IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 January 2023, accepted 13 February 2023, date of publication 22 February 2023, date of current version 1 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3247968

RESEARCH ARTICLE

INS-Aided Multi-Antenna GNSS Carrier Phase Double Difference Spoofing Detection

XIN ZHANG[1], CHENCONG DING[1], HUI XIA[1], HAO LIU[1], AND YAO YAO[2]
[1]Naval Research Institute, Shanghai 200436, China
[2]Naval Research Institute, Beijing 100036, China
Corresponding author: Xin Zhang (marmy@163.com)

ABSTRACT The effective spoofing detection can prevent GNSS receiver from providing erroneous positioning, velocity and timing information. Most of the available multi-antennas carrier phase double difference-based spoofing detection methods, regardless of the aiding of inertial navigation system (INS), exploit the divergence in carrier phase double differences derived from the direction of arrival (DOA) characteristics of the authentic signal and spoofing signal. However, the traditional methods mainly implemented by dual-antenna GNSS receivers has spatial ambiguity and lacks global detection performance analysis. Furthermore, an INS-aided multi-antenna spoofing detection method is proposed without spatial ambiguity comparing the predicted signal DOA by INS and the vectoral carrier phase double differences measured by multi antennas. To analyze the influence of the antenna array baseline length and signal DOA on the detection performance, a comprehensive numerical simulation was conducted. The dead zone of the proposed detection method is revealed to assess the global spoofing detection performance. The effectiveness of the proposed method is verified under the GNSS positioning scenarios. In the worst case, spoofing signals can be effectively detected in 95.2% of the airspace under one time the wavelength antenna baseline configuration and in 99.3% of the airspace under five times the wavelength antenna baseline configuration, respectively.

INDEX TERMS Inertial navigation system aiding, GNSS spoofing detection, carrier phase, multi-antenna.

I. INTRODUCTION

Global Navigation Satellite System (GNSS) can provide continuous and reliable positioning, velocity and timing services in both military and civil fields [1], [2]. It has the characteristics of global, all-weather and high accuracy. However, the open structure and weak power of satellite signals have made GNSS services vulnerable to various intentional and unintentional interferences, seriously impairing the reliability of GNSS applications [3], [4], [5], [6]. Among all kinds of interferences, the jamming that destroys the signal receiving capability of GNSS receiver by strong interference power can be easily squelched by forming nulls filter in the directions of interference through antenna array [7], [8]. Unfortunately, the spoofing is deliberately designed to mislead GNSS receivers by generating fabricated GNSS signals, for which GNSS receivers cannot discriminate the spoofing and authentic signals, resulting in the hazardously misleading navigation solution [9]. Hence, the detection of spoofing attacks has become a more general concern in recent years. Several different GNSS spoofing detection methods have been proposed, which can be categorized into three groups: with cryptographic anti-spoofing, anti-spoofing with external sources aiding, and anti-spoofing by extracting features between spoofing and authentic signals [10], [11], [12], [13], [14], [15]. Among the different spoofing detection methods, the DOA defense is considered as one of the most effective methods when the spoofing signals are broadcasted from a single source. But it's not well adapted to the situation where the spoofing signals come from different directions [13], [16]. On the other hand, checking the consistency of the navigation solutions with other reference sources is also an effective

The associate editor coordinating the review of this manuscript and approving it for publication was Hongli Dong.

spoofing detection method [17], [18], [19]. More importantly, it is theoretically unaffected by whether the spoofing signals come from the same direction. In particular, the consistency check of GNSS and INS has attracted increasingly attention with the complementary characteristics of these two systems, where GNSS relies on external signals, but the positioning error does not accumulate over time while INS is just the opposite. For this reason, in a GNSS/INS integration system, as only GNSS measurements are potentially erroneous due to spoofing, INS measurements can play the role of integrity monitor to detect an attack [3]. Some of the proposed GNSS-INS spoofing detection methods are as follows: receiver autonomous integrity monitoring (RAIM) based anti-spoofing [20], platform relative motion estimation results comparison method [21], and integrated navigation residuals monitoring method [22]. Meanwhile, the spoofing detection method proposed in [23], [24], and [25] combines DOA method and INS-aided method in a dual-antenna receiver to detect the spoofing signals based on carrier phase double differenced measurements [26], which needs no modifications on the receiver or antennas configuration. It is a very promising GNSS-INS consistent spoofing detection method. However, it is obvious that there is a spatial ambiguity in DOA when using a dual-antenna receiver for DOA detection. In addition, the method cannot be directly generalized to spoofing detection with more than two nonlinear antenna arrays.

Herein, a spoofing detection approach based on INS-aided nonlinear multi-antenna array receiver is proposed, which can be applied to the spoofing detection of receivers using more than two antennas. To detect a spoofing attack, the proposed method calculates the DOA of an authentic signal with the position and attitude provided by the INS. Comparing the DOA of calculated signal with the corresponding signal obtained by the multi-antenna receiver through the carrier phase double-differences, a hypothesis test procedure is implemented to discriminate the spoofing. Different from the current INS-aided dual-antenna receiver spoofing detection methods [23], [24], [25], the nonlinear multi-antennas array receiver can eliminate the spatial ambiguity DOA. Eventually, comprehensively analysis on the corresponding detection performance is conducted by simulated experiments, which are the main contribution of this paper.

II. DUAL-ANTENNA CARRIER PHASE DOUBLE DIFFERENCE

As shown in Figure 1, taking the dual-antenna receiver as an example, the principle of the antenna array measuring the signal DOA of satellite i is explained [27].

In Figure 1, $\mathbf{S}^i$ is the unit line of sight (LOS) vector to satellite i in the east-north-up (ENU) coordinate frame, $\mathbf{J}$ denotes the LOS vector to the spoofer transmitting antenna in the ENU frame, $\mathbf{b}$ is the baseline vector between the two antennas (in the body frame) in the units of wavelength cycles. Herein, the carrier phase difference of the

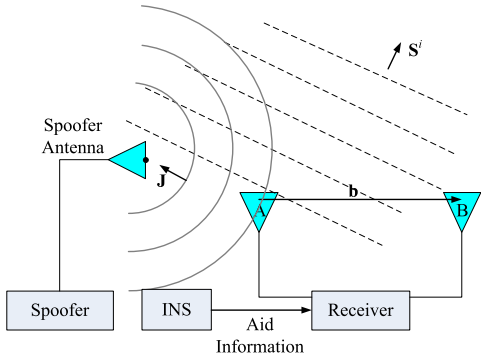


FIGURE 1. Schematic principle of the signal DOA measurement using dual-antenna.

satellite i received by the two antennas is

$$d\phi^i = \mathbf{b}^{\mathrm{T}}\mathbf{P}\mathbf{S}^i + N^i + Q + \gamma^i \tag{1}$$

where $\mathbf{P}$ is the direction cosine matrix to rotate vectors in the ENU frame to the body frame, N^i is the integer ambiguity for satellite i, Q is a constant line bias or time varying delta-clock term (depending on implementation), γ^i is the summation of the carrier phase error terms for satellite i received by each antenna.

It is noted that Q can be ignored after the calibration which takes no effect on the subsequent double differences constructed by the carrier phase difference. Therefore, Q and the arbitrary integer ambiguity N^i can be neglected [24]. The expression $\mathbf{b}^{\mathrm{T}}\mathbf{P}\mathbf{S}^i$ should be recognized as the inner product between vectors $\mathbf{S}^i$ and $\mathbf{b}$. When the attitude of the dual-antenna array is determined by INS [23], $\mathbf{b}^{\mathrm{T}}\mathbf{P}\mathbf{S}^i$ can be converted to the scalar form $\|\mathbf{b}\|\cos\left(\Psi^i\right)$, where Ψ^i denotes the incidence angle of satellite i in the body frame, as shown in Figure 2.

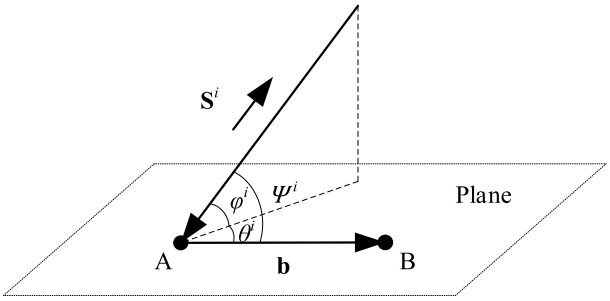


FIGURE 2. Geometric relationship between Ψ^i, φ^i and θ^i.

Then, we have

$$d\phi^i = \|\mathbf{b}\|\cos\left(\Psi^i\right) + \gamma^i \tag{2}$$

Decomposing the incident angle Ψ^i into elevation φ^i and azimuth θ^i in the body frame plane, we have the geometric relation:

$$\cos(\Psi^i) = \cos\left(\varphi^i\right)\cos\left(\theta^i\right) \tag{3}$$

According to (3), equation (1) can be rearranged as

$$d\phi^i = \|\mathbf{b}\| \cos\left(\varphi^i\right) \cos\left(\theta^i\right) + \gamma^i \tag{4}$$

Namely, the carrier phase difference of satellite i received by the two antennas is determined by three factors: the length of the antenna baseline, signal elevation and azimuth.

In a similar manner, taking satellite j into consideration, the carrier phase double difference can be formed as

$$\begin{aligned}\Delta d\phi^{ij} &= d\phi^i - d\phi^j \\ &= \|\mathbf{b}\| \left[\cos\left(\varphi^i\right) \cos\left(\theta^i\right) - \cos\left(\varphi^j\right) \cos\left(\theta^j\right)\right] + \gamma^{ij}\end{aligned} \tag{5}$$

where $\gamma^{ij} = \gamma^i - \gamma^j$. With or without INS aiding, the dual-antenna carrier phase double difference in (5) is always the basis for numerous spoofing detection methods [6], [23], [24], [25].

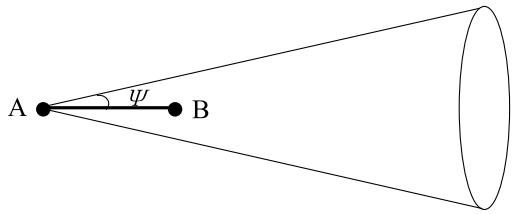


FIGURE 3. Spatial ambiguity of dual-antennas.

However, as shown in Figure 3, when the signals incident from the cone surface to the dual-antennas A and B, there are almost identical carrier phase differences computed from (4). It is implied that the signal DOA obtained by dual-antenna has spatial ambiguity. This feature is adverse for spoofing detection, which makes it difficult to evaluate detection performance spatially.

III. PRINCIPLE OF INS-AIDED MULTI-ANTENNA SPOOFING DETECTION

A. MULTI-ANTENNAS CARRIER PHASE DOUBLE DIFFERENCE

1) MINIMUM NUMBER OF ANTENNAS REQUIRED TO ELIMINATE SPATIAL AMBIGUITY

In the multi-antenna GNSS application system, it is a widely used configuration that the number of antennas is greater than two. Therefore, by deploying more antennas in detection, the spatial ambiguity of signal DOA can be eliminated to achieve a more robust spoofing detection performance. Taking a triple-antenna receiver as an example, the three antennas, which is the least minimum number of required antennas, are denoted as A, B and C, respectively. The x-axis and the y-axis lie within the plane where the three antennas are located. A is the origin to establish a Cartesian coordinate system. The baseline direction of B is aligned with the y-axis, the z-axis points along the zenith direction mutually perpendicular to the plane, and the xyz-axis satisfies the right-handed convention, as viewed in Figure 4.

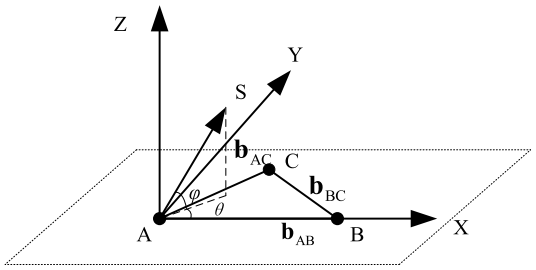


FIGURE 4. Signals DOA relationship under triple-antenna configuration.

The LOS vector of the satellite incident signal in the triple-antenna coordinate system can be expressed as:

$$\mathbf{S} = [x_s, y_s, z_s]^{\mathrm{T}} = [\cos\varphi\cos\theta, \cos\varphi\sin\theta, \sin\varphi]^{\mathrm{T}} \tag{6}$$

It is noted that $\mathbf{S}$ can be transformed from $\mathbf{S}^i$ with the a priori attitude information provided by INS, which is almost unaffected by signal spoofing. The coordinates of the three antennas are A=$[0, 0, 0]^{\mathrm{T}}$, B=$[x_{\mathrm{B}}, 0, 0]^{\mathrm{T}}$ and C=$[x_{\mathrm{C}}, y_{\mathrm{C}}, 0]^{\mathrm{T}}$. The corresponding antenna baseline vectors are $\mathbf{b}_{\mathrm{AB}}$, $\mathbf{b}_{\mathrm{AC}}$, and $\mathbf{b}_{\mathrm{BC}}$, respectively. Since the A, B and C coordinates can be measured in advance, $\mathbf{b}_{\mathrm{AB}}$, $\mathbf{b}_{\mathrm{AC}}$, and $\mathbf{b}_{\mathrm{BC}}$ are also known vectors. When the carrier phase measurement noise is absent, applying (1) and (2) into (7) yields

$$\begin{cases} \mathbf{b}_{\mathrm{AB}}^{\mathrm{T}}\mathbf{S} = d\phi_{\mathrm{AB}} \\ \mathbf{b}_{\mathrm{AC}}^{\mathrm{T}}\mathbf{S} = d\phi_{\mathrm{AC}} \\ \mathbf{b}_{\mathrm{BC}}^{\mathrm{T}}\mathbf{S} = d\phi_{\mathrm{BC}} \end{cases} \tag{7}$$

The equation (7) can be rewritten in matrix form:

$$\mathbf{ES} = \mathbf{c} \tag{8}$$

where

$$\mathbf{E} = \begin{bmatrix} \mathbf{b}_{\mathrm{AB}}^{\mathrm{T}} \\ \mathbf{b}_{\mathrm{AC}}^{\mathrm{T}} \\ \mathbf{b}_{\mathrm{BC}}^{\mathrm{T}} \end{bmatrix} = \begin{bmatrix} x_{\mathrm{B}} & 0 & 0 \\ x_{\mathrm{C}} & y_{\mathrm{C}} & 0 \\ x_{\mathrm{C}} - x_{\mathrm{B}} & y_{\mathrm{C}} & 0 \end{bmatrix} \tag{9}$$

$$\mathbf{c} = [d\phi_{\mathrm{AB}}, d\phi_{\mathrm{AC}}, d\phi_{\mathrm{BC}}]^{\mathrm{T}} \tag{10}$$

When $y_c \neq 0$, namely the three antennas are not arranged in a line, it is concluded that $rank(\mathbf{E})$=2 by the elementary matrix transformation. Then the augmented matrix $\mathbf{U}$ is

$$\mathbf{U} = \left[\mathbf{E}\ \mathbf{c}\right] \tag{11}$$

The rank of $\mathbf{U}$ and $\mathbf{E}$ is identical, so the coefficient matrix of (7) is not a full-rank. Consequently, the solution of the nonlinear equation is not unique, which means that the obtained signal LOS vector $\mathbf{S}$ is also ambiguous.

However, considering that the elevation φ ranges from 0 to $\pi/2$, we have

$$\begin{aligned} z_{\mathrm{S}} &= \sqrt{1 - \cos^2\varphi} \\ &= \sqrt{1 - \left(\cos^2\varphi\cos^2\theta + \cos^2\varphi\sin^2\theta\right)} \\ &= \sqrt{1 - \left(x_{\mathrm{S}}^2 + y_{\mathrm{S}}^2\right)} \end{aligned} \tag{12}$$

Then, we can see that in (7) only x_S and y_S need to be solved, so (7) can be rewritten as:

$$\begin{cases} x_B x_S = d\phi_{AB} \\ x_C x_S + y_C y_S = d\phi_{AC} \end{cases} \tag{13}$$

Considering $rank(\mathbf{U})=rank(\mathbf{E})=2$, equation (13) has a unique solution, which means that the LOS vector $\mathbf{S}$ of the incident signal calculated from the carrier phase difference is unique, then spatial ambiguity in the DOA is eliminated.

2) CARRIER PHASE DOUBLE DIFFERENCE VECTOR

Based on (4), the carrier phase differences of two satellites i and j on baseline AB are as follows,

$$d\phi_{AB}^{i} = x_B \cos\left(\varphi^{i}\right)\cos\left(\theta^{i}\right) + \gamma_{AB}^{i} \tag{14}$$

$$d\phi_{AB}^{j} = x_B \cos\left(\varphi^{j}\right)\cos\left(\theta^{j}\right) + \gamma_{AB}^{j} \tag{15}$$

Similarly, we have the carrier phase difference on baseline AC:

$$d\phi_{AC}^{i} = x_C \cos\left(\varphi^{i}\right)\cos\left(\theta^{i}\right) + y_C \cos\left(\varphi^{i}\right)\sin\left(\theta^{i}\right) + \gamma_{AC}^{i} \tag{16}$$

$$d\phi_{AC}^{j} = x_C \cos\left(\varphi^{j}\right)\cos\left(\theta^{j}\right) + y_C \cos\left(\varphi^{j}\right)\sin\left(\theta^{j}\right) + \gamma_{AC}^{j} \tag{17}$$

Since the carrier phase differences of the three baselines AB, AC, and BC are correlated, the carrier phase difference on the BC baseline can be directly obtained from the carrier phase difference on the AB and AC. Therefore, the corresponding carrier phase difference on the BC baseline has no contribution to the carrier phase double difference spoofing detection.

Furthermore, the carrier phase difference of the same satellite signal with respect to the two baselines AB and AC is written as a vector form:

$$d\mathbf{\Phi}^{i} = \mathbf{H}\Lambda^{i} + \mathbf{Y}^{i} \tag{18}$$

$$d\mathbf{\Phi}^{j} = \mathbf{H}\Lambda^{j} + \mathbf{Y}^{j} \tag{19}$$

where

$$d\mathbf{\Phi}^{k} = \begin{bmatrix} d\phi_{AB}^{k} \\ d\phi_{AC}^{k} \end{bmatrix}, k = i, j \tag{20}$$

$$\mathbf{H} = \begin{bmatrix} x_B & 0 \\ x_C & y_C \end{bmatrix} \tag{21}$$

$$\mathbf{\Lambda}^{k} = \begin{bmatrix} \cos\left(\varphi^{k}\right)\cos\left(\theta^{k}\right) \\ \cos\left(\varphi^{k}\right)\sin\left(\theta^{k}\right) \end{bmatrix}, k = i, j \tag{22}$$

$$\mathbf{Y}^{k} = \begin{bmatrix} \gamma_{AB}^{k} \\ \gamma_{AC}^{k} \end{bmatrix}, k = i, j \tag{23}$$

Subtracting (18) from (19) yields the carrier phase double difference vector for satellites i and j,

$$\begin{aligned} \Delta d\mathbf{\Phi}^{ij} &= d\mathbf{\Phi}^{i} - d\mathbf{\Phi}^{j} \\ &= \mathbf{H}\left(\mathbf{\Lambda}^{i} - \mathbf{\Lambda}^{j}\right) + \left(\mathbf{Y}^{i} - \mathbf{Y}^{j}\right) \\ &= \mathbf{H}\mathbf{R}^{ij} + \boldsymbol{\eta}^{ij} \end{aligned} \tag{24}$$

It can be seen that the probability density function (PDF) of the carrier phase double difference vector is a two-dimensional PDF, rather than a one-dimensional PDF when using two antennas. It means that the spoofing detection method of dual-antenna carrier phase double difference cannot be directly used.

B. INS-AIDED MULTI-ANTENNA SPOOFING DETECTION PROCESS

1) HYPOTHESIS TEST MODEL

With the triple-antenna configuration shown in Figure 4, the INS-aided navigation system can precisely estimate its own attitude and position. Furthermore, with the known attitude and restored ephemeris, it is practicable to predict the DOA of each tracked satellite signal by using the a priori antenna baseline vector. For simplicity, a predicted satellite signal is set as p, and the signal of the same satellite received by the antennas is t. The incidence angles of p and t are denoted as Ψ^{p} and Ψ^{t}, the corresponding elevations are φ^{p}, φ^{t}, and the azimuths are θ^{p}, θ^{t}. Then, the carrier phase difference between the predicted signal p and the received signal t on AB can be expressed as

$$d\phi_{AB}^{p} = x_B \cos\varphi^{p}\cos\theta^{p} \tag{25}$$

$$d\phi_{AB}^{t} = x_B \cos\varphi^{t}\cos\theta^{t} + \gamma_{AB}^{t} \tag{26}$$

where γ_{AB}^{t} is the carrier phase difference noise of t on AB.

Then, the carrier phase difference on AC takes the similar expression,

$$d\phi_{AC}^{p} = x_C \cos\varphi^{p}\cos\theta^{p} + y_C \cos\varphi^{p}\sin\theta^{p} \tag{27}$$

$$d\phi_{AC}^{t} = x_C \cos\varphi^{t}\cos\theta^{t} + y_C \cos\varphi^{t}\sin\theta^{t} + \gamma_{AC}^{t} \tag{28}$$

Based on (18) and (19), the carrier phase difference of p or t on AB and AC can be written as:

$$d\mathbf{\Phi}^{p} = \mathbf{H}\Lambda^{p} + \boldsymbol{\gamma}^{p} \tag{29}$$

$$d\mathbf{\Phi}^{t} = \mathbf{H}\Lambda^{t} + \boldsymbol{\gamma}^{t} \tag{30}$$

The corresponding carrier phase double difference vector of p and t follows

$$\begin{aligned} \Delta d\mathbf{\Phi}^{pt} &= d\mathbf{\Phi}^{p} - d\mathbf{\Phi}^{t} \\ &= \mathbf{H}\left(\Lambda^{p} - \Lambda^{t}\right) + \left(\gamma^{p} - \gamma^{t}\right) \\ &= \mathbf{H}\mathbf{R}^{pt} + \boldsymbol{\eta}^{pt} \end{aligned} \tag{31}$$

assuming that p has no measurement noise, i.e. $\gamma^{p} = 0$.

When t is a spoofing signal, $\mathbf{R}^{pt} \neq 0$; When t is an authentic signal, $\mathbf{R}^{pt} = 0$. It is assumed that the hypotheses capture the spoofing signal. As a result, the carrier phase double difference vector $\Delta d\mathbf{\Phi}^{pt}$ can be used for spoofing detection. By using the principle of carrier phase double difference detection, a binary hypothesis test for spoofing detection is constructed as

$$\Delta d\mathbf{\Phi}^{pt} = \mathbf{H}\mathbf{R}^{pt} + \boldsymbol{\eta}^{pt} \quad \begin{cases} H_0 : \mathbf{R}^{pt} = 0 \\ H_1 : \mathbf{R}^{pt} \neq 0 \end{cases} \tag{32}$$

The assumptions under H_0/H_1 are:

(1) H_0: The received signal t in the carrier phase double difference detection is an authentic signal;

(2) H_1: The received signal t in the carrier phase double difference detection is a spoofing signal.

2) TEST STATISTIC

It is considered that the errors of the carrier phase measurements of the same signal provided by A, B and C are independent of each other. Assuming that they all follow a zero-mean Gaussian distribution with a variance of σ^2, then $\mathbf{Y}_{\mathrm{AB}}$ and $\mathbf{Y}_{\mathrm{AC}}$ obey a zero-mean Gaussian distribution with a variance of $2\sigma^2$, and $\boldsymbol{\eta}^{pt}$ can be expressed as

$$\boldsymbol{\eta}^{pt} = \left(\gamma^{p} - \gamma^{t}\right) = \begin{bmatrix} 0 - \gamma_{\mathrm{AB}}^{t} \\ 0 - \gamma_{\mathrm{AC}}^{t} \end{bmatrix} = \begin{bmatrix} \gamma_{\mathrm{AB}}^{t} \\ \gamma_{\mathrm{AC}}^{t} \end{bmatrix} \tag{33}$$

It is apparent that $\boldsymbol{\eta}^{pt}$ follows the $\boldsymbol{N}(\mathbf{0}, \mathbf{C})$ distribution, where the covariance matrix $\mathbf{C}$ can be expressed as

$$\begin{aligned} \mathbf{C} &= E\left[\boldsymbol{\eta}^{pt}\left(\boldsymbol{\eta}^{pt}\right)^{\mathrm{T}}\right] \\ &= \begin{bmatrix} E\left[\left(\gamma_{\mathrm{AB}}^{t}\right)^{2}\right] & E\left[\left(\gamma_{\mathrm{AB}}^{t}\right)\left(\gamma_{\mathrm{AC}}^{t}\right)\right] \\ E\left[\left(\gamma_{\mathrm{AC}}^{t}\right)\left(\gamma_{\mathrm{AB}}^{t}\right)\right] & E\left[\left(\gamma_{\mathrm{AC}}^{t}\right)^{2}\right] \end{bmatrix} \\ &= \sigma^{2}\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \end{aligned} \tag{34}$$

Furthermore,

$$\mathbf{C}^{-1} = \frac{1}{\sigma^{2}}\begin{bmatrix} 2/3 & -1/3 \\ -1/3 & 2/3 \end{bmatrix} \tag{35}$$

If t is an authentic signal, the distribution of the carrier phase double difference vector satisfies

$$\Delta d\boldsymbol{\Phi}^{pt} = \boldsymbol{\eta}^{pt} \sim \boldsymbol{N}\left(\mathbf{0}, \mathbf{C}\right) \tag{36}$$

If t is a spoofing signal, the distribution of the carrier phase double difference vector satisfies

$$\Delta d\boldsymbol{\Phi}^{pt} = \boldsymbol{\eta}^{pt} \sim \boldsymbol{N}\left(\mu, \mathbf{C}\right), \ with\ \boldsymbol{\mu} = \mathbf{H}\mathbf{R}^{pt} \tag{37}$$

It can be seen that $\Delta d\boldsymbol{\Phi}^{pt}$ is always a two-dimensional Gaussian distribution under different assumptions, and the probability distribution cannot be directly obtained as the traditional dual-antennas method. Therefore, the quadratic form of the Gaussian random variable is constructed by using $\Delta d\boldsymbol{\Phi}^{pt}$ under different assumptions respectively.

The detection statistic T_{H_0}, which follows the χ_2^2 distribution with 2 degrees of freedom under H_0 is constructed as

$$T_{H_0} = \left(\Delta d\boldsymbol{\Phi}^{pt}\right)^{\mathrm{T}}\mathbf{C}^{-1}\left(\Delta d\boldsymbol{\Phi}^{pt}\right) \sim \chi_2^2 \tag{38}$$

The detection statistic T_{H_1}, which follows the non-central χ'' distribution with 2 degrees of freedom under H_1, can be expressed as

$$T_{H_1} = \left(\Delta d\boldsymbol{\Phi}^{pt}\right)^{\mathrm{T}}\mathbf{C}^{-1}\left(\Delta d\boldsymbol{\Phi}^{pt}\right) \sim \chi''\left(\lambda\right) \tag{39}$$

where

$$\lambda = \boldsymbol{\mu}^{\mathrm{T}}\mathbf{C}^{-1}\boldsymbol{\mu} \tag{40}$$

The detection statistics under H_0 and H_1 can be universally expressed as $r = \left(\Delta d\boldsymbol{\Phi}^{pt}\right)^{\mathrm{T}}\mathbf{C}^{-1}\left(\Delta d\Phi^{pt}\right)$, then the detection procedure is defined as follows,

(1) $r \leq \rho_{th}$, H_0 is accepted;

(2) $r > \rho_{th}$, H_1 is accepted.

where ρ_{th} denotes the detection threshold. It can be known that the test statistics distribution under the H_1 condition will vary with the decentralization parameter λ, which makes different signal DOA under the constant false alarm rate have different detection performance.

3) DETECTION PROBABILITY CALCULATION

In this paper, the corresponding detection threshold is determined using a constant probability of false alarm. When P_{FA} is given, the spoofing signal detection threshold is derived as

$$\rho_{th} = Q_{\chi_2^2}^{-1}\left(P_{FA}\right) \tag{41}$$

where $Q_{\chi_2^2}^{-1}(\cdot)$ is the inverse function of the right-tailed probability of a central χ^2 distribution with two degrees of freedom.

Using the threshold, the corresponding spoofing detection probability reads

$$P_D = P\left\{T_{H_1} > \rho_{th} | H_1\right\} = Q_{\chi''}\left(\lambda\right) \tag{42}$$

where $Q_{\chi''}\left(\lambda\right)(\cdot)$ is the right-tail probability of a non-central distribution χ^2 with two degrees of freedom and a non-centrality parameter λ.

IV. SIMULATION

The performance of the proposed spoofing detection method was evaluated through simulations include: (a) the impact assessment of signal DOA and antenna array baseline length on detection performance; (b) the global detection performance evaluation; (c) the assessment of spoofing detection in two classical positioning scenarios accounting for attitude errors and antenna position errors. In our simulations, based on the antenna array shown in Figure 4, we assume that the received signal is GPS L1C/A code signal, whose carrier wavelength is set to ξ. The antenna array baseline length b is the integer multiples of carrier wavelength, and the receiver carrier measurement noise variance σ is set as 0.01ξ [28]. Furthermore, in order to simplify the calculation process, the antenna array is set as an equilateral triangle array, namely

$$x_B = b, x_C = \frac{1}{2}b, y_C = \frac{\sqrt{3}}{2}b \tag{43}$$

A. DETECTION PERFORMANCE

According to (42), the baseline length b and the signal DOA will directly affect $\mathbf{H}$ and $\mathbf{R}^{pt}$, thus changing the decentralization parameter λ under the condition of H_1, which results the different spoofing detection performance.

The effects of b and signal DOA on λ obtained from (21), (37) and (39) can be expressed as

$$\begin{aligned}\lambda &= \boldsymbol{\mu}^{\mathrm{T}}\mathbf{C}^{-1}\boldsymbol{\mu} \\ &= \frac{b^2\left[(\cos\varphi^p)^2+(\cos\varphi^t)^2-2\cos\varphi^p\cos\varphi^t\cos\left(\theta^p-\theta^t\right)\right]}{2\sigma^2}\end{aligned} \tag{44}$$

Based on the properties of $Q^2_{\chi''}(\lambda)(\cdot)$ and $Q_{\chi^2_2}(\cdot)$, the increase of λ will increase the spoofing detection probability.

1) ANTENNA ARRAY BASELINE LENGTH

Equation (44) shows that the increase of b will increase the λ, thereby improving the detection performance. Assuming that the azimuth/elevation of the predicted signal and received signal are (20°,40°) and (121°,40°) respectively, the spoofing detection ROC with different b can be presented in Figure 5.

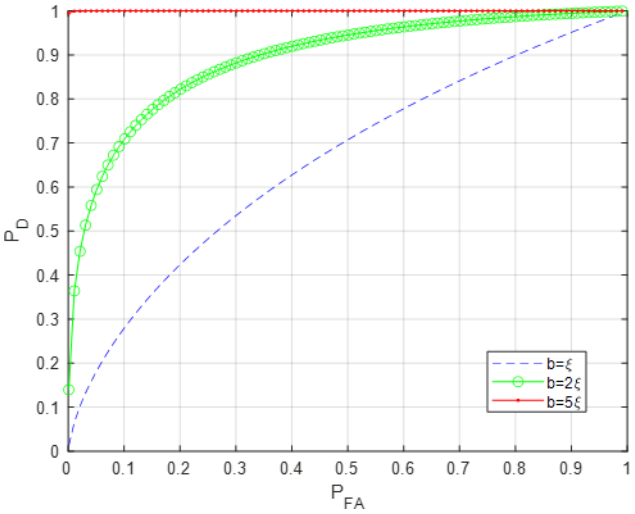


FIGURE 5. Carrier phase double difference spoofing detection ROC with different b.

It can be seen that, given the DOA, the detection performance is significantly improved with the increase of b.

2) DIRECTION OF ARRIVAL

The spoofing detection performance is not only nonlinearly related to the elevations of the predicted signal, but also the difference between the azimuths of them. We take the two different groups of predicted signals and received signals as an example. The simulation result is shown in Figure 6, where the azimuth/elevation of the first group of signals are (110°,35°), (110°,34°), the second are (10°,10°), (10°,9°). In addition, the ROC is simulated at $b = 5\xi$. It can be seen that the two groups of signals have a significant difference in detection performance.

It is difficult to obtain intuitive analysis results for the complex relationship between the detection performance and DOA. Therefore, we set the predicted signal DOA, and then

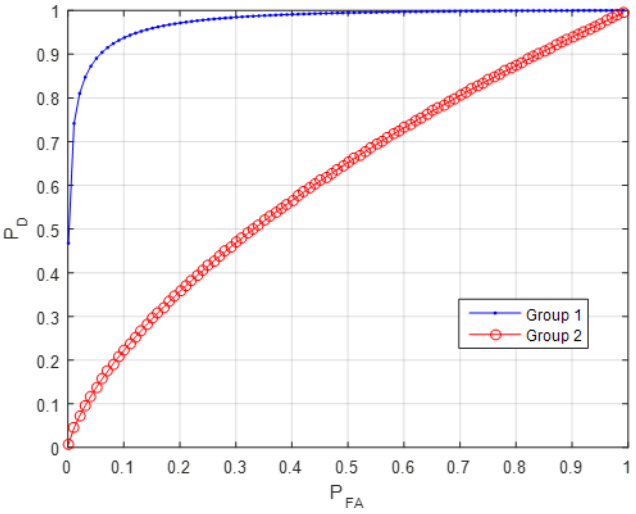


FIGURE 6. Carrier Phase Double Difference Detection ROC with Different DOA.

within the entire azimuth/elevation range, traversal calculations can be performed according to a certain angular resolution. Under a fixed false alarm rate, the detection probability distribution with the received signal coming from different directions can be obtained to illustrate the detection performance variation.

The azimuth/elevation of five predicted signals are (40°,35°), (160°,20°), (240°,55°), (320°,70°) and (120°,70°), respectively. The angular resolution is set to 1° and the false alarm rate is fixed to 0.01. Under the condition of $b = \xi$, the detection probability distribution on the case that the reference signal DOA is fixed while spoofing signal incident signal varies from different azimuth/elevation is calculated, as shown in Figure 7. Figure 7a illustrates the probability distribution of a single prediction signal. Figure 7b illustrates the variation in detection probability as the DOA changes.

From Figure 7, the spoofing detection probability around the predicted signal drops remarkably. In addition, the predicted signals with different elevations present different decreasing patterns of detection probability. Moreover, comparing the results among the same elevation (320°,70°) and (120°,70°), it can be seen that the detection probability distribution around the two signals are the same. These situations are consistent with the influence characteristics of elevation and azimuth on detection probability.

B. GLOBAL DETECTION PERFORMANCE EVALUATION

1) DETECTION DEAD ZONE

From the evaluation results of the detection performance at different signal DOA, there is a region with a small detection probability around the incident angle at each predicted signal. This is because the spoofing detection performance drops significantly when the spoofing signal is close to the predicted signal. Especially when the spoofing signal and the predicted signals come from the same direction, there will be λ =0. So,

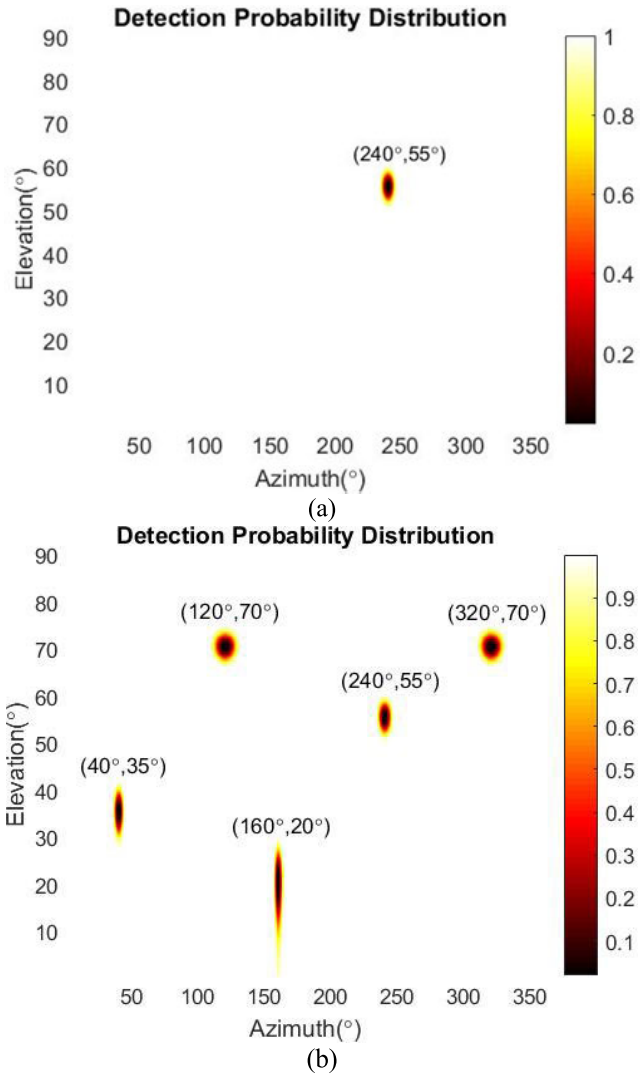


FIGURE 7. Detection probability distribution with different DOA: (a) the probability distribution of a single predicted signal; (b) the probability distribution of five predicted signals.

the test statistic distributions under the H_0 and H_1 are exactly same. The detection probability is equal to the false alarm probability.

Therefore, a detection probability threshold is set at a specific false alarm rate, and the area around the predicted signal, in which detection probability smaller than the threshold is defined as a detection dead zone. Under the condition of a constant false alarm ratio, the false alarm rate of spoofing detection is set to P_{FA}, and the area of detection probability $P_D < P_{D,th}$ around the predicted signal is the detection dead zone.

As shown in Figure 7, under every predicted signal DOA, the detection probability threshold $P_{D,th} = 0.99$ is set when the false alarm rate $P_{FA} = 0.01$. When the detected signal is a spoofing signal, the area around the predicted signals, which have a worse detection probability than $P_{D,th}$, are detection dead zone.

2) GLOBAL DETECTION PERFORMANCE

By defining the detection dead zone, the maximum size of the detection dead zone of all possible predicted signals DOA can be used as a reference for global detection performance assessment. Under the condition where $P_{FA} = 0.01$, and $b = \xi, b = 5\xi$ respectively, we use an azimuth/elevation of 5° × 5° square block for the traversal simulation. When setting the detection probability threshold to 0.99, the simulation can give the detection dead zone size in the whole DOA range. In the simulation, the middle angle of each block is taken as the incident angle of the predicted signal. Additionally, the angular resolution of the other incident signal from different azimuth/elevation angles is set to 1°. The simulation results are shown in Figure 8.

The size of the detection dead zone in Figure 8 is represented by the number of azimuth/elevation blocks of 1° × 1°. From equation (44), it can be seen that when the elevation angle is close to 90°, λ tends to 0, which causes the detection performance to drop sharply. Therefore, a more detailed analysis of the size of the detection dead zone is carried out for the area. The obtained maximum detection dead zone is used as the maximum size of the detection dead zone, so as to obtain the lower bound of the global spoofing detection performance.

Supposing the elevation range in [85°,90°), and the azimuth range in [0°,360°), we traverse the azimuth/elevation angle blocks of 1° × 1° and calculate the distribution of detection dead zone within a limited area. The calculation results show that the maximum detection dead zone is 1554 when $b = \xi$, and the maximum detection dead zone size is reduced to 232 when $b = 5\xi$.

As for the azimuth/elevation block of 1° × 1°, the area denotes as 1. Based on the analysis above, when $b = \xi$ or $b = 5\xi$, the maximum detection dead zone is no more than 4.8% or 0.7% of the entire area, an excellent detection performance outcome in most cases.

C. ANALYSIS OF SPOOFING DETECTION CAPABILITY UNDER POSITIONING SCENARIOS

With the comparison of two different spoofing and positioning scenarios at two different locations, the proposed INS-aided detection method is simulated and analyzed accounting for attitude errors and antenna position errors. Typical values are on the order of 0.05 deg [29] on all axes in the simulation when a navigation grade INS (i.e., position drifts of approximately 1 nmi/hr unaided) is equipped. In addition, typical antenna installation error with 3 mm uncertainty is added in the simulation. It is noted that the predicted signals are calculated by simulated INS-derived solutions and GNSS ephemeris. The detailed simulation conditions are as follows:

(1) With antenna A as the origin, the positions are set to Location 1 ($30°N$,$120°E$) and Location 2 ($38°N$,$77°E$), as shown in Figure 9. Attitude is set to (0°,0°,0°).

(2) Scenario 1: The DOA of all the spoofing signals are completely different. At 12:00 UTC, spoofing signals with

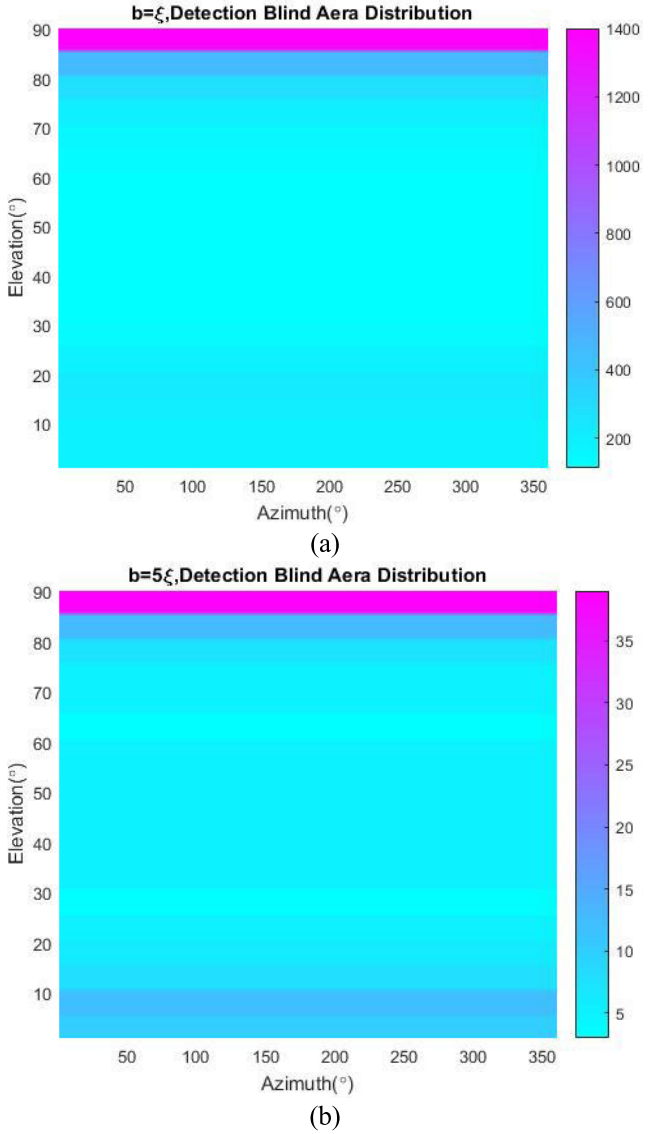


FIGURE 8. Distribution of detection dead zone with different baseline lengths: (a) b= ξ; (b) b=5ξ.

PRN 3, 29 and 32 arrive at the receiver antennas with incident angle of (276°,24°), (60°,30°), (150°,23°), respectively; Scenario 2: The DOA of all the spoofing signals are exactly consistent. At 12:00 UTC, spoofing signals with PRN 2, 20 and 29 arrive at the receiver antennas at the incident angle of (150°,23°). The specific incident angles of the spoofing signals under the two scenarios are shown in Table 1.

(3) The x-axis is along the baseline direction of the array element AB, lying in the east-west direction. With the assistance of INS, the angle at which each visible satellite signal reaches the antenna is predicted. After setting the satellite cut-off angle to 10°, the sky plot of the corresponding predicted satellite signal and spoofing signal are shown in Figure 10.

(4) Given carrier phase measurement noise variances are 0.01ξ, 50000 samples of carrier phase double differences are generated using the Monte Carlo method;

TABLE 1. Spoofing signal DOA setting.

No	Scenario	Jam No.	Azim	Elev
1	Scenario 1	J03	276°	24°
		J29	60°	30°
		J32	150°	23°
	Scenario 2	Jam (3,29,32)	150°	30°
2	Scenario 1	J02	276°	24°
		J20	60°	30°
		J29	150°	23°
	Scenario 2	Jam (02,20,29)	150°	30°

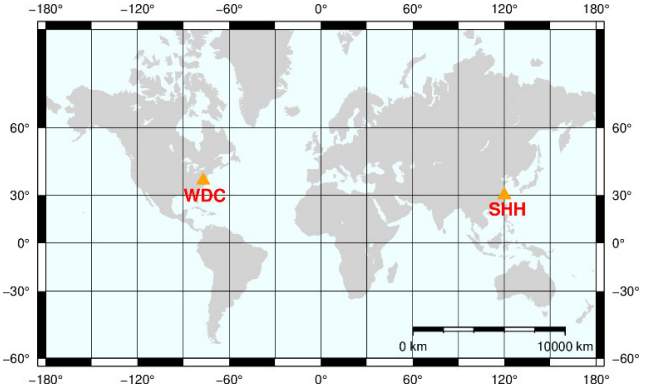


FIGURE 9. Simulation location (Location 1: SHH, Location 2: WDC).

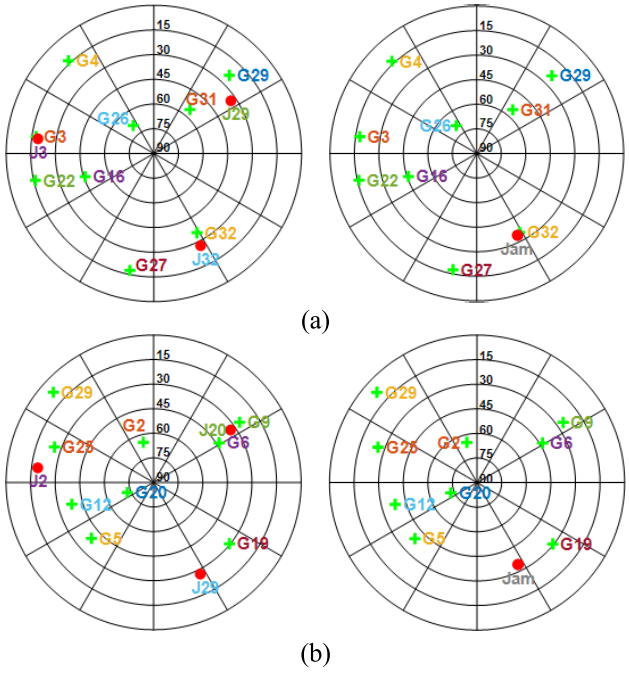


FIGURE 10. Sky plot of satellite signals and spoofing signals: (a) Location 1; (b) Location 2. The left is under Scenario 1, and the right is under Scenario 2.

(5) The false alarm probability P_{FA} is 0.01 and the antenna array baseline length is set to the carrier wavelength ξ.

As shown in Figure 10, both location 1 and location 2 can receive G9 satellite signal. For each scene at Location 1 and

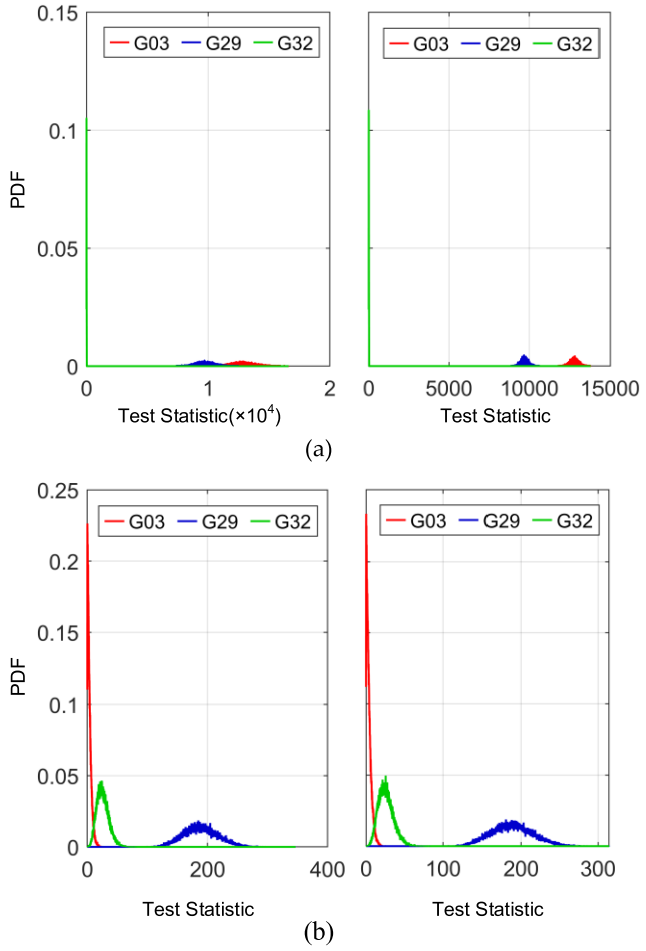


FIGURE 11. Distribution of different PRNs test statistics at location 1: (a) Scenario 1; (b) Scenario 2. The right panel represents the case accounting for attitude and antenna position errors, and the left does not.

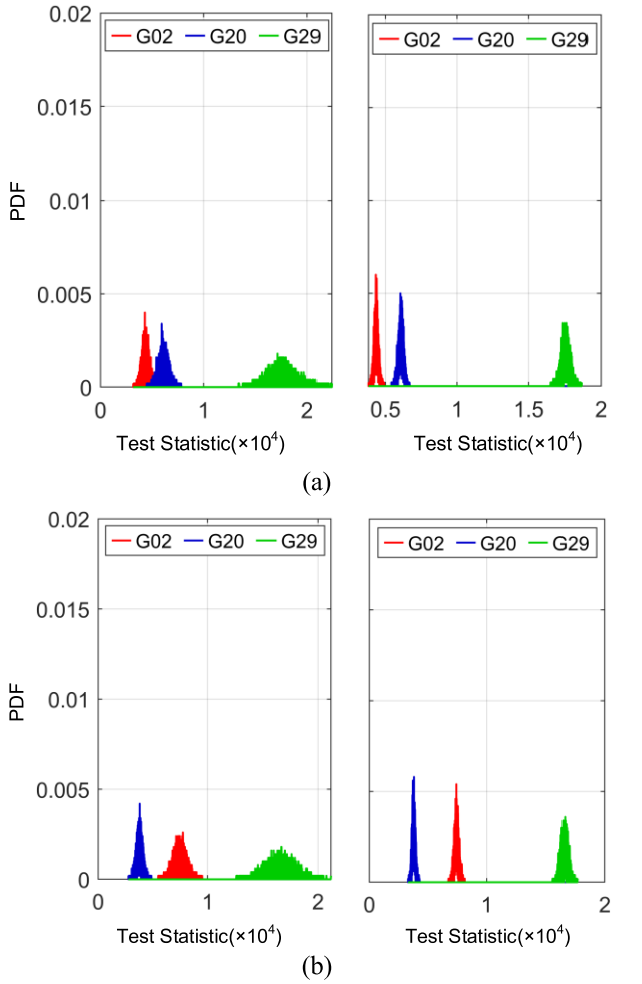


FIGURE 12. Distribution of different PRNs test statistics at location 2: (a) Scenario 1; (b) Scenario 2. The right panel represents the case accounting for attitude and antenna position errors, and the left does not.

TABLE 2. Simulation results.

No	PRN	Predicted Signal		P_D(%)	
		Azim	Elev	Scenario1	Scenario2
1	G03	276°	22°	6.57/6.60/(**6.49**)	100/100(**100**)
	G29	48°	21°	100/100(**100**)	100/100(**100**)
	G32	148°	30°	97.4/97.7(**97.6**)	24.4/24.4(**24.7**)
2	G02	356°	67°	100/100(**100**)	100/100(**100**)
	G20	233°	76°	100/100(**100**)	100/100(**100**)
	G29	313°	12°	100/100(**100**)	100/100(**100**)

Location 2, the test statistics distribution of spoofing signals is shown as follows.

Equations (41) and (42) indicate that we can calculate the theoretical detection probability of each satellite. The corresponding detection threshold is 9.21 when P_{FA} is 0.01. The statistical results of the detection performance for each satellite are shown in Table 2. It should be noted that the first, before slash, denotes the detection probability accounting for attitude errors and antenna position errors. The second term without accounting for these errors is shown here for comparison. It can be seen that the distributions of test statistics have varied slightly before and after adding attitude errors and antenna positions in the simulation case. But the detection of each satellite is basically consistent with the theoretical value (listed in brackets). As shown in Figure 11, for location 1, the probability performance of G03 is lower in scenario 1. Nevertheless, higher detection performance can be obtained in scenario 2, which can be seen from Figure 12. This is because under scenario 1, the DOA of the spoofing signal is relatively close to the predicted signal. The decreasing decentralization parameter λ leads to lower detection performance. Similar experimental results can be seen for G32.

In fact, it is rare for the spoofing signal to have a similar incidence angle with the authentic satellite signal. Under the case of spoofing signals from different directions, even if the DOA of few spoofing signals are close to a corresponding authentic signal, there is a high probability that it can be detected and excluded by RAIM [20]. This process is feasible

to perform in the case of spoofing signals coming from a same direction. All the simulation results verify the effectiveness of the proposed detection method.

V. CONCLUSION

A novel INS-aided multi-antenna carrier phase double difference spoofing detection method is developed and tested in this contribution. Unlike the traditional dual-antenna carrier phase double difference spoofing detection methods, the proposed method extends the carrier phase double differenced spoofing detection model to a vector form by inducing one more antenna, which eliminates the spatial ambiguity of dual-antenna DOA detection. Then, in the absence of spatial ambiguity, the influence of the antenna array baseline length and signal DOA on the proposed detection method are analyzed. Through the numerical simulation, the global evaluation of detection performance is comprehensively assessed on the basis of detection dead zone. In the worst case, spoofing signals can be effectively detected in 95.2% of the airspace with λ antenna baseline configuration and in 99.3% of the airspace with 5λ antenna baseline configuration, respectively. Simulation results have demonstrated that the proposed method perform a good application prospect for spoofing detection when applied to a system with both INS and antenna array equipped GNSS receivers.

The current work of this paper focuses on the spoofing detection procedure, including the detection probability calculation method and the analysis of detection performance. Further research will be conducted to deal with the influence of INS errors, antenna configuration and other influencing factors on the practical performance.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] F. Rothmaier, Y. Chen, S. Lo, and T. Walter, "GNSS spoofing detection through spatial processing," *NAVIGATION*, vol. 68, no. 2, pp. 243–258, Jun. 2021.

[2] J. Song, H. Wu, X. Guo, D. Jiang, X. Guo, T. Lv, and H. Luo, "GNSS spoofing identification and smoothing localization method for GNSS/Visual SLAM system," *Appl. Sci.*, vol. 12, no. 3, p. 1386, Jan. 2022.

[3] A. Broumandan and G. Lachapelle, "Spoofing detection using GNSS/INS/Odometer coupling for vehicular navigation," *Sensors*, vol. 18, no. 5, p. 1305, Apr. 2018.

[4] S. Daneshmand and G. Lachapelle, "Integration of GNSS and INS with a phased array antenna," *GPS Solutions*, vol. 22, no. 1, p. 3, Jan. 2018.

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

[6] 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.

[7] R. L. Fante and J. J. Vaccaro, "Wideband cancellation of interference in a GPS receive array," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 36, no. 2, pp. 549–564, Apr. 2000.

[8] Y. Zhao, F. Shen, G. Xu, and G. Wang, "A spatial–temporal approach based on antenna array for GNSS anti-spoofing," *Sensors*, vol. 21, no. 3, p. 929, Jan. 2021.

[9] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surv.*, vol. 48, no. 4, pp. 64:1–64:31, May 2016.

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

[11] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *J. Inst. Navigat.*, vol. 64, no. 1, pp. 51–66, 2017.

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

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

[14] A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Spoofing countermeasure for GNSS receivers—A review of current and future research trends," *Eur. Space Agency*, vol. 4, p. 6, Dec. 2013.

[15] 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.*, Feb. 2012, pp. 790–800.

[16] 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.

[17] P. D. Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*. Norwood, MA, USA: Artech House, 2013.

[18] N. Gu, F. Xing, and Z. You, "GNSS spoofing detection based on coupled visual/inertial/GNSS navigation system," *Sensors*, vol. 21, no. 20, p. 6769, Oct. 2021.

[19] B. Yuan, D. Liao, and S. Han, "Error compensation of an optical gyro INS by multi-axis rotation," *Meas. Sci. Technol.*, vol. 23, no. 2, 2012, Art. no. 025102.

[20] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, May 2014, pp. 1232–1239.

[21] 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. 27th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS+)*, 2014, pp. 745–758.

[22] S. Manickam and K. O'Keefe, "Using tactical and MEMS grade INS to protect against GNSS spoofing in automotive applications," in *Proc. 29th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS+)*, Nov. 2016, pp. 2991–3001.

[23] Y. Liu, Q. Fu, S. Li, and X. Xiao, "The effect of IMU accuracy on dual-antenna GNSS spoofing detection," in *Proc. Int. Tech. Meeting Inst. Navigat.*, Feb. 2016, pp. 169–180.

[24] Y. Liu, S. H. Li, X. Xiao, and Q. W. Fu, "INS-aided GNSS spoofing detection based on two antenna raw measurements," *Gyroscopy Navigat.*, vol. 7, no. 2, pp. 178–188, 2016.

[25] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proc. Int. Tech. Meeting Inst. Navigat.*, 2009, pp. 124–130.

[26] A. J. Jahromi, A. Broumandan, and G. Lachapelle, "GNSS signal authenticity verification using carrier phase measurements with multiple receivers," in *Proc. 8th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2016, pp. 1–11.

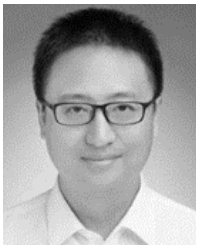
[27] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, no. 2, pp. 40–46, 2009. [Online]. Available: https://insidegnss.com/a-multi-antenna-defense-receiver-autonomous-gps-spoofing-detection/

[28] P. W. Ward, "Performance comparisons between FLL, PLL and a novel FLL-assisted-PLL carrier tracking loop under RF interference conditions," in *Proc. 11th Int. Tech. Meeting Satell. Division The Inst. Navigat.*, pp. 783–795, 1998.

[29] D. Gebre-Egziabher and Y. Shao, "Model for JPALS/SRGPS flexure and attitude error allocation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 46, no. 2, pp. 483–495, Apr. 2010.

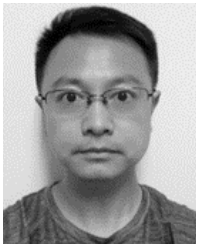
XIN ZHANG received the Ph.D. degree in information and communication engineering from the National University of Defense Technology, in 2015. He is currently an Engineer with Naval Research Institute. His current research interests include anti-spoofing and signal simulation for GNSS/BDS users.

CHENCONG DING received the master's degree in communication and information system from Beihang University, in 2010. He is currently a Senior Engineer with Naval Research Institute. His current research interest includes avionics systems.



HUI XIA received the master's degree in navigation guidance and control from the National University of Defense Technology, in 2004. He is currently a Senior Engineer with Naval Research Institute. His current research interests include airborne inertial navigation systems and ECM-electronic countermeasures.

HAO LIU received the master's degree in information and communication engineering from the Naval Aeronautical Engineering College, in 2003. He is currently a Senior Engineer with Naval Research Institute. His current research interest includes ECM-electronic countermeasures.



YAO YAO received the Ph.D. degree in communication and information system from the Academy of Equipment Command and Technology, in 2011. He is currently an Engineer with Naval Research Institute. His current research interests include navigation and time-frequency applications.