IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 23, 2017, accepted April 19, 2017, date of publication April 26, 2017, date of current version June 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2698070

GNSS Spoofing Countermeasure With a Single Rotating Antenna

FEI WANG, HONG LI, AND MINGQUAN LU
Department of Electronic Engineering, Tsinghua University, Beijing 100084, China
Corresponding author: Hong Li (lihongee@tsinghua.edu.cn)

This work was supported by the Natural Science Foundation of China under Grant 61571255.

ABSTRACT Security of global navigation satellite systems (GNSS) is important since the navigation capability provided by the GNSS is a key enabler for many civilian and military applications. Spoofing attacks threaten the GNSS security and have caught much attention recently. The spatial processing method is one of the most robust GNSS spoofing countermeasures, which detects spoofing signals with a moving antenna or multi-antenna, but it cannot work in a static single-antenna receiver. In this paper, we propose a spoofing countermeasure based on the power measurements of a single rotating antenna, which can be implemented in a static receiver. The method takes advantages of the anisotropy of the antenna's gain pattern to detect spoofing signals. When the antenna is rotating, the power measurements of the spoofing signals coming from the same direction change similarly and the correlation coefficients between them are close to 1, but the power measurements of the authentic signals are uncorrelated. Since it is not easy to evaluate the anti-spoofing performance of the correlation coefficient, another metric named phase difference of power measurements is proposed. Its theoretical performance is derived based on generalized likelihood ratio test and validated with simulations. Actual experiments indicate that both the simulated and meaconing spoofing signals can be distinguished from the authentic ones, and the method can be implemented in a static or low-dynamic conventional receiver, only with an additional low-cost rotary table.

INDEX TERMS GNSS spoofing, Antenna, power, correlation coefficient, GLRT.

I. INTRODUCTION

Global navigation satellite systems (GNSS) provide users with position, velocity, and time (PVT) solutions. Many civilian and military applications are dependent on GNSS services, making the GNSS receiver a likely interference target [1]. However, GNSS signals are vulnerable to interference because their powers are weak on the earth's surface [2]. GNSS spoofing attack is a kind of structural interference which misleads victim receivers to generate false PVT solution, and it is one of the most vicious interferences because the spoofing signals imitate the authentic ones and are very difficult to be detected in a conventional receiver [3]–[5]. Since the GNSS based services are widely used, GNSS spoofing countermeasures need to be developed to guarantee secure and robust GNSS services.

Many GNSS spoofing countermeasures have been proposed to detect the spoofing signals or mitigate the effects of the spoofing attacks. Some methods require additional sensors such as multiple antennas, reference receivers, power monitoring units or inertial measurement units (IMU) to provide additional measurements. These methods are normally robust, but need changes to receivers and suffer from higher expenses [6]–[8]. The other methods are implemented in a conventional receiver with a single antenna, such as the cryptographic authentication techniques, moving receiver methods, signal quality monitoring techniques, code and carrier Doppler cross-check, and multi-modal detection method [9]–[15].

As commented in [16], anti-spoofing methods based on multiple antennas, multiple receivers and the moving receiver technique are categorized as spatial processing method, which is one of the most powerful spoofing countermeasures. It assumes that all the spoofing signals are transmitted from the same emitter, and the propagation paths of the spoofing signals are all the same. Hence, the measurements of the spoofing signals are more correlated than those of the authentic ones, and they result in the same positioning results in receivers which are located separately. The spatial processing method takes advantage of the spatial information to find the anomalies and distinguish the authentic/spoofing signals [17]–[20]. However, previous spatial processing method cannot be implemented in a static single-antenna receiver, which may limit its application.

In this paper, we propose a novel spatial processing method based on a single rotating antenna. Different from the previous spatial processing methods, the proposed method employs the anisotropy of the antenna gain pattern to discriminate the authentic/spoofing signals. It does not require multiple antennas or receivers, and can be implemented in a static receiver.

The rest of the paper is organized as follows. Section II proposes the rotating antenna based method and discusses its theoretical foundation and performance. Section III provides simulations to evaluate and validate the performance of the proposed method. Section IV provides experiments under simulated and meaconing GNSS spoofing attacks. In section V, a summary and conclusions are provided.

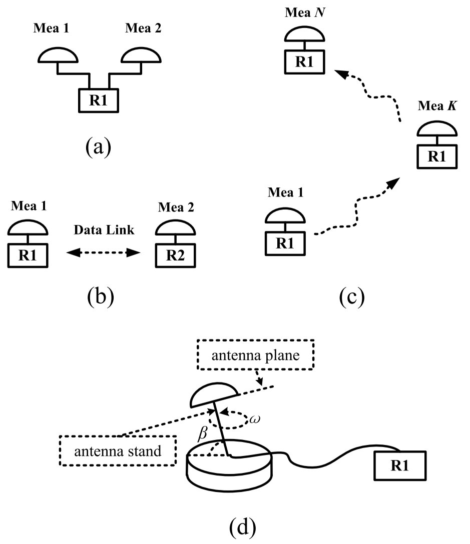


FIGURE 1. Different spatial processing techniques for GNSS spoofing detection. (a) represents the multiple antennas based technique [17], (b) represents the multiple receivers based technique [18]–[20], and (c) represents the moving receiver technique [11], [12]. All of them take advantage of the measurements at different positions to discriminate the authentic/spoofing signals. (d) represents rotating antenna based spoofing countermeasure. The antenna is fixed on a horizontal table which rotates at a constant angular velocity ω. The antenna plane is vertical to the antenna stand. The angle between the antenna stand and the horizontal plane is β.

II. ANTI-SPOOFING METHOD BASED ON SINGLE ROTATING ANTENNA

In this section, we describe the rotating antenna based anti-spoofing method.

A. PROBLEM FORMULATION

Current spatial processing methods detect GNSS spoofing attacks with measurements from more than one antennas or receivers at the same time interval [17]–[20], or measurements from one moving receiver at different time intervals [11], [12]. They all require measurements from antennas at different positions, as shown in Fig. 1 (a) ∼ (c).

In this paper, we propose a single rotating antenna based method that can discriminate the authentic/spoofing signals in a static receiver. It can also be categorized into the spatial processing method and its scheme is shown in Fig. 1 (d).

The elevation angle of the ith satellite is defined as the angle between the line of sight (LOS) of the ith satellite and the horizontal plane, which is denoted as el_i. The angle between the ith satellite's LOS and the antenna plane is denoted as θ_i. When the antenna plane is parallel to the horizontal plane, θ_i is equal to el_i. Otherwise, they are no longer equal. The user/satellite relative geometry and the above-mentioned angles are shown in Fig. 7 in the appendix. Even though θ_i and el_i are different when the antenna is rotating and $\beta \neq 90°$, they can be transformed to each other with additional spatial information. Assume that at epoch t, the azimuth angle difference between the antenna stand and the ith satellite is $\gamma_i(t)$. Then θ_i can be given by (1), which is derived in the appendix.

$$\theta_i = 90° - arccos[cos(\gamma_i(t))cos(el_i)cos(\beta) + sin(el_i)sin(\beta)], \tag{1}$$

where β has been introduced in Fig. 1 (d), and it is also called the antenna's slant angle in the paper. When the angular velocity ω is constant, $\gamma_i(t)$ can be expressed as follows:

$$\gamma_i(t) = \pi(t) - az_i = \pi(0) + \omega \cdot t - az_i, \tag{2}$$

where $\pi(t)$ is the azimuth angle of the antenna stand at epoch t and az_i is the azimuth angle of the ith satellite, which is assumed to be constant in a short period. It can be seen from (1) and (2) that θ_i is the function of t when ω, β , el_i, az_i, and $\pi(0)$ are determined. It changes periodically and its period is the same as the period of the rotation of the antenna.

The variations of the signals' powers during the rotation of the antenna are used to discriminate the authentic/spoofing signals. It is assumed that the spoofing signals come from the same emitter. Authentic signals come from different directions and their power variations are different from each other. However, the spoofing signals come from the same direction and their power variations caused by the antenna rotation are the same.

The most widely used GNSS antennas are fixed reception pattern antennas (FRPAs), which have nearly omnidirectional patterns in the upper hemisphere [21]. The L1 C/A gain pattern of a commercial GPS FRPA in the upper hemisphere is shown in Fig. 2. The antenna gain is much lower at low elevation angles to avoid potential deleterious effects such as multipath and interference [21]. In the rest of the paper, the gain pattern in Fig. 2 is applied to introduce the proposed spoofing countermeasure.

It should be noted that the elevation angle in Fig. 2 corresponds to θ_i in (1), which is different from the ith satellite's elevation angle el_i when the antenna plane is not parallel to the horizontal plane. Fig. 2 shows that the antenna gain is the function of θ_i.

θ_i changes when the antenna is rotating. Therefore, the antenna gain to a certain satellite also changes according to

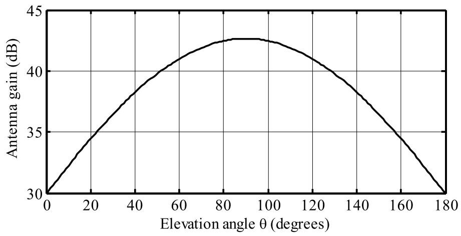


FIGURE 2. GPS L1 C/A antenna gain of a commercial receiver antenna.

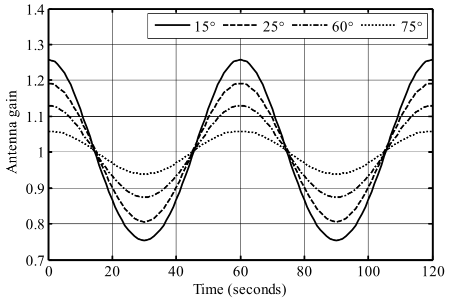


FIGURE 3. Relative antenna gains with respect to time for different el_i from 15° to 75°, $\beta = 85°$, $az_i = \pi(0)$, and $\omega = 6°/s$.

Fig. 2. In order to model the change of the power of the received signal, the relative rotating antenna gain is induced, which is defined as the ratio between the antenna gain during rotation and the mean value of the antenna gain. Denote G as the relative rotating antenna gain, it can be determined based on (1), (2) and Fig. 2, and the results are shown in Fig. 3. It shows that the changing patterns of G are different for different el_i and az_i. In practical applications, ω, β and $\pi(0)$ are all determined, and el_i and az_i are different for different satellites. However, they are all the same for the spoofing signals which come from the same source. Hence, the changing patterns of powers of the authentic signals are different, but those of the spoofing signals are the same. Therefore, the signal power measurements can be used to discriminate the authentic/spoofing signals.

The anti-spoofing procedure is implemented in two phases, namely the correlation phase and the parameter estimation phase. Firstly, spoofing signals can be discriminated by calculating the correlation coefficients of power measurements of pairwise signals. Correlation results which are close to 1 indicate that the signals come from the same source. However, it is hard to evaluate the performance of this metric and set a threshold for the spoofing detection theoretically. Therefore, we propose the second phase which detects the spoofing signals based on parameter estimation, whose test statistic and theoretical performance are derived with the theory of generalized likelihood ratio test (GLRT).

B. SPOOFING COUNTERMEASURE BASED ON PARAMETER ESTIMATION

As can be seen in Fig. 3, G is periodical and similar to a cosine function when el_i and az_i are determined. Therefore, we fit the ith satellite's relative rotating antenna gain G_i with the following equation:

$$\begin{aligned} G_i &= F[t|\omega, \beta, el_i, az_i, \pi(0)] \\ &\approx 1 + A_i cos(\omega t + \phi_i)|_{\beta_i, el_i, az_i, \pi(0)}, \end{aligned} \tag{3}$$

Assume that the coherent time T_{coh} is much shorter than the rotating period of antenna. The in-phase and quadrature coherent integration results of the ith satellite can be expressed as [1]:

$$\begin{aligned} I_i(n) &= a_i\sqrt{1 + A_i cos(\omega t + \phi_i)} d_i(n) \\ &\quad \times sinc(f_{ei}T_{coh})R(\tau_i)cos\phi_{ei} + w_{Ii} \\ Q_i(n) &= a_i\sqrt{1 + A_i cos(\omega t + \phi_i)} d_i(n) \\ &\quad \times sinc(f_{ei}T_{coh})R(\tau_i)sin\phi_{ei} + w_{Qi} \end{aligned} \tag{4}$$

where a_i represents the direct component of the signal's amplitude, $d_i(n)$ represents the navigation message, f_{ei} and ϕ_{ei} are the frequency and carrier phase tracking errors, $R(\tau_i)$ represents the autocorrelation function of the pseudorange code, τ_i is the time difference between the prompt local code and the received signal, and w_{Ii} and w_{Qi} are zero-mean additive white Gaussian noises (AWGN).

Then, the signal-plus-noise power in $1/T_{coh}$ noise bandwidth is given by:

$$P_i = \sum_{n=1}^{N_{nc}} [I_i^2(n) + Q_i^2(n)] \tag{5}$$

where N_{nc} is the non-coherent integration times. P_i is distributed according to a noncentral χ^2 distribution with noncentral parameter λ_i and $2N_{nc}$ degrees of freedom. λ_i is given by [22]:

$$\lambda_i = 2(C_i/N_0)T_{coh} \cdot [1 + A_i cos(\omega t + \phi_i)] \cdot N_{nc} \tag{6}$$

where C_i/N_0 is the carrier to noise ratio of the ith satellite in Hz. The mean value and variance of P_i are given by [23]:

$$\begin{aligned} \mu_i &= 2N_{nc} + \lambda_i \\ \sigma_i^2 &= 4N_{nc} + 4\lambda_i \end{aligned} \tag{7}$$

σ_i^2 changes with time, thus it's hard to analyze P_i. However, when the slant angle β of antenna is close to 90°, A_i is much smaller than 1. Therefore $\sigma_i^2 \approx 4N_{nc} + 8(C_i/N_0)T_{coh}N_{nc}$ and it can be assumed constant in the rotation.

In the sequel, the subscript i is omitted for simplification. According to the central limit theorem, when $N_{nc} \gg 1$, P is approximately distributed according to the Gaussian distribution $P \sim \mathcal{N}(\mu, \sigma^2)$. Therefore, P can be rewritten as:

$$\begin{aligned} P &= 2N_{nc} + \lambda_i + w_P \\ &= 2N_{nc} + 2(C/N_0)T_{coh}N_{nc} \\ &\quad + 2(C/N_0)T_{coh}N_{nc}Acos(\omega t + \phi) + w_P \end{aligned} \tag{8}$$

where w_P is zero-mean AWGN with variance σ^2. P can be rewritten as the following simplified form:

$$\begin{aligned} P &= u + gcos(\omega t + \phi) + w_P \\ &= s(t; u, g, \phi) + w_P \qquad (9) \end{aligned}$$

where $u = 2N_{nc} + 2(C/N_0)T_{coh}N_{nc}$ and $g = 2(C/N_0)T_{coh}N_{nc}A$. The power measurements are denoted as $\boldsymbol{x} = [P(0), P(T_0), P(2T_0), \cdots, P((N-1)T_0)]^T$, where T_0 is the sampling interval of the power measurements. The maximum likelihood estimation (MLE) of $\boldsymbol{\theta} = [u, g, \phi]$ can be calculated by minimizing the following cost function:

$$\begin{aligned} J(\boldsymbol{\theta}) &= \sum_{n=0}^{N-1}[P(nT_0) - u - gcos(\omega nT_0 + \phi)]^2 \\ &= \sum_{n=0}^{N-1}[P(nT_0) - u - gcos(\phi)cos(\omega nT_0) \\ &\qquad + gsin(\phi)sin(\omega nT_0)]^2 \qquad (10) \end{aligned}$$

Then, the following equations are provided to further simplify (10):

$$\boldsymbol{\alpha} = \begin{bmatrix} u & \alpha_1 & \alpha_2 \end{bmatrix}^T = \begin{bmatrix} u & gcos(\phi) & -gsin(\phi) \end{bmatrix}^T \qquad (11)$$

$$\begin{aligned} \boldsymbol{H} &= \begin{bmatrix} \boldsymbol{e} & \boldsymbol{h}_1 & \boldsymbol{h}_2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 \\ 1 & cos(\omega T_0) & sin(\omega T_0) \\ 1 & cos(2\omega T_0) & sin(2\omega T_0) \\ \vdots & \vdots & \vdots \\ 1 & cos((N-1)\omega T_0) & sin((N-1)\omega T_0 \end{bmatrix} \qquad (12) \end{aligned}$$

Then, the cost function in (10) can be rewritten as the following compact form:

$$J(\boldsymbol{\theta}) = (\boldsymbol{x} - \boldsymbol{H\alpha})^T(\boldsymbol{x} - \boldsymbol{H\alpha}) \qquad (13)$$

Consequently, the ML estimate of $\boldsymbol{\alpha}$ is given by [24]:

$$\hat{\boldsymbol{\alpha}} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{x} \qquad (14)$$

Considering the characteristic of $\boldsymbol{h}_1$ and $\boldsymbol{h}_2$, the matrix $\boldsymbol{H}^T\boldsymbol{H}$ can be simplified as follows [24]:

$$\boldsymbol{H}^T\boldsymbol{H} = \begin{bmatrix} \boldsymbol{e}^T\boldsymbol{e} & \boldsymbol{e}^T\boldsymbol{h}_1 & \boldsymbol{e}^T\boldsymbol{h}_2 \\ \boldsymbol{h}_1^T\boldsymbol{e} & \boldsymbol{h}_1^T\boldsymbol{h}_1 & \boldsymbol{h}_1^T\boldsymbol{h}_2 \\ \boldsymbol{h}_2^T\boldsymbol{e} & \boldsymbol{h}_2^T\boldsymbol{h}_1 & \boldsymbol{h}_2^T\boldsymbol{h}_2 \end{bmatrix} \approx \begin{bmatrix} N & 0 & 0 \\ 0 & \frac{N}{2} & 0 \\ 0 & 0 & \frac{N}{2} \end{bmatrix} \qquad (15)$$

Substitute (15) back into (14), the ML estimate of $\boldsymbol{\alpha}$ can be written as follows:

$$\hat{\boldsymbol{\alpha}} = \begin{bmatrix} \hat{u} \\ \hat{\alpha}_1 \\ \hat{\alpha}_2 \end{bmatrix} \approx \frac{2}{N}\begin{bmatrix} \frac{1}{2}\boldsymbol{e}^T\boldsymbol{x} \\ \boldsymbol{h}_1^T\boldsymbol{x} \\ \boldsymbol{h}_2^T\boldsymbol{x} \end{bmatrix} \qquad (16)$$

Then, the ML estimate of ϕ is given by:

$$\begin{aligned} \hat{\phi} &= arctan\frac{-\hat{\alpha}_2}{\hat{\alpha}_1} \\ &= arctan\frac{-\sum_{n=0}^{N-1} P(nT_0)sin(n\omega T_0)}{\sum_{n=0}^{N-1} P(nT_0)cos(n\omega T_0)} \qquad (17) \end{aligned}$$

Denote $\rho = n\omega T_0 + \phi$, the elements of Fisher information matrix can be expressed as [24]:

$$\begin{aligned} [\boldsymbol{I}(\boldsymbol{\theta})]_{uu} &= \frac{1}{\sigma^2}\sum_{n=0}^{N-1}[\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial u}]^2 = \frac{1}{\sigma^2}\sum_{n=0}^{N-1}1 = \frac{N}{\sigma^2} \\ [\boldsymbol{I}(\boldsymbol{\theta})]_{ug} &= [\boldsymbol{I}(\boldsymbol{\theta})]_{gu} = \frac{1}{\sigma^2}\sum_{n=0}^{N-1}\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial u}\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial g} \\ &= \frac{1}{\sigma^2}\sum_{n=0}^{N-1}cos(\rho) \approx 0 \\ [\boldsymbol{I}(\boldsymbol{\theta})]_{u\phi} &= [\boldsymbol{I}(\boldsymbol{\theta})]_{\phi u} = \frac{1}{\sigma^2}\sum_{n=0}^{N-1}\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial u}\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial \phi} \\ &= -\frac{1}{\sigma^2}\sum_{n=0}^{N-1}gsin(\rho) \approx 0 \\ [\boldsymbol{I}(\boldsymbol{\theta})]_{gg} &= \frac{1}{\sigma^2}\sum_{n=0}^{N-1}[\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial g}]^2 = \frac{1}{\sigma^2}\sum_{n=0}^{N-1}cos^2(\rho) \\ &= \frac{1}{\sigma^2}\sum_{n=0}^{N-1}[\frac{1}{2} + \frac{1}{2}cos(2\rho)] \approx \frac{N}{2\sigma^2} \\ [\boldsymbol{I}(\boldsymbol{\theta})]_{g\phi} &= [\boldsymbol{I}(\boldsymbol{\theta})]_{\phi g} = \frac{1}{\sigma^2}\sum_{n=0}^{N-1}\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial g}\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial \phi} \\ &= -\frac{1}{\sigma^2}\sum_{n=0}^{N-1}gcos(\rho)sin(\rho) \\ &= -\frac{g}{2\sigma^2}\sum_{n=0}^{N-1}sin(2\rho) \approx 0 \\ [\boldsymbol{I}(\boldsymbol{\theta})]_{\phi\phi} &= \frac{1}{\sigma^2}\sum_{n=0}^{N-1}[\frac{\partial s(nT_0;\boldsymbol{\theta})}{\partial \phi}]^2 = \frac{1}{\sigma^2}\sum_{n=0}^{N-1}g^2sin^2(\rho) \\ &= \frac{g^2}{\sigma^2}\sum_{n=0}^{N-1}[\frac{1}{2} - \frac{1}{2}cos(2\rho)] \approx \frac{Ng^2}{2\sigma^2} \qquad (18) \end{aligned}$$

Consequently, the Fisher information matrix is given by:

$$\boldsymbol{I}(\boldsymbol{\theta}) = \frac{1}{\sigma^2}\begin{bmatrix} N & 0 & 0 \\ 0 & N/2 & 0 \\ 0 & 0 & Ng^2/2 \end{bmatrix} \qquad (19)$$

According to the asymptotic characteristic of MLE, $\hat{\phi} \overset{a}{\sim} \mathcal{N}(\phi, \sigma_\phi^2)$, where σ_ϕ^2 is given by [24]:

$$\sigma_\phi^2 = \frac{2\sigma^2}{Ng^2} = \frac{2 + 4(C/N_0)T_{coh}}{NN_{nc}(C/N_0)^2T_{coh}^2A^2} \qquad (20)$$

When two signals are considered, two estimates of ϕ can be obtained and they are distributed according to $\hat{\phi}_i \overset{a}{\sim} \mathcal{N}(\phi_i, \sigma^2_{\phi i})$ and $\hat{\phi}_j \overset{a}{\sim} \mathcal{N}(\phi_j, \sigma^2_{\phi j})$, respectively. Based on the estimates of phase parameters, the following metric is proposed:

$$\Delta\hat{\phi}_{ij} = \hat{\phi}_i - \hat{\phi}_j \tag{21}$$

Since the signals are processed in different tracking channels, $\hat{\phi}_i$ and $\hat{\phi}_j$ can be viewed as independent. Hence, $\Delta\hat{\phi}_{ij} \sim \mathcal{N}(\Delta\phi_{ij}, \sigma^2_{\phi_{ij}})$, where $\Delta\phi_{ij} = \phi_i - \phi_j$ and $\sigma^2_{\phi_{ij}} = \sigma^2_{\phi i} + \sigma^2_{\phi j}$. If the ith and jth signals are spoofing signals coming from a common emitter, $\Delta\phi_{ij}$ will be zero. If there is no spoofing attack, the signals are very likely to come from different directions, and $\Delta\phi_{ij}$ will be non-zero. Based on the above analysis, the following hypothesis test can be given:

$$\begin{aligned} \mathcal{H}_0 &: x = \omega \\ \mathcal{H}_1 &: x = \Delta\phi_{ij} + \omega \end{aligned} \tag{22}$$

where $\omega \sim \mathcal{N}(0, \sigma^2_{\phi_{ij}})$. Under $\mathcal{H}_0$, the phases of power measurements of the pairwise signals are the same and the signals are judged as spoofing ones. Under $\mathcal{H}_1$, the phases of power measurements are different, indicating that the signals come from different sources, thus the signals are judged as authentic ones. With GLRT, it is easy to know that when $|x| > \gamma'$, $\mathcal{H}_1$ is decided. The threshold γ' and the detection probability of the authentic signals P_d are given by [25]:

$$\gamma' = Q^{-1}(\frac{P_{fa}}{2})\sigma_{\phi_{ij}} \tag{23}$$

$$P_d = Q\Big(\frac{\gamma' - \Delta\phi_{ij}}{\sigma_{\phi_{ij}}}\Big) + Q\Big(\frac{\gamma' + \Delta\phi_{ij}}{\sigma_{\phi_{ij}}}\Big) \tag{24}$$

where $Q(\cdot)$ is the tail probability of the standard normal distribution and the false alarm probability P_{fa} denotes the probability of a detection of authentic signals when the signals are spoofing ones.

C. OVERALL SPOOFING COUNTERMEASURE

Based on the analyses in subsection II-A and II-B, the detailed steps of the spoofing countermeasure are concluded as follows:

Phase I: Correlation

1) Record the power measurements of the ith and jth satellite, denoted as $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$, respectively.
2) Calculate the correlation coefficients between $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$. Results close to 1 indicate that the pairwise signals come from the same direction. Then, both the signals should be categorized as spoofing ones.

Phase II: Parameter Estimation

1) Estimate the phase $\hat{\phi}_i$ and $\hat{\phi}_j$ of the ith and jth satellites' power measurements with (17).
2) Calculate $\sigma^2_{\phi i}$ and $\sigma^2_{\phi j}$ with (20). $(C/N_0)_i$ and $(C/N_0)_j$ can be obtained from the tracking loops. Consider (20) and (23), it is easy to see that smaller A leads to larger γ', which reduces P_{fa}. Therefore, even though it's hard to know the exact value of A, a small A can be used here to determine the variance.
3) Calculate $\sigma^2_{\phi_{ij}}$ and set a P_{fa}. Then, the threshold γ' can be determined with (23).
4) Calculate $\Delta\phi_{ij}$. If $|\Delta\phi_{ij}|$ is larger than γ', the pairwise signals are authentic signals. Otherwise, both of the signals should be suspected.

It should be noted that the two phases mentioned above can work independently. In section III, We only simulate the second phase since it is not easy to evaluate the performance of the first phase. But in the practical experiments in section IV, both the two phases are performed.

D. COUNTERMEASURE FOR THE SIGNAL POWER MANIPULATION OF SPOOFER

Note that when the power fluctuations induced by the manipulation of a spoofer are larger than those induced by the rotating antenna, the anti-spoofing method may fail. In order to detect such kind of spoofing attacks, we can let the antenna be static and rotate alternatively. Since the system is implemented in a static or low-dynamic receiver, the power measurements should be relatively constant in a short period of time. Hence, the spoofing attack can be detected by monitoring excessive changes of power measurements when the antenna is static. On the other hand, when the transmitting powers of spoofing signals are constant or change gradually, the spoofing attack can be detected with the method in subsection II-C when the antenna rotates.

The central tenet of the method is that the user can adjust the attitude of the antenna and know well about the variations of its gain pattern, but a spoofer can never forecast when and how the user changes the antenna's attitude.

III. PERFORMANCE EVALUATION

In this section, simulations are performed to evaluate the performance of the proposed method. Signals are generated with a Matlab based GPS L1 C/A signal generator and they are sampled at a rate of 5 MHz. The coherent time T_{coh} is 1 ms. The angular velocity of the antenna is $6°/s$. The data length is 60 seconds and the power measurements are recorded every second, thus N is 60. The relative gain pattern follows (3). Four groups of Monte Carlo simulations are performed to investigate the influence factors of the performance. The receiver operating characteristic (ROC) curve is employed to illustrate the performance, which are shown in Fig. 4. The circles ('S') represent the simulation results and the dashed lines ('T') represent the theoretical results obtained with (23) and (24).

The first group of simulations investigates the influence of the phase difference ($\Delta\phi$) between the power measurements. C/N_0 of both the signals are 40 dBHz, N_{nc} is 10, and A is 0.2. $\Delta\phi$ are set to 10, 15, 20, and 25 degrees, respectively. Corresponding ROC curves are shown in Fig. 4 (a). It shows that larger $\Delta\phi$ leads to better performance.

The second group of simulations investigates the influence of the C/N_0. $\Delta\phi$ is 10 degrees, N_{nc} is 10, and A is 0.2.

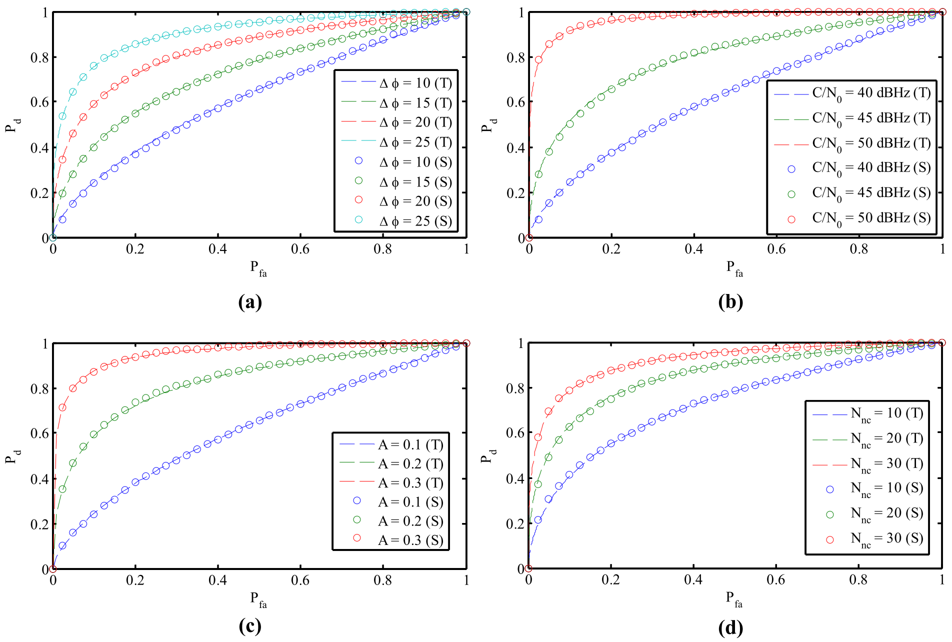


FIGURE 4. Comparisons of ROC curves obtained with different parameters. The circles ('S') represent the simulation results and the dashed lines ('T') represent the theoretical results. In (a), $C/N_0 = 40$ dBHz, $N_{nc} = 10$, $A = 0.2$, and $\Delta\phi$ are set to 10, 15, 20, and 25 degrees. In (b), $N_{nc} = 10$, $A = 0.2$, $\Delta\phi = 10$ degrees, and C/N_0 are set to 40, 45, 50 dBHz. In (c), $C/N_0 = 40$ dBHz, $N_{nc} = 10$, $\Delta\phi = 20$ degrees, and A are set to 0.1, 0.2, and 0.3. In (d), $C/N_0 = 40$ dBHz, $A = 0.2$, $\Delta\phi = 15$ degrees, and N_{nc} are set to 10, 20, and 30.

It is assumed that the C/N_0 of the signals are equal and set to 40, 45, and 50 dBHz, respectively. Corresponding ROC curves are shown in Fig. 4 (b). It shows that higher C/N_0 leads to better performance.

The third group of simulations investigates the influence of A. $\Delta\phi$ is 20 degrees, N_{nc} is 10, and C/N_0 of both the signals are 40 dBHz. A are set to 0.1, 0.2, and 0.3, respectively. Corresponding ROC curves are shown in Fig. 4 (c). It shows that larger A leads to better performance. In addition, it can be concluded from Fig. 3 that when the elevation angle is lower, A is larger. Therefore, the anti-spoofing performance is better when the spoofing signals come from low elevation angles.

The fourth group of simulations investigates the influence of N_{nc}. $\Delta\phi$ is 15 degrees, A is 0.2, and C/N_0 of both the signals are 40 dBHz. N_{nc} are set to 10, 20, and 30, respectively. Corresponding ROC curves are shown in Fig. 4 (d). It shows that larger N_{nc} leads to better performance.

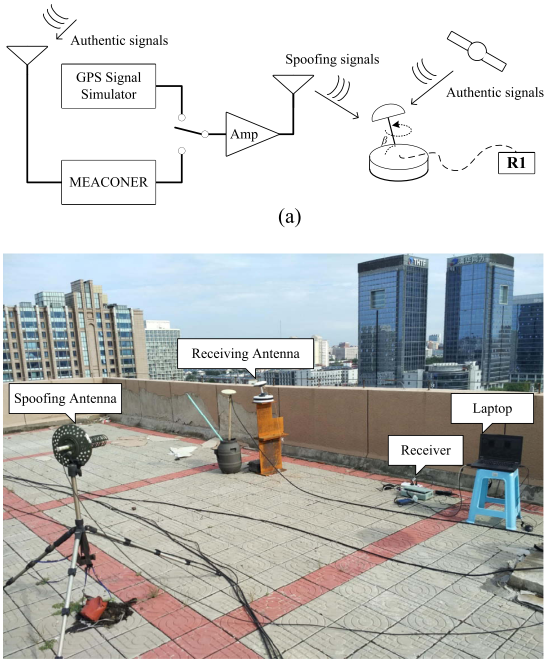
Figure 4 shows that the simulated and theoretical ROC curves are very close for different parameters, which validates the analyses in section II. In practical applications, the threshold can be calculated according to (20), (23), and (24) to guarantee expected P_{fa} and P_d.

IV. EXPERIMENTS AND DISCUSSIONS

In this section, experiments of real GPS spoofing attacks are performed in a real-time receiver to validate the proposed spoofing countermeasure. The configuration and the deployment of the experiments are shown in Fig. 5. Three scenarios are considered. In scenario 1 (S1), the switch is not connected, and the receiver will only receive authentic signals. In scenario 2 (S2), the switch is connected to a GPS simulator, and simulated spoofing signals will be sent to the receiver. The simulated spoofing signals are generated with a GPS L1 C/A simulator. In scenario 3 (S3), the switch is connected to a meaconer, and meaconing spoofing signals will be sent to the receiver. The meaconing signals are rebroadcasted radio navigation signals. The gain pattern of the receiving antenna has been given in Fig. 2. The angular velocity of the rotary table is $\omega = 6°/s$. The slant angle of the antenna is $\beta = 85°$. The received signals are sampled at a rate of 62 MHz. The coherent integration time T_{coh} is 1ms and N_{nc} is 100. The total processing time is 300 seconds and the power measurements are recorded every second, thus N is 300 in the experiment.

A conventional receiver which only tracks the highest accumulated result in the acquisition is used. Hence, when the power of a spoofing signal is higher than that of the corresponding authentic one, the receiver will only track the spoofing signal.

Power measurements are shown in Fig. 6. They are normalized with the mean values for clarity of illustration. It can be seen that the power measurements of the signals change periodically. There are 5 periods in 300 seconds for each signal, which is consistent with the $6°/s$ angular velocity. Figure 6 (a) shows that the changing patterns of power measurements of authentic signals are different. However, the power measurements of the simulated spoofing signals are almost the



(b)

FIGURE 5. (a) The configuration of the experiment. In S1, the switch is not connected. In S2, the switch is connected to the GPS simulator. In S3, the switch is connected to the meaconer. (b) The deployment of the experiment at the roof of Weiqing Building.

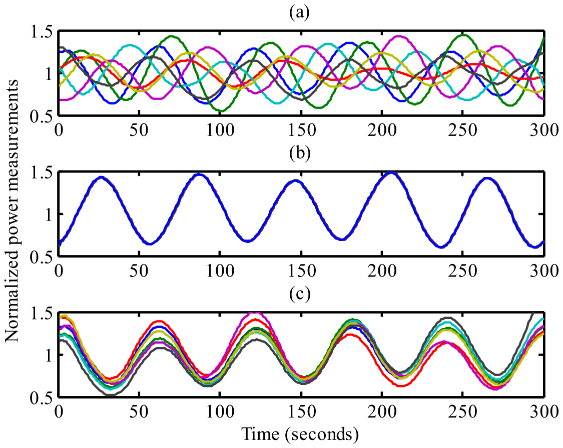


FIGURE 6. Normalized power measurements in different scenarios. (a) In scenario 1, authentic signals are processed. (b) In scenario 2, simulated signals are processed. (c) In scenario 3, meaconing signals are processed.

same after normalization and they are overlapped as shown in Fig. 6 (b). Similarly, the normalized power measurements of the meaconing signals in Fig. 6 (c) are also very similar. Figure 6 (b) and (c) indicate that the corresponding received signals are spoofing ones.

The power measurements of the first signal in each scenario are chosen as the reference data, and the correlation coefficients between the power measurements of the other signals and the reference data are calculated. Table 1 shows the correlation coefficient results. When the antenna is rotating, the power measurements of the authentic signals (S1) are uncorrelated since the signals come from different directions. However, the correlation coefficients are all close to 1 for the simulated (S2) and meaconing (S3) signals. In addition, the correlation coefficients of the simulated signals are higher than those of the meaconing ones, because the simulated signals are generated by a GPS simulator and their powers are constant and stable. However, the meaconing signals come from different satellites and their powers change differently due to the meaconer/satellites relative motions. Nevertheless, these changes are much smaller than the changes caused by the rotation of antenna. Hence, the correlation coefficients are still very high in S3.

TABLE 1. Correlation coefficients between the power measurements of the first signal and the other signals in different scenarios.

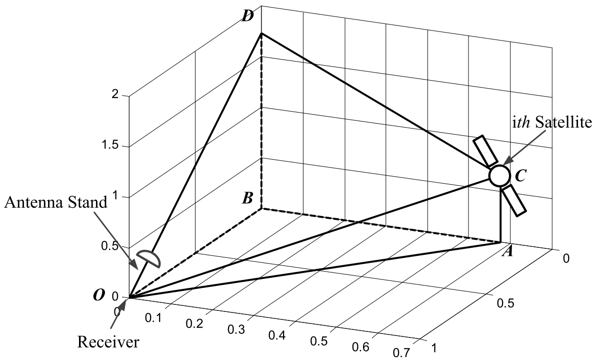
	S1	S2	S3
r_{12}	0.575	0.999	0.963
r_{13}	-0.158	1.000	0.935
r_{14}	-0.163	0.999	0.932
r_{15}	-0.899	1.000	0.905
r_{16}	-0.433	0.999	0.986
r_{17}	-0.856	1.000	0.949

Table 2 shows the phase differences of power measurements between pairwise signals. The phase parameters of different signals in S1 are quite different from each other, therefore, $\Delta\phi$ is not close to zero. However, $\Delta\phi$ in S2 and S3 are very close to zero because all the processed signals come from the same emitter. $|\Delta\phi|$ should be compared with the threshold γ' to determine whether the signals are authentic or not. As shown in (20) and (23), A is required to calculate γ'. Even though A cannot be obtained directly, a small A can be chosen to calculate γ' to reduce the P_{fa}. Here, A, P_{fa} and C/N_0 are set to 0.1, 0.001 and 45 dBHz, respectively, and γ' can be calculated as 5.5 degrees. Table 2 shows that all the $|\Delta\phi|$ in S1 are larger than γ', but the $|\Delta\phi|$ in S2 and S3 are smaller than γ', which validates that the proposed method can distinguish the authentic signals from the spoofing ones.

TABLE 2. $\Delta\phi$ (degrees) between the power measurements of the first signal and the other signals in different scenarios.

	S1	S2	S3
$\Delta\phi_{12}$	-45.6	2.20	-1.45
$\Delta\phi_{13}$	-41.8	-0.16	1.73
$\Delta\phi_{14}$	-230.0	2.19	-0.47
$\Delta\phi_{15}$	-77.0	-0.25	-0.09
$\Delta\phi_{16}$	-35.8	1.99	-1.32
$\Delta\phi_{17}$	10.9	-0.01	-0.18

It should be noted that the proposed method sacrifices the tracking sensitivity of the receiver. When the antenna's slant angle β is smaller, the tracking sensitivity is lower. However, smaller β leads to larger antenna gain variation, which can help resist the disturbance of the signals' original power fluctuations, improving the anti-spoofing performance. Therefore, a trade-off needs to be made between the tracking and anti-spoofing performance. In addition, since the antenna phase center is not static, the approach is not suitable for high precision navigation.



$el_i = \angle AOC$, $\beta = \angle BOD$, $\gamma_i(t) = \angle AOB$, $\theta_i(t) = 90° - \angle COD$

FIGURE 7. User/satellite relative geometry. The phase center of the antenna can be viewed as located at *O* because the length of the antenna stand is much shorter than the distance between the satellite and the receiver. *OBA* is the horizontal plane. *OC* is the line of sight between the satellite and the receiver, and the satellite is located on the extension cord of *OC*. The antenna stand is along *OD*. *BO*, *BA*, and *BD* are orthogonal to each other. *B* is the origin of the coordinate. *BO*, *BA*, and *BD* are set as the x, y, and z axes, respectively. Then, the rectangular coordinate system is built.

V. CONCLUSIONS

In this paper, we establish the theoretical foundation for the rotating antenna based GNSS spoofing countermeasure. The countermeasure consists of two phases. In the first phase, correlation coefficients between the power measurements of different signals are calculated. Correlation coefficient close to 1 indicates that the pairwise signals are spoofing ones. Different from the moving receiver based anti-spoofing technique which also calculates the correlation coefficient between measurements of pairwise signals, the proposed method in the paper is based on the anisotropy of the antenna's gain pattern. In the second phase, phase difference of the power measurements of pairwise signals are estimated and compared with a threshold to determine whether the signals are authentic ones or not, and the theoretical performance is analysed based on GLRT and validated by simulations. Experiments of actual GPS spoofing attacks are also performed in a practical real-time receiver to test the proposed method. Compared with the moving receiver based method, the proposed method can be implemented in a static receiver. Compared with the multi-antenna based method, the proposed method only requires one antenna. Consequently, the rotating antenna based GNSS spoofing countermeasure is a good supplementation to the spatial processing GNSS anti-spoofing method.

APPENDIX

The geometry relationship between the satellite and the slant antenna is shown in Fig. 7. *OBA* is the horizontal plane. The elevation angle of the ith satellite is $\angle AOC$, which is equal to el_i in (1). The slant angle of the antenna is $\angle BOD$, which is equal to β in (1). The difference between the azimuth angle of the antenna and the ith satellite is $\angle AOB$, which is equal to $\gamma_i(t)$ in (1). In the sequel, these angles are denoted as α, β and γ, respectively. The angle between the ith satellite's LOS (OC) and the antenna plane is denoted as θ_i. $\angle COD$ is the complementary angle of $\theta_i(t)$.

A rectangular coordinate system is built as shown in Fig. 7, it is assumed that the length of BO is 1 and B is set as the origin, then the coordinates of the points in the figure can be given as: $B(0, 0, 0)$, $O(1, 0, 0)$, $A(0, tan(\gamma), 0)$, $D(0, 0, tan(\beta))$, and $C(0, tan(\gamma), tan(\alpha)/cos(\gamma))$. Then $\boldsymbol{OD}$ and $\boldsymbol{OC}$ can be expressed as $\boldsymbol{OD} = (-1, 0, tan(\beta))$, $\boldsymbol{OC} = (-1, tan(\gamma), tan(\alpha)/cos(\gamma))$. Therefore, θ_i can be given by:

$$\begin{aligned}\theta_i(t) &= 90° - \angle COD \\ &= 90° - arccos[\boldsymbol{OC} \cdot \boldsymbol{OD} / |\boldsymbol{OC}| \cdot |\boldsymbol{OD}|] \\ &= 90° - arccos[cos(\gamma)cos(\alpha)cos(\beta) + sin(\alpha)sin(\beta)] \\ &= 90° - arccos[cos(\gamma_i(t))cos(el_i)cos(\beta) \\ &\qquad + sin(el_i)sin(\beta)] \end{aligned} \tag{25}$$

REFERENCES

[1] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications*. Dedham, MA, USA: Artech House, 1996.

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

[3] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Secur. J.*, vol. 25, no. 2, pp. 19–27, 2003.

[4] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," *GPS Solutions*, vol. 19, no. 3, pp. 475–487, Jul. 2015.

[5] T. E. Humphreys, B. M. Ledvina, M. L. Psiak, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. ION GNSS 21st. Int. Techn. Meeting Satellite Division*, Savannah, GA, USA, Sep. 2008, pp. 2314–2325.

[6] 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. Inst. Navigat. Int. Tech. Meeting*, Anaheim, CA, USA, 2009, pp. 124–130.

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

[8] P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals, and R. J. Hartnett, "GNSS spoof detection using shipboard IMU measurements," in *Proc. ION GNSS 27th Int. Tech. Meeting Satellite Division*, Tampa, FL, USA, 2014, pp. 745–758.

[9] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proc. ION GNSS 16st. Int. Tech. Meeting Satellite Division*, 2003, pp. 1543–1552.

[10] 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. (PLANS)*, May 2014, pp. 262–269.

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

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

[13] R. E. Phelts, "Multicorrelator techniques for robust mitigation of threats to GPS signal quality," Ph.D. dissertation, Dept. Mech. Eng., Stanford Univ., Stanford, CA, USA, 2001.

[14] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," in *Proc. 5th ESA Workshop Satellite Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2010, pp. 1–6.

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

[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] S. Daneshmand, A. Jafarnia, A. Broumandan, and G. Lachapelle, "Low-complexity spoofing mitigation," *GPS World Mag.*, vol. 22, pp. 44–46, Dec. 2011.

[18] P. F. Swaszek, R. J. Hartnett, M. V. Kempe, and G. W. Johnson, "Analysis of a simple, multi-receiver GPS spoof detector," in *Proc. ION ITM*, San Diego, CA, USA, Jan. 2013, pp. 884–892.

[19] P. F. Swaszek and R. J. Hartnett, "A multiple COTS receiver GNSS spoof detector—Extensions," in *Proc. ION ITM*, San Diego, CA, USA, Jan. 2014, pp. 316–326.

[20] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1794–1805, Aug. 2015.

[21] B. R. Rao, W. Kunysz, R. Fante, and K. McDonald, *GPS/GNSS Antennas*. Norwood, MA, USA: Artech House, 2013.

[22] D. Borio and D. Akos, "Noncoherent integrations for GNSS detection: Analysis and comparisons," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 45, no. 1, pp. 360–375, Jan. 2009.

[23] M. K. Simon, *Probability Distributions Involving Gaussian Random Variables: A Handbook for Engineers and Scientists*. New York, NY, USA: Springer, 2007.

[24] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*, vol. 1. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[25] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

FEI WANG was born in 1989. He received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 2011, where he is currently pursuing the Ph.D. degree with the Department of Electronic Engineering. His current interests include security of GNSS and ionospheric modeling.

HONG LI was born in 1981. He received the B.S. degree (Hons.) from Sichuan University, Chengdu, China, in 2004, and the Ph.D. degree (Hons.) from Tsinghua University, Beijing, China, in 2009. He joined the Department of Electronic Engineering, Tsinghua University, where he is currently an Associate Professor. He leads the research of GNSS security with the GNSS Laboratory of the Department, including evaluation of GNSS vulnerabilities, spoofing and anti-spoofing techniques, and the associated signal processing techniques. He has authored and co-authored over 50 papers and holds 14 patents with five pending applications. He was a recipient of the Academic Young Talent of Tsinghua University for Young Faculties in 2016, the Innovation Foundation for Young Talents of the National Remote Sensing Center of China in 2016, several excellent paper awards for Young Scholars of China Satellite Navigation Conference in 2010, 2012, 2013, and 2015, the Leadership Scholarship Program of Committee of 100 in 2009, the Outstanding Ph.D. Graduate Award of Tsinghua University in 2009, and the Excellent Doctoral Dissertation Award of Tsinghua University in 2009.

MINGQUAN LU was born in 1965. He received the M.S. degree in electronic engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 1993. He joined the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2003, where he is currently a Professor and the Director of the Institute of Information System. His research interests include signal processing, simulation of satellite navigation system, local area navigation system, and software-defined receivers.