithms has been studied in various research works. The commonly used C/N_0 estimation methods for receivers include the narrow-wideband power ratio (NWPR) method [36], variance summing method (VSM) [37], moments method (MM) [38], and many other methods. Researchers have studied the above-mentioned algorithms in more detail, and the theory of specific algorithms will not be discussed here. Sliarawi et al. [39] have investigated the behavior of the two popular methods as VSM and power ratio method (PRM) in the presence of broadband interference. The study pointed out that the empirical standard deviation of the C/N_0 estimated by VSM is lower than 1 dB as the number of samples for summing is greater than 50. According to the conclusion in [38], it is convenient for us to fix the threshold γ to be 2 dB empirically in this article.

IV. Simulation Analysis

To further verify the performance of our proposed CSD metric for spoofing detection, we evaluated it over a simulated dataset of GNSS array in this section.

A. Antenna Element and Array Model

According to the previous analysis in (21), the impact of the antenna element pattern on the actual C/N_0 measurement should not be neglected. In order to simulate the pattern characteristics of the antenna element, we used CST Studio Suite to simulate a typical antenna (see Fig. 1) used in GNSS adaptive arrays, which performs the right-hand circular polarization (RHCP) by a dual-feed configuration providing

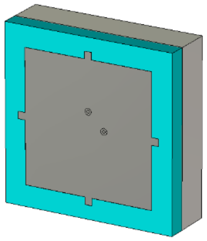
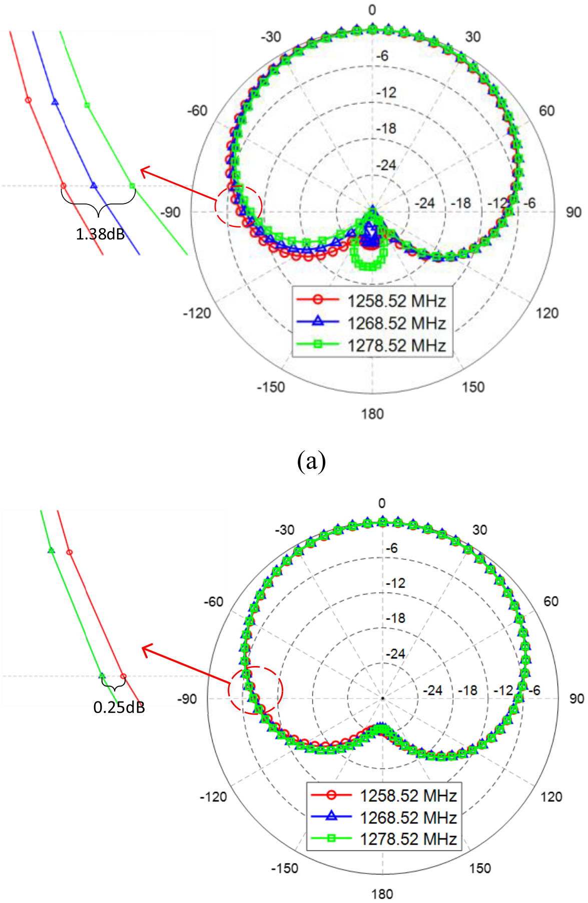


Fig. 1. Patch antenna used for simulations in this study (Modeling in CST Studio Suite 2018).



(a)

(b)

Fig. 2. Comparison of simulated radiation characteristics of the antenna at different frequencies. (a) E-plane. (b) H-plane.

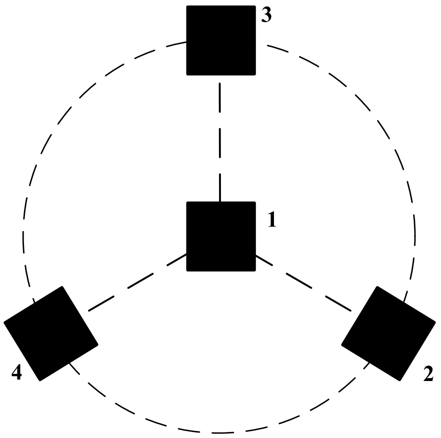


Fig. 3. Geometry of a four-element array in this study.

TABLE I

Parameter Settings of the Generated Data

Type of signal	PRN	Elevation (°)	Azimuth (°)	SNR（dB）
Authentic signal	2	10	310	-28
	4	20	48	-28
	8	40	350	-28
	11	68	235	-28
	14	70	235	-28
Spoofing	2,4,8,11,14	75	0	-18
jamming 1	/	80	120	35
jamming 2	/	85	45	40
jamming 3	/	75	10	40

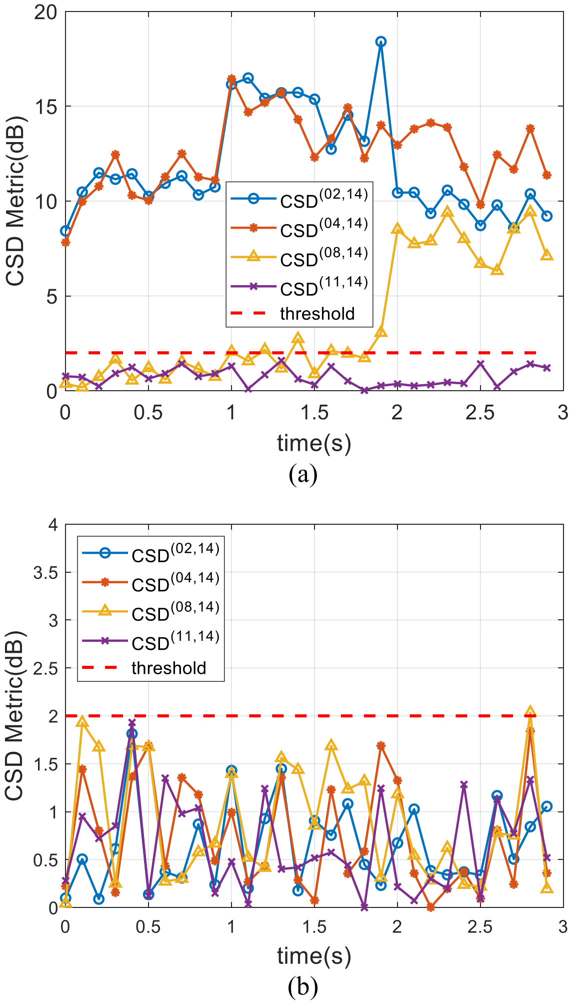
two ports with a 90° phase difference. The square patch element is located on a substrate with a height of 5 mm and a relative dielectric constant of 16. The patch element works at 1268.52 MHz, which is the central frequency of the B3 signal of the BeiDou Satellite Navigation System, and its $S_{11} < -15$ dB.

The comparison of simulated radiation patterns at different frequencies is plotted in Fig. 2. We assume that the elevation angles of satellite signals vary within the range of 0°–90°. As shown in Fig. 2, the maximum discrepancy of the gain pattern between different frequency points is approximately 1.38 dB. According to the simulation results, the mean difference between 1258.52 and 1278.52 MHz within the range of 0°–90° is about 0.23 dB. It can be demonstrated that the gain patterns of the antenna are similar within the signal bandwidth. Therefore, this article assumes that the pattern of patch antenna can ignore the impact of broadband characteristics, i.e., the gain patterns of the antenna are the same under each frequency point. In this way, we will focus on the differences introduced by the pattern of antenna elements.

We consider the common array geometry used for GNSS antenna arrays in the simulation. As depicted in Fig. 3, the array consists of three elements that are equally spaced on a circle with a half-wavelength spacing and an element at the circle's center. It is assumed that the configuration of the antenna element is shown as Fig. 1 and the STAP filter length is 5 taps.

B. Spoofing Detection Using CSD Metric

The IF signals of Beidou B3I and interference including jamming and spoofing were generated by an array signal simulator based on MATLAB software, which we have developed in [33]. We considered two signal scenarios both of which have a length of 3 s. One contains authentic satellite signals while the other contains spoofed signals incident from the same direction. Moreover, each scenario has three high-power broadband interference signals starting at 0, 1, and 2 s, respectively. The detailed signal parameters are given in Table I. Notice that PRN 11 is set to have a similar elevation angle



(a)

(b)

Fig. 4. CSD detector results in simulation of (a) authentic signals and (b) spoofing.

and the same azimuth angle with PRN 14, which simulate the case where the real signals have the similar angle of arrival (AOA).

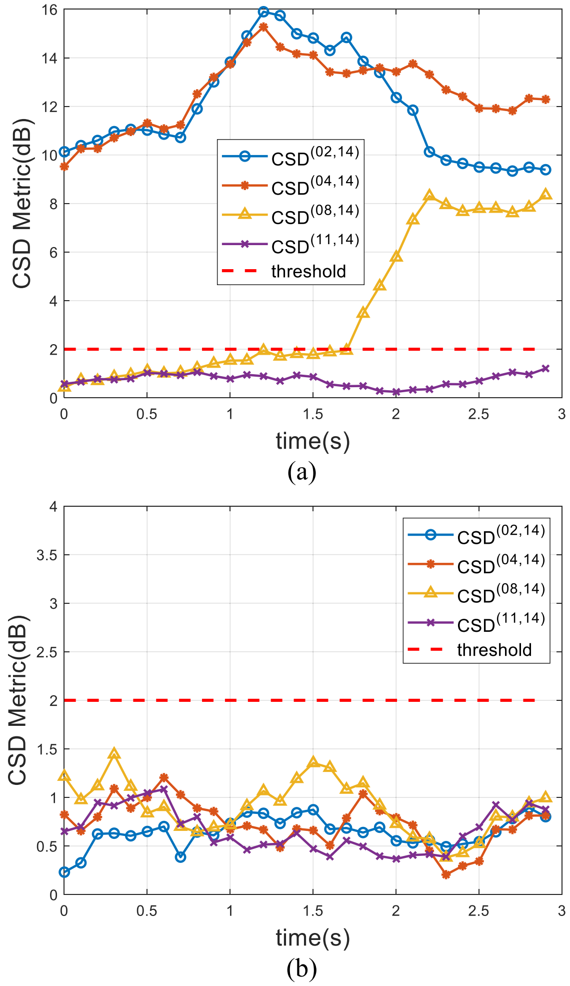
The sampling rate is set to 62 MHz and the IF frequency is 46.52 MHz. Then, an SDR for the GNSS array instrument is utilized to process the simulated data output by the STAP filter and test the CSD metric after tracking.

The simulation results considered as an example of a CSD detector are reported in Fig. 4. Based on the parameters mentioned above, we calculated the CSD metrics between the pairwise satellites. Fig. 4 shows the CSD results obtained when PRN 14 is used as the reference satellite.

The results verify the previous analysis that the raw CSD metrics actually capture the variation of the array pattern especially when the jamming changes dynamically, however, its performance is affected by the uncertainty of C/N_0 measurement under the interference.

Furthermore, we adopt a method of moving averaging to boost the performance of the raw CSD metric expressed as follows:

$$\Delta\bar{C}^{(h,l)}(n) = \frac{1}{k}\sum_{i=n-\frac{k-1}{2}}^{n+\frac{k-1}{2}} \Delta C^{(h,l)}(i) \tag{29}$$



(a)

(b)

Fig. 5. Results after averaging CSD metrics of (a) authentic signals and (b) spoofing.

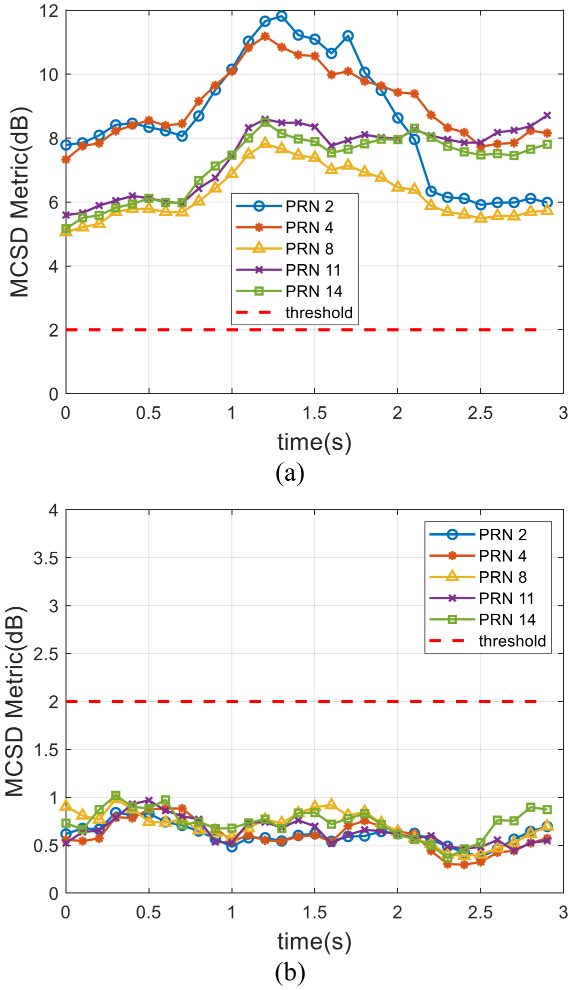
where k is the length of the window for averaging and $\Delta\bar{C}^{(h,l)}$ corresponds to the mean value computed from the data subsets of CSD between hth and lth satellite in sequence. The results after moving averaging where k is selected as 5 are plotted in Fig. 5.

It is clearly visible from Fig. 5 that the CSD metrics after averaging better identify the case where two signals are from the same direction, that is to say, both signals are counterfeit. Comparison of Figs. 4(b) and 5(b) shows that the detection probability increases from 99.7% to 100%. However, the false alarm probability is 29% mainly introduced by authentic signals incident from the closely direction (PRN 11 and PRN 14). A mean mechanism over the set of available satellites can be used to solve this problem, given by

$$M^h_{\Delta C} = \frac{1}{N_s - 1}\sum_{l\in\Lambda, l\neq h} \Delta C^{(h,l)} \tag{30}$$

where Λ is the set of the available satellites in which N_s is the total number of the elements. $M^h_{\Delta C}$ corresponds to the mean of CSD (MCSD) metrics of hth satellite with the other available satellites.

We tested the performance of the proposed MCSD metric based on the results of Fig. 5. As shown in Fig. 6, the



(a)

(b)

Fig. 6. MCSD metrics in the simulation of (a) authentic signals and (b) spoofing.

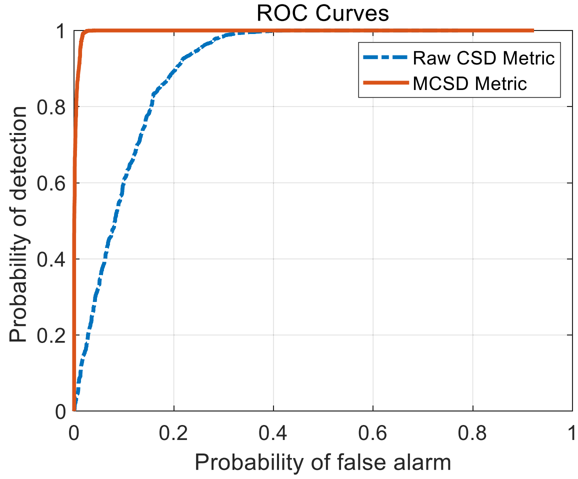


Fig. 7. Comparison of ROC curves for the MCSD metric with the raw CSD metric.

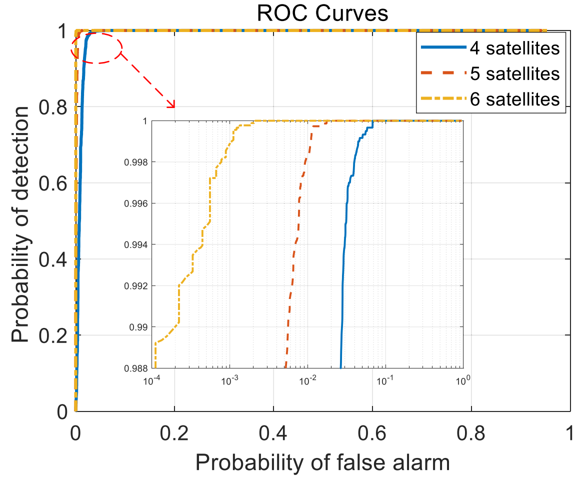


Fig. 8. Comparison of ROC curves for the MCSD metrics computed by different numbers of available satellites.

proposed MCSD metrics of all available satellites are much lower in the case of spoofing [see Fig. 6(a)] than that in the case where all signals are authentic [see Fig. 6(b)]. Notice that despite the similar incident angles of PRN 11 and 14, the MCSD method can still effectively distinguish between authentic and spoofing signals. The simulation results confirm that the MCSD metric can utilize the average mechanism to boost the spoofing detection performance, unless the majority of the available satellites in the receiver have similar incidence angles. However, the probability of this situation is very low. During the design of satellite constellations, this situation is to be avoided as much as possible, as it leads to poor dilution of precision (DOP) values.

C. Performance Evaluation via Receiver Operation Characteristic Curves

To evaluate the performance of the spoofing detection method, we plot the receiver operation characteristic (ROC) curves of the proposed MCSD metric. As is known to all, the closer the ROC curve is to the upper left corner of the figure, the better the corresponding detector is. As plotted in Fig. 7, it is obvious that the proposed MCSD metric outperforms the raw CSD metric, while the performance of the latter will degrade significantly as the authentic signals come from the nearby direction.

It should be noted that the MCSD metric proposed in this article is effective when all visible satellites are spoofed, while the decision will be confused when the signals entering the tracking loop contain both authentic signals and spoofed signals. However, if the authentic signal and the spoofed signal are tracked by the victim simultaneously, it is difficult for the attacker to achieve the purpose of controlling the receiver to the planned solution. Since the harm of this uncommon scenario does not reach the expectation of spoofer, we only consider the case where all the signals are authentic or counterfeit in this article.

Furthermore, we investigate the performance of the proposed MCSD method with different numbers of available satellites. Fig. 8 illustrates the ROC curves of the MCSD metric when the number of available satellites is 4, 5, and 6, respectively. The results verify that the performance of the MCSD metric will improve as the number of available satellites involved in the computation increases, since the spatial

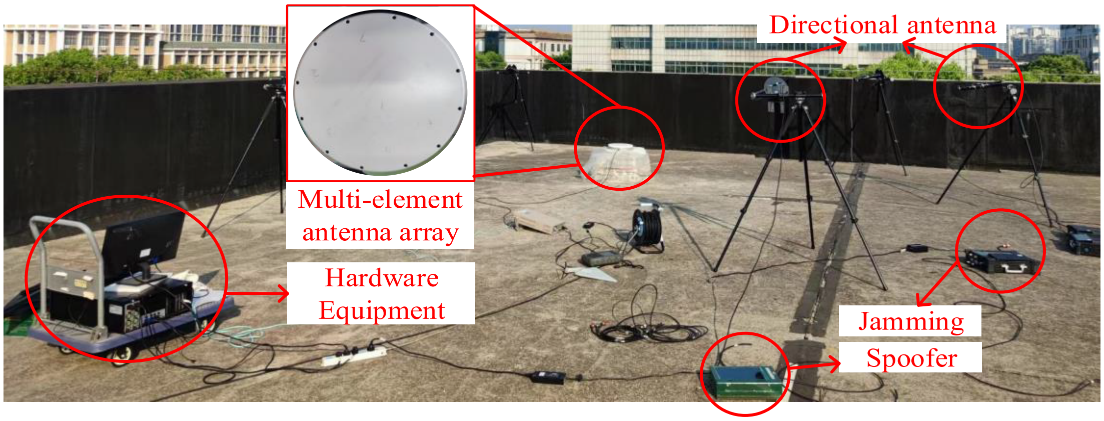


Fig. 9. Diagram of the experimental arrangement.

distribution of real satellites is actually distributed across the entire sky.

V. Experiment Results

We have conducted experiments to verify the proposed spoofing detection method. Considering that it is illegal to conduct outdoor spoofing experiments, we set the transmit power of the over-the-air spoofing signal low enough not to affect users outside the university campus building.

As shown in Fig. 9, we arranged an antenna array instrument to collect the real-world GNSS data under the spoofing and jamming circumstance. The GNSS array data collector includes a four-element circular array connected to the corresponding synchronized front-ends. The front-ends down-convert B3 frequency band to the intermediate frequency which is chosen to be 46.52 MHz. The front-ends have a maximum sample rate of 62 MHz with 13-bit quantization. The sampled data are transferred to a server in real-time through the optical fiber and stored for further postprocess using the SDR GNSS array instrument developed for spoofing detection in MATLAB.

The recording of authentic signals and spoofing were collected using the above hardware equipment. Notice that the power of the authentic signal is assumed to be the received power levels on the ground specified in the interface control document (ICD) [40], where the corresponding power of the B3 signal is −163 dBW.

In the presence of jamming (jamming to signal ratio is 55 dB), the antenna array first gathered the authentic signals in the open-sky environment. The signals of PRN 01, 03, 08, 22, and 35 are transmitted from the satellites. The spoofing device emulated the signals received from the available satellites in advance. Then the antenna array instrument collected the counterfeit signals generated by the spoofer of which power is set to 5 dB above the authentic signals.

We used the software receiver to process the stored data. STAP introduced in the previous analysis was utilized to mitigate the jamming. The output of STAP was given to the baseband processor to track the available satellites and to calculate the MCSD metrics. As illustrated in Fig. 10, the observed MCSD metrics in the presence of spoofing are consistent with the predictions, which is determined by the measurement noise. It is obvious that the value of the MCSD metric for authentic signals is much larger than the case of counterfeit signals from the same direction. By setting the reasonable threshold, the proposed MCSD metric successfully identifies the spoofing.

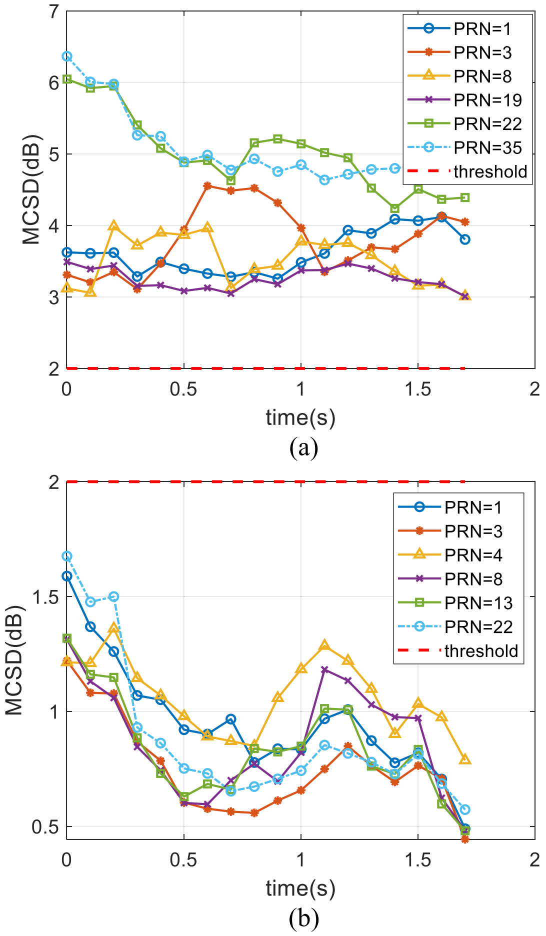


Fig. 10. MCSD metrics in the empirical experiment of (a) authentic signals and (b) spoofing.

VI. Conclusion

This article proposes a method for detecting spoofing attacks on GNSS array instruments after anti-jamming. We derive a theoretical model of the effective C/N_0 in the presence of jamming and spoofing and propose the MCSD metric between satellites as a testing statistic for spoofing detection.

Simulation results demonstrate that the proposed method can effectively detect abnormal C/N_0 features of counterfeit signals after anti-jamming by the antenna array. The experiments presented in Section V are examples to demonstrate the effectiveness of the MCSD metric.

In addition, the idea in this article depends on the raw measurements in instruments and does not require additional modifications to conventional GNSS array receivers. It should be noted that although the results of this article are given in the scenario with the jamming. But in the absence of high-power interference, a set of fixed weights can be used for beamforming to change the array's pattern before spoofing detection. Therefore, the method proposed in this article can provide the solution to array instruments whether there is high-power interference. In future, we will combine this with the method used under a single antenna to provide more flexible and robust spoofing detection.

References

[1] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*. Lincoln, MA, USA: Ganga-Jamuna Press, 2012.

[2] R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente, and E. S. Lohan, "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 249–291, 1st Quart., 2020.

[3] B. Li et al., "Influence of sweep interference on satellite navigation time-domain anti-jamming," *Frontiers Phys.*, vol. 10, Jan. 2023, Art. no. 1063474, doi: 10.3389/fphy.2022.1063474.

[4] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016.

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

[6] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," *IEEE Access*, vol. 8, pp. 165444–165496, 2020.

[7] S. Bian, Y. Hu, and B. Ji, "Research status and prospect of GNSS anti-spoofing technology," *Scientia Sinica Inf.*, vol. 47, no. 3, pp. 275–287, 2017.

[8] United States Department of Transportation. *2017–005A-Black Sea-GPS Interference*. Marad. Accessed: Feb. 19, 2019. [Online]. Available: https://www.maritime.dot.gov/content/2017-005a-black-seagps-interference

[9] L. Huang and Q. Yang, "Low-cost GPS simulator—GPS spoofing by SDR," in *Proc. DEFCON* , Las Vegas, NV, USA, 2015, pp. 1–54.

[10] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, "Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part I," *Sensors*, vol. 20, no. 4, p. 1806, Feb. 2020.

[11] M. L. Psiaki and T. E. Humphreys. (Jul. 2016). *Protecting GPS from Spoofers is Critical to the Future of Navigation*. IEEE Spectrum. [Online]. Available: https://spectrum.ieee.org/telecom/security/protecting-gpsfrom-spoofers-is-critical-to-the-future-of-navigation

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

[13] E. Schmidt, Z. Ruble, D. Akopian, and D. J. Pack, "Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 8, pp. 2768–2784, Aug. 2019.

[14] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/N$_0$ estimates," in *Proc. ION GNSS*, Nashville, TN, USA, 2012, pp. 2878–2884.

[15] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," *Proc. IEEE*, vol. 104, no. 6, pp. 1246–1257, Jun. 2016.

[16] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, "Autonomous spoofing detection and mitigation in a GNSS receiver with an adaptive antenna array," in *Proc. ION GNSS*, Nashville, TN, USA, Sep. 2013, pp. 2937–2948.

[17] V. H. Nguyen, G. Falco, M. Nicola, and E. Falletti, "A dual antenna GNSS spoofing detector based on the dispersion of double difference measurements," in *Proc. 9th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2018, pp. 1–8.

[18] A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attacks on a vector based tracking GPS receiver," in *Proc. Int. Tech. Meeting Inst. Navigat.*, Newport Beach, CA, USA, Jan. 2012, pp. 790–800.

[19] M. T. 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. 577–589, Apr. 2017.

[20] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.

[21] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, and W. Feng, "GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations," *IEEE Access*, vol. 6, pp. 66428–66441, 2018.

[22] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proc. IEEE/ION Position, Location Navigat. Symp. Meeting (PLANS)*, Monterey, CA, USA, May 2014, pp. 262–269.

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

[24] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, "Effective GPS spoofing detection utilizing metrics from commercial receivers," in *Proc. Int. Tech. Meeting Inst. Navigat.*, Jan. 2018, pp. 672–689.

[25] Z. Zhang, M. Trinkle, L. Qian, and H. Li, "Quickest detection of GPS spoofing attack," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2012, pp. 1–6.

[26] 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. Satell. Commun. Netw.*, vol. 30, no. 4, pp. 181–191, Jul. 2012.

[27] J. Nielsen, A. Broumandan, and G. Lachapelle, "GNSS spoofing detection for single antenna handheld receivers," *Navigation*, vol. 58, no. 4, pp. 335–344, Dec. 2011.

[28] A. J. O'Brien and I. J. Gupta, "Comparison of output SINR and receiver C/N$_0$ for GNSS adaptive antennas," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 45, no. 4, pp. 1630–1640, Oct. 2009.

[29] C. Fernández-Prades, J. Arribas, and P. Closas, "Robust GNSS receivers by array signal processing: Theory and implementation," *Proc. IEEE*, vol. 104, no. 6, pp. 1207–1220, Jun. 2016, doi: 10.1109/JPROC.2016.2532963.

[30] Z. Lu, J. Nie, F. Chen, H. Chen, and G. Ou, "Adaptive time taps of STAP under channel mismatch for GNSS antenna arrays," *IEEE Trans. Instrum. Meas.*, vol. 66, no. 11, pp. 2813–2824, Nov. 2017.

[31] R. T. Compton, "The power-inversion adaptive array: Concept and performance," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-15, no. 6, pp. 803–814, Nov. 1979.

[32] F. Chen et al., "Improved least mean square algorithm for power-inversion global navigation satellite system antenna array," *J. Nat. Univ. Defense Technol.*, vol. 39, no. 3, pp. 47–51, Jun. 2017.

[33] J. Liu, L. Li, Z. Lv, F. Chen, and S. Ni, "Impact of element pattern on the performance of GNSS power-inversion adaptive arrays," *Electronics*, vol. 8, no. 10, p. 1120, Oct. 2019.

[34] A. J. O'Brien, *Adaptive Antenna Arrays for Precision GNSS Receivers*. Columbus, OH, USA: Ohio State Univ., 2009.

[35] J. W. Betz and K. R. Kolodziejski, "Generalized theory of code tracking with an early-late discriminator—Part I: Lower bound and coherent processing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 45, no. 4, pp. 1538–1556, Oct. 2009.

[36] M. L. Psiaki, D. M. Akos, and J. Thor, “A comparison of direct RF sampling and down-covert & sampling GNSS receiver architectures,” in *Proc. ION GPS*, Sep. 2003, pp. 1941–1952.

[37] A. J. Van Dierendonck, “GPS receivers,” in *Global Positioning System: Theory and Applications*, vol. 1, B. W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge, Eds. Reston, VA, USA: American Institute for Aeronautics and Astronautics, 1996.

[38] D. R. Pauluzzi and N. C. Beaulieu, “A comparison of SNR estimation techniques for the AWGN channel,” *IEEE Trans. Commun.*, vol. 48, no. 10, pp. 1681–1691, Oct. 2000.

[39] M. Sharawi, D. Akos, and D. Aloi, “GPS C/N_0 estimation in the presence of interference and limited quantization levels,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, no. 1, pp. 227–238, Jan. 2007.

[40] *BeiDou Navigation Satellite System Signal in Space Interface Control Document Open Service Signal B3I (Version 1.0)*, China Satell. Navigat. Office, Nanchang, China, Feb. 2018.

Jinyuan Liu received the B.S. and M.S. degrees from the National University of Defense Technology, Changsha, China, in 2017 and 2019, respectively, where he is currently pursuing the Ph.D. degree with the College of Electronic Science and Engineering.

His current research interests include array signal processing, Global Navigation Satellite System (GNSS) anti-jamming, and anti-spoofing.

Feiqiang Chen received the Ph.D. degree in satellite navigation technology from the National University of Defense Technology, Changsha, China, in 2017.

He is currently an Assistant Professor with the College of Electronic Science and Engineering, National University of Defense Technology. His current research interests include Global Navigation Satellite System (GNSS) antijamming and low earth orbit (LEO) navigation enhancement.

Yuchen Xie received the Ph.D. degree in satellite navigation technology from the National University of Defense Technology, Changsha, China, in 2022.

He is currently a Lecturer with the College of Electronic Science and Engineering, National University of Defense Technology. His current research interests include Global Navigation Satellite System (GNSS) signal processing and GNSS anti-jamming.

Beibei Ge received the B.S. degree in information engineering from the National University of Defense Technology, Changsha, China, in 2017, where she is currently pursuing the Ph.D. degree in information and communication engineering.

Her research interests include synthetic aperture radar imaging and ground moving target indication (GMTI).

Zukun Lu received the B.S. and M.S. degrees from the Chinese Aviation University of Air Force, Changchun, China, in 2011 and 2013, respectively, and the Ph.D. degree from the College of Electronic Science and Technology, National University of Defense Technology, Changsha, China, in 2018.

Since 2014, he has been with the College of Electronic Science and Technology, National University of Defense Technology. He is currently a Lecturer. His current research interests include satellite-based navigation antijamming and measurements.

Guangfu Sun is currently a Full Professor and the Director of the College of Electronic Science and Technology, National University of Defense Technology, Changsha, China. His current research interests include Global Navigation Satellite System (GNSS) signal processing, GNSS time synchronization, and low earth orbit (LEO) navigation enhancement.