Received 17 May 2024, accepted 27 May 2024, date of publication 3 June 2024, date of current version 12 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3408836

RESEARCH ARTICLE

Generalized Likelihood Ratio Satellite Navigation Spoofing Detection Algorithm Based on Moving Variance

PINGPING QU[1,2], **TIANFENG LIU**[1], **TENGLI YU**[3], **ERSHEN WANG**[1,2], **SONG XU**[1], **AND ZIBO YUAN**[1]

[1]School of Electronic and Information Engineering, Shenyang Aerospace University, Shenyang 110136, China
[2]State Key Laboratory of Dynamic Measurement Technology, North University of China, Taiyuan 038507, China
[3]School of Aerospace Engineering, Shenyang Aerospace University, Shenyang 110136, China

Corresponding author: Pingping Qu (qupingping_79@sau.edu.cn)

This work was supported in part by the Open Fund of State Key Laboratory of Dynamic Measurement Technology, North University of China under Grant 2023-SYSJJ-04; in part by the National Natural Science Foundation of China under Grant 62173237; in part by the Songshan Laboratory Foundation under Grant YYJC062022017; in part by the Open Fund of State Key Laboratory of Satellite Navigation System and Equipment Technology under Grant CEPNT2022B04 and Grant CEPNT2022A01; in part by the Applied Basic Research Programs of Liaoning Province under Grant 2022020502JH2/1013; in part by the Open Fund of Key Laboratory of Flight Techniques and Flight Safety CAAC under Grant FZ2020KF09 and Grant FZ2021ZZ06; and in part by the Special Funds Program of Shenyang Science and Technology under Grant 22-322-3-34.

ABSTRACT The vulnerability of Global Navigation Satellite Systems (GNSS) to spoofing limits their widespread use in military security and national economy. Therefore, fast and accurate detection of GNSS spoofing is of great significance. When spoofing cannot be accurately detected in the capture tracking phase, spoofing detection needs to be performed again at the localization solver. In order to detect the spoofing jamming of Global Navigation Satellite System in pseudo-range measurements, a generalized likelihood ratio satellite navigation spoofing detection algorithm based on moving variance is proposed by analyzing the pseudo-ranges cleared by the positioning of global satellite navigation signals. A new data subset is created by calculating the variance of the pseudo-range of different satellites at the same time and moving it forward. The variance is calculated again by this data subset to obtain the moving variance, the generalized likelihood ratio detection model is used to calculate the detection statistics of the pseudo-range movement variance, the detection statistic is then compared to the detection threshold under the condition that the probability of false alarm is 1×10^{-7}, so as to realize the spoofing jamming detection of global satellite navigation receiver for pseudo-range. Taking the software receiver as the experimental platform, the effectiveness of the proposed algorithm is verified by comparing it with two other algorithms. The result show that when the number of spoofed satellites is less than 9, the algorithm has a good detection effect. When the false alarm rate is 1×10^{-7}, the average prediction accuracy rate is kept above 98 %.

INDEX TERMS Satellite navigation, moving variance, generalized likelihood ratio test, spoofing detection, pseudo-range.

I. INTRODUCTION

At present, the real-time position information, time information and speed information generated by the global satellite navigation system have been widely used in civil and military applications [1]. In the military, satellite navigation is widely used in missiles, weapons guidance, operational command, control, intelligence, surveillance, reconnaissance, military communications, military logistical support, unmanned systems, emergency rescue and so on. In civilian use, satellite navigation is widely used in vehicles, aviation, ships, mobile equipment navigation, outdoor sports travel, map

The associate editor coordinating the review of this manuscript and approving it for publication was Tae Wook Kim.

services, emergency rescue, precision agriculture, logistics and transportation, etc. The relatively low strength of satellite navigation signals, unencrypted signal broadcasting, and the possibility of a single point of failure in the system lead to a satellite navigation system that is susceptible to malicious attacks, threatening the security of the system [2].

Spoofing jamming to satellite navigation systems can be categorized as intentional and unintentional, with unintentional spoofing jamming usually caused by other electronic equipment, weather conditions or natural disturbances, for example, electromagnetic interference, changes in atmospheric conditions, multipath effects and so on, which may cause distortion or weakening of satellite navigation signals, thus affecting the performance of the navigation system. Although such jamming is usually not intentional, it may still have a negative impact on the system. Intentional spoofing jamming is a purposeful and deliberate act aimed at misleading or disrupting the normal operation of a satellite navigation system. Intentional spoofing jamming can be carried out by a variety of means, including transmitting false navigation signals, altering the characteristics of real signals, simulating multiple false satellite signals, and so on. Attackers may attempt to cause users to receive false position information, thereby affecting the reliability and accuracy of the navigation system [3]. Spoofing is an intentionally false jamming to a satellite navigation system designed to mislead the receiver into calculating incorrect critical information such as position, speed and time. The vulnerability of satellite navigation system signals makes it vulnerable to spoofing jamming. The receiver captures and track spoofing signal instead of the real navigation satellite signals. Hence, the receiver gets a wrong position fix which could lead to serious consequences [4]. On the military front, Satellite navigation system can provide accurate positioning for precision guided weapons such as cruise missiles and guided bombs, greatly improve the hit rate of weapons, and effectively kill enemy targets. Iran controlled the landing of a United States RQ-170 Sentinel drone through the use of a spoofing attack. On the civilian side, it plays an irreplaceable role in the fields of geological mapping, earthquake monitoring, vehicle navigation, personal positioning, civil aviation air traffic control and power grid time service. there were more than 50 incidents of GPS spoofing at Manila airport in just three months. In addition, autonomous driving requires higher integrity and reliability of position, time, and speed information, otherwise the use of a falsified spoofed information can lead to serious traffic accidents [5]. Therefore, for applications that rely heavily on positioning schemes, it is important to ensure that the positioning information obtained by GNSS receivers from satellites has a high degree of accuracy and reliability [6].

Spoofing jamming is a more sophisticated and covert attack than traditional jamming such as suppression jamming. It can spoof the receiver to the wrong time and position by sending false GNSS signals without being detected by the terminal equipment. Spoofing jamming techniques include generating spoofing attacks and forwarding spoofing attacks. Generating spoofing attacks are carried out by an attacker who generates and sends fake navigation signals that are similar to real navigation signals in terms of frequency, phase and code type. This approach causes the receiver to mistake these fake signals for real satellite signals, thus calculating the wrong position. A forward spoofing attack is where an attacker captures the real navigation signal and then resends it to the receiver, possibly adding some misleading information. This approach allows the receiver to receive the same or similar signal as the real one, but the attacker can guide the receiver to compute the wrong position by modifying some properties of the signal [7]. Therefore, spoofing has a higher risk factor than jamming. Currently, research on anti-spoofing countermeasures against spoofing jamming attacks is emerging [8]. Spoofing detection techniques are the first step in anti-spoofing technology research, and it is also a very critical step. Domestic and foreign scholars have proposed many methods for spoofing detection. Feng et al. [9] proposed an algorithm based on unsupervised machine learning Gaussian mixture model (GMM). Zhang et al. [10] proposed transforming the spoofing detection problem into the sequence linearity detection problem by jointly monitoring the linearity of the pseudo-range difference (PRD) sequence and pseudo-range sum (PRS) sequence. Bose [11] proposed an alternate anti-spoofing method using neural networks. Tao et al. [12] proposed a practical method of detections' fusion based on an approach to assign the belief function for spoofing detections. Chen et al. [13] proposed a GNSS multi-parameter joint detection method based on support vector machine (SVM). Li [14] proposed a method against single antenna spoofing jamming utilizing the Fréchet distance of Doppler frequency difference. Liu et al. [15] proposed a deception detection algorithm based on pseudo-range difference. Wu et al. [16] proposed an anti-spoofing method for BeiDou navigation system based on the combination of SM commercial cryptographic algorithm and Timed Efficient Stream Loss-tolerant Authentication (TESLA) for spoofing attacks. Guo et al. [17] proposed a novel algorithm based on maximum likelihood (ML) estimation to remove counterfeit signals. Zhang and Zhan [18] proposed a novel spoofing network monitoring (SNM) mechanism aiming to reveal the presence of spoofing within an area. Sun et al. [19] used the moving variance of the delta test and the ratio test measured by the SQM technique to detect spoofing. SQM technology detects the occurrence of spoofing attacks by identifying the deformation of the correlation function caused by intermediate spoofing attacks. However, when the deception signal does not undergo correlation function deformation, the method cannot detect deception well. Rothmaier [20], [21] summarized and analyzed spoofing detection methods in multiple papers. However, the spoofing detection method for pseudo-range remains to be further studied.

Clustering algorithms are more sensitive to the presence of noise or outliers in the data, causing them to be incorrectly assigned to a cluster [9]. Complex neural network models require long inference times, which can affect the real-time performance of the system [13]. Although encrypted authentication technology improves the security of the system, it increases the complexity of the satellite navigation system and adds a certain amount of latency [16]. While the receiver is unable to achieve spoofing detection at the signal level, spoofing detection against the pseudo-range solved by localization is necessary. Therefore, this paper proposes a generalized likelihood ratio satellite navigation spoofing detection algorithm based on moving variance for pseudo-range, which is used to detect forged GNSS signals whose pseudo-range is changed. The core of the algorithm is to calculate the moving variance of the pseudo-range of different satellites at the same time, and then bring the moving variance into the generalized likelihood ratio spoofing detection model to achieve spoofing detection. The algorithm is well suited for detecting spoofed signals because of the difference in the moving variance of the positions generated by spoofed and normal signals.

II. PSEUDO-RAGNE SPOOFING MODEL

The distance measurement value of the receiver to the satellite signal is the pseudo-range, which is the observation value of the real distance, The real distance measurements contain a margin error resulting from ionospheric and tropospheric delays and etc. The spoofers can modify the arrival time of the satellite signals measured by the receiver by introducing artificial time delays, changing the carrier phase, and enhancing or weakening the strength of the signals. This results in the pseudorange value calculated by the receiver deviating from the true value. Pseudo-range spoofing refers to the difference between the pseudo-range measurement values obtained by demodulating the spoofing signal and the normal signal. The spoofing source introduces pseudo-range spoofing by changing the ranging code of the normal satellite signals, thereby generating a spoofing signal and causing the navigation device to produce an erroneous positioning result [22].

When the satellite navigation signal has spoofing jamming, the attacker will add pseudo-range deviation to the satellite signal and increase the signal power for transmission, so that the receiver will preferentially capture and track the signal to achieve the purpose of spoofing. In this way, the true pseudo-range will be affected by the deviation, forming a pseudo-range of spoofing jamming [23]. In this case, the pseudo-range of N satellites can be expressed as:

$$y_s = Gx + I_{\mathrm{ss}} y_{\mathrm{b}} + \varepsilon \tag{1}$$

R^N represents the spoofing pseudo-range of N satellites; $\boldsymbol{G} \in \boldsymbol{R}^N$ is a geometric matrix that projects x to y_s; $x \in R^P$ is the estimated position; P is the number of states including the number of coordinates and the number of clocks; $y_b \in R^s$ is the pseudo-range deviation introduced by the attacker, and s represents the dimension of the set of real numbers;$\boldsymbol{I}_{ss} \in \boldsymbol{R}^{N\times s}$ is a matrix that maps the deviation to the pseudo-distance of N satellites, ss is the corner scale of the $N \times s$ dimensional real matrix that denotes the deception projection matrix, $N \times s$ represents the dimension of the set of real numbers; $\varepsilon \in R^N$ is the noise, which obey the normal distribution $\varepsilon \sim N\left(0, w^{-1}\right)$. Next, the unbiased least squares estimation is used to calculate the receiver's position [24], and the estimated vector of the position x is represented by the following

$$\hat{x} = Sy_s \tag{2}$$

where $\boldsymbol{S}$ is the position estimation matrix, denoted by

$$S = \left(G^T WG\right)^{-1} G^T W \tag{3}$$

where the geometric matrix $\boldsymbol{G}$ represents the geometric relationship between position of the satellite and position of the receiver. $\boldsymbol{W}$ is the weight vector matrix.

By using unbiased least squares estimation, the average position deviation x_b can be expressed as a linear function of the pseudo-range deviation y_b [25], as follows

$$x_b = S_{ss} y_b \tag{4}$$

where $\boldsymbol{S}_{ss}$ is the matrix that maps the pseudo-range deviation y_b to the average position deviation x_b.

$$S_{ss} = SI_{ss} \tag{5}$$

χ^2 Statistics can be expressed as [26]

$$\left\| y_s - G\hat{x} \right\|_P^2 = -2 \log \Lambda \tag{6}$$

where the states P can be expressed as

$$P = W - WG\left(G^T WG\right)^{-1} G^T W \tag{7}$$

$-2 \log \Lambda$ obeys the distribution in two assumptions as follows formula (8)

$$\begin{cases} -2 \log \Lambda | H_0 \sim \chi_k^2 \\ -2 \log \Lambda | H_1 \sim \chi_{k,\lambda}^2 \end{cases} \tag{8}$$

The degree of freedom k and the non-centrality parameters λ can be expressed as

$$k = N - P \tag{9}$$

$$\lambda = y_b^T I_{ss}^T P I_{ss} y_b = y_b^T W_{ss} y_b - x_b^T G^T WG x_b \tag{10}$$

where

$$W_{ss} = I_{ss}^T W I_{ss} \tag{11}$$

When $s{>}p$ pseudo-range is spoofing, the spoofer can introduce a state bias x_b. Pseudo-range bias y_b is given by

$$y_b = W_{ss}^{-1} S_{ss}^T \left(S_{ss} W_{ss}^{-1} S_{ss}^T\right)^{-1} x_b \tag{12}$$

III. GENERALIZED LIKELIHOOD RATIO SPOOFING DETECTION MODEL BASED ON MOVING VARIANCE

General likelihood ratio test (GLRT) is the likelihood ratio test that is more applicable to a wide range of scenarios. The unknown parameters can be estimated by using the maximum likelihood estimation (MLE) algorithm, which can be used in the case of unknown parameters or incompletely known probability density function (PDF). We selected the Neyman-Pearson criterion in this paper. This criterion is effective in dealing with hypothesis testing problems when the prior probability and cost are difficult to determine [27]. It is defined as: minimize the probability of missed alarms or maximize the probability of correct detection while maintaining a specified probability of false alarms. This means that GLRT usually has the lowest error rate given the same sample data. However, through research, it is found that in the face of multiple satellite spoofing, the generalized likelihood ratio test model has a high probability of missed detection, resulting in inaccurate and unreliable detection results. In order to solve this problem, a generalized likelihood ratio test model based on moving variance is proposed. Combining the moving variance algorithm with the generalized likelihood ratio test model can significantly improve the detection effect of the generalized likelihood ratio test model [28].

In this paper, a new data subset is created by calculating the variance of the pseudo-range of different satellites at the same time and moving it forward. The variance is calculated again by this data subset to obtain the moving variance. This process is repeated throughout the pseudo-range calculation. The new data set composed of the calculated variance represents the moving variance. The detection statistic of the moving variance is calculated by the generalized likelihood ratio test model to determine whether the pseudo-range of the satellite signal is spoofed or not. When the detection statistic exceeds a threshold, it is considered that the pseudo-range of the satellite signal may be spoofed [29]. The formula for the variance of the movement is shown as follows

$$\begin{aligned}\sigma_{MV}^{2}\left(y_{s}\right) &= \frac{1}{M}\sum\nolimits_{k=n-M+1}^{n}\left[x\left(k\right)-\overline{x\left(n\right)}\right]^{2}-x\left(n\right)\\ &= \overline{x^{2}\left(n\right)}-\overline{x\left(n\right)}\end{aligned} \tag{13}$$

where $\overline{x(n)}$ is average value of the samples in subset M, $\overline{x^2(n)}$ is quadratic sum of samples in the subset M, n is sample size, M is window size, when the window size is 2, the spoofing detection effect is the best.

Next, let H_0 denote the assumption that there is no spoofing jamming, and H_1 denotes the assumption that spoofing jamming exists [30]. The spoofing detection problem is expressed as formula (14)

$$\begin{cases} P\left(\log\Lambda\left(\sigma_{MV}^{2}\left(y_{s}\right)\right)\geq\gamma|H_{1}\right)\\ P\left(\log\Lambda\left(\sigma_{MV}^{2}\left(y_{s}\right)\right)<\gamma|H_{0}\right)\end{cases} \tag{14}$$

where γ is the detection threshold, Λ is the pseudo-range moving variance detection statistic [31], defined as

$$\log\Lambda\left(\sigma_{MV}^{2}\left(y_{s}\right)\right)=\log\frac{\max_{\theta_0\in\Omega_0}p(\sigma_{MV}^{2}\left(y_{s}\right)|\theta_0)}{\max_{\theta_1\in\Omega_1}p(\sigma_{MV}^{2}\left(y_{s}\right)|\theta_1)} \tag{15}$$

where the distribution parameter θ_i of the pseudo-range moving variance $\sigma_{MV}^{2}\left(y_{s}\right)$ in the distribution space Ω_i is maximum likelihood estimation (MLE) of unknown parameter when assuming that H_0 and H_1 are true, respectively. If $\log\Lambda\geq\gamma$, then the judgment H_1 is true, issuing a deceptive alarm.

Maximum false alarm probability$\left(P_{FA_{\max}}\right)$ is the probability that the system erroneously generates an alarm or detects a signal when no signal is actually detected. The solution of (14), the detection threshold γ, is obtained by solving the inverse cumulative density function (CDF) of $\log\Lambda|H_0$ [32], as shown in Eq. (16)

$$P_{FA_{\max}}=\int_{-\infty}^{\gamma}p\left(\log\Lambda|H_0\right)\mathrm{d}\log\Lambda \tag{16}$$

The probability of missed detection P_{MD} is obtained by calculating $\log\Lambda|H_1$ as follows

$$P_{MD}=\int_{\gamma}^{\infty}p\left(\log\Lambda|H_1\right)\mathrm{d}\log\Lambda \tag{17}$$

For the pseudo-range moving variance of a normal distribution with equal covariance (noise) under assumptions H_0 and H_1 [33]. Assume that the mean value of distribution is different, so $\theta_i=\mu_i$. μ_i is the distribution parameter of the pseudo-range moving variance $\sigma_{MV}^{2}\left(y_{s}\right)$ in the distribution space Ω_i.

$$\begin{aligned}&\sigma_{MV}^{2}\left(y_{s}\right)|H_0\sim N\left(\mu_0,\Sigma\right);\ \mu_0\in\Omega_0\\ &\sigma_{MV}^{2}\left(y_{s}\right)|H_1\sim N\left(\mu_1,\Sigma\right);\ \mu_1\in\Omega_1\end{aligned} \tag{18}$$

This is common in spoofing detection methods [34]. For pseudo-range moving variance of normal distribution with equal covariance, under any assumption, the equation (15) takes the form of formula (19).

$$\begin{aligned}\log\Lambda &= \log\frac{p(\sigma_{MV}^{2}\left(y_{s}\right)|\mu_0,\Sigma)}{p(\sigma_{MV}^{2}\left(y_{s}\right)|\mu_1,\Sigma)}\\ &= \frac{1}{2}\left(\mu_0-\mu_1\right)^{T}\Sigma^{-1}\left(\sigma_{MV}^{2}\left(y_{s}\right)-\mu_0+\sigma_{MV}^{2}\left(y_{s}\right)-\mu_1\right)\end{aligned} \tag{19}$$

where μ_i is known a priori or is given by the following maximum likelihood estimator [35]

$$\mu_i=\underset{\mu\in\Omega_i}{\arg\max}\,p\left(\sigma_{MV}^{2}\left(y_{s}\right)|\mu,\Sigma\right) \tag{20}$$

where $\Omega_0=\mu_0$, μ_0 is obtained by parameter estimation before spoofing detection. The covariance $\sum$ is calculated by calibrating under credible conditions.

For normal distribution, the solution of equation (20) is given by $\mu_1=\sigma_{MV}^{2}\left(y_{s}\right)$, and the form of equation (19) is rewritten as follows

$$\log\Lambda=-\frac{1}{2}\left\|\sigma_{MV}^{2}\left(y_{s}\right)-\mu_0\right\|_{\Sigma^{-1}}^{2} \tag{21}$$

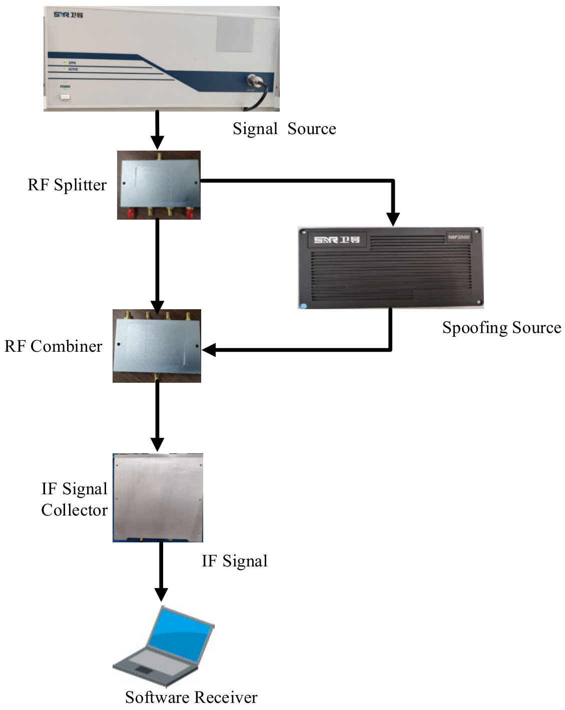


FIGURE 1. Hardware system architecture for performance verification of spoofing detection algorithm.

where $\| \|_{\Sigma^{-1}}^{2}$ is the squared Mahalanobis distance.

$$\left\| \sigma_{MV}^{2}\left(y_{s}\right) - \mu_{0} \right\|_{\Sigma^{-1}}^{2} = \left(\sigma_{MV}^{2}\left(y_{s}\right) - \mu_{0}\right)^{T} \Sigma^{-1} \left(\sigma_{MV}^{2}\left(y_{s}\right) - \mu_{0}\right) \tag{22}$$

Therefore, generalized likelihood ratio spoofing detection algorithm based on moving variance is the χ^2 test of matching degree between the pseudo-range moving variance detection statistic and H_0 [36]. Under H_0, $-2 \log \Lambda$ obeys the χ^2 distribution of k freedom degree. Under H_1, it obeys non-central χ^2 distribution, non-central parameter λ.

$$\begin{cases} -2 \log \Lambda | H_0 \sim \chi_k^2 \\ -2 \log \Lambda | H_1 \sim \chi_{k,\lambda}^2 \end{cases} \tag{23}$$

IV. SIMULATION EXPERIMENT

In order to verify the effectiveness of the proposed spoofing detection algorithm. Hardware system architecture for performance verification of spoofing detection algorithm is shown in Figure 1. The signal source generates normal satellite navigation signals. These signals are transmitted to the spoofing source through an RF splitter to create spoofing signals. The spoofing signals then enter the IF signal collector via the RF combiner. Subsequently, the collected IF signals are captured, tracked, and localized to determine the pseudorange in software receivers. Finally, spoofing signals are detected using the pseudorange information. The signal source is NSS8900 analog source of Hunan Satellite Navigation Company, and the spoofing source is NSF2000 portable navigation spoofing signal generation module of the same company.

TABLE 1. The detection threshold satisfying the requirement of false alarm probability.

$P_{FA_{\max}}$	Threshold
10^{-7}	-23.97
10^{-6}	-21.35
10^{-5}	-18.66

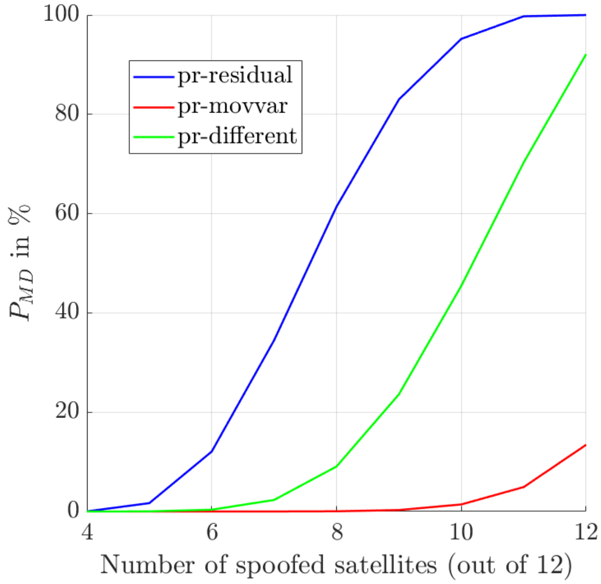
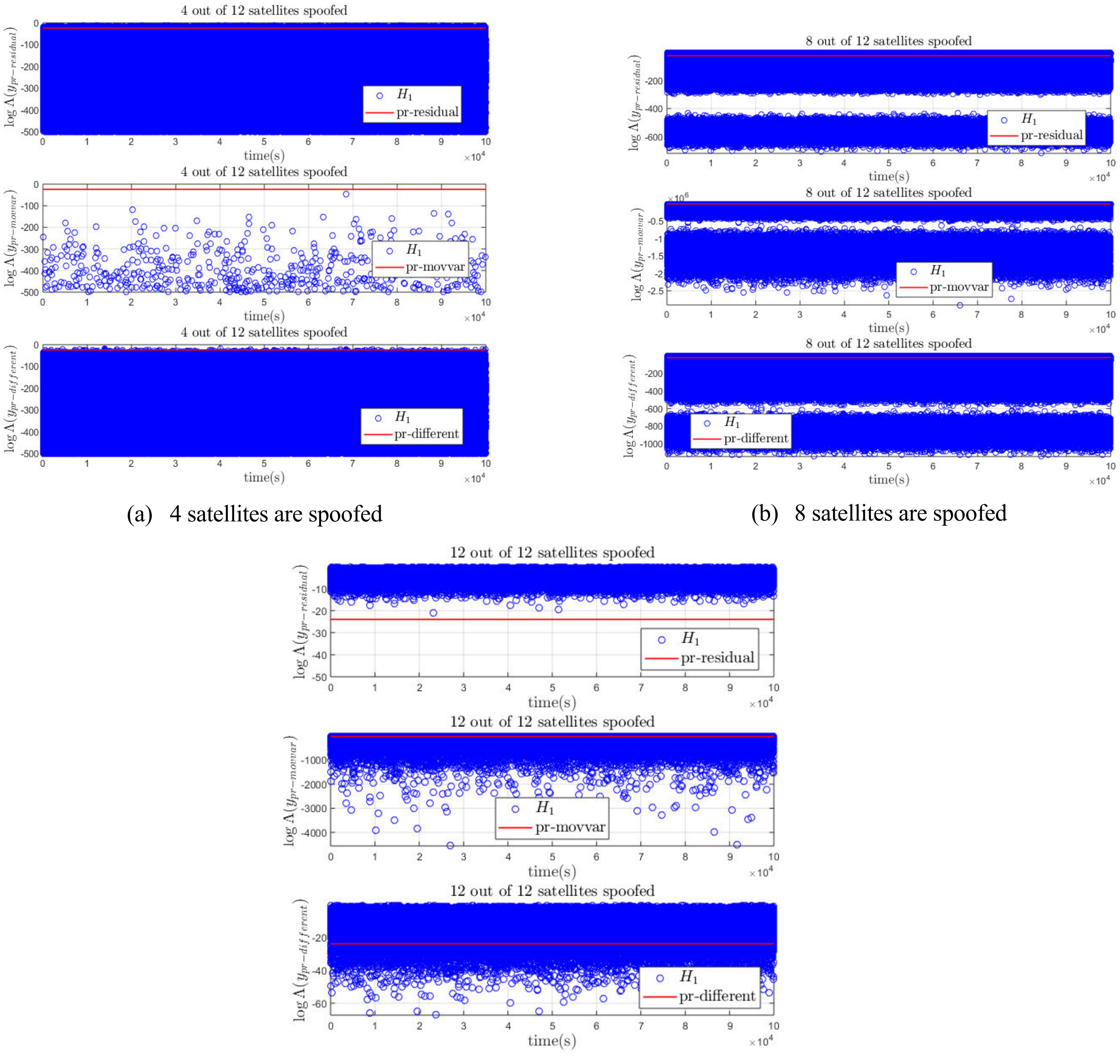


FIGURE 2. The missed detection probability for which pseudo-range deviation is 10 m.

In a true spoofing attack, numbers of spoofed satellites are unknown, and at least four visible satellites are required to provide a stable positioning service. Therefore, the number of spoofed satellites is first selected as 4, and then the number of spoofed satellites is continuously increased until all satellites are spoofed. The visible satellite is set to 12 satellites in one constellation. The B3I signal carrier frequency is 1268.52MHz, the IF frequency is 46.52MHz, the IF sampling frequency is 62MHz, and the signal bandwidth is 4.092MHz. The spoofed signal pseudorange deviations of the joined three are 2m, 10m, and 30m, respectively. The states P = 4 contains three coordinates and one clock. The spoofing module sends 4 to 12 satellites signals to induce the same pseudo-range deviation. The pseudo-range deviations are set to 2m, 10m, and 30m, respectively. Detection threshold is the threshold used by the system to determine whether a received signal is a target signal. If the probability of false alarms is too high, the navigation system may frequently misreport spoofing attacks, causing users to generate unnecessary alerts or take incorrect actions. This could pose a serious risk to flight safety, military operations or other critical applications. Therefore, to ensure the reliability and security of a satellite navigation system, a very low false alarm probability, typically at the 10^{-7} level, is often required. This means that the probability



(a) 4 satellites are spoofed

(b) 8 satellites are spoofed

(c) 12 satellites are spoofed

FIGURE 3. Detection statistics scatter plot.

of false alarms occurring in each detection decision is very small to reduce the risk of false alarms. When the false alarm probability is kept at a very low level, the navigation system is better able to cope with malicious interference and spoofing attacks, improving the robustness and availability of the system. Table 1 gives the detection thresholds when the maximum false alarm probability requirements are 10^{-7}, 10^{-6} and 10^{-5} respectively.

To emphasize the advantages of the algorithm presented in this paper, we compare it with two outstanding generalized likelihood ratio satellite navigation spoofing detection algorithms in related references. One is based on pseudo-range residual, the other on pseudo-range difference. The first algorithm is to calculate the detection statistics of the residual error of pseudo-range measurement value and pseudo-range estimation value, and then compare it with the detection threshold to achieve spoofing detection. The second algorithm is to calculate the detection statistics of the pseudo-range difference of the two adjacent satellites, and then compare it with the detection threshold to achieve spoofing detection.

For all subsets of 4 to 12 satellites, 3797 spoofing detections are performed. Now the simulation analysis is carried out for the spoofing scheme in which pseudo-range deviation is 10 m. The false alarm probability is set to 10^{-7}, at which point the detection threshold is -23.97. As shown in Figure 2, pr-residual refers to the generalized likelihood ratio satellite navigation spoofing detection algorithm based

TABLE 2. Missed detection probability table FOR which pseudo-range deviation is 10 m.

The number of spoofed satellites	pr-residual	pr-different	pr-movvar
4	0.02%	0.02%	0.00%
5	1.68%	0.05%	0.00%
6	12.07%	0.36%	0.00%
7	34.50%	2.32%	0.00%
8	61.40%	9.06%	0.04%
9	83.00%	23.60%	0.29%
10	95.20%	45.46%	1.42%
11	99.75%	70.33%	4.92%
12	100.00%	92.13%	13.44%

on pseudo-range residual, pr-movvar refers to the generalized likelihood ratio satellite navigation spoofing detection algorithm based on moving variance, and pr-different refers to the generalized likelihood ratio satellite navigation spoofing detection algorithm based on pseudo-range difference.

For the pr-residual, when the number of spoofed satellites is 4 and 5 respectively, the probability of missed detection is about 1%. When the number of spoofed satellites is higher than 6, the probability of missed detection increases significantly. When all satellites are spoofed, the probability of missed detection is increased to 100 %, and pseudo-range spoofing cannot be detected at this time. For the pr-different, when the number of spoofed satellites is 4,5,6, the probability of missed detection is about 0 %. while the number of spoofed satellites is higher than 7, the probability of missed detection is significantly improved. When all satellites are spoofed, the missed detection probability is 92.13 %. For the pr-movvar, while the number of spoofed satellites is 4,5,6 and 7 respectively, the probability of missed detection is stable at 0 %. When the number of spoofed satellites is 8,9,10, and 11, the missed detection probability is slightly increased. While all satellites are spoofed, the missed detection probability is increased to 13.44 %.

It is obvious that the missed detection probability of the pr-movvar is greatly reduced. The specific probability is shown in Table 2.

Figure 2 shows that when the correct number of satellites is spoofed, receivers using pr-residual may be completely spoofed, the receiver using the pr-different has a high probability of being spoofed. Receivers using the pr-movvar can avoid this situation.

In order to better illustrate and understand this result. In Fig.3, the situation when 4,8,12 satellites are spoofed is studied in more detail. This set of plots shows a scatter plot of the detection statistic for spoofing pseudo-range. The spoofing pseudo-range residual statistics are represented by $\log\Lambda(y_{\text{pr}-\text{residual}})$, the spoofing pseudo-range moving variance statistics are represented by $\log\Lambda(y_{\text{pr}-\text{movvar}})$, and the spoofing pseudo-range difference statistics are represented by $\log\Lambda(y_{\text{pr}-\text{different}})$. The red line is expressed as the detection threshold of the spoofing pseudo-range residual statistics, the spoofing pseudo-range difference statistics, and the spoofing pseudo-range moving variance statistics. Due to the excessive amount of data in this experimental test statistic, all observations cannot clearly see the detection results. In situations where observing the maximum value of the group's detection statistics can discern detection outcomes, the observation range is adjusted to focus on detecting the maximum value within a specific interval below the detection threshold.

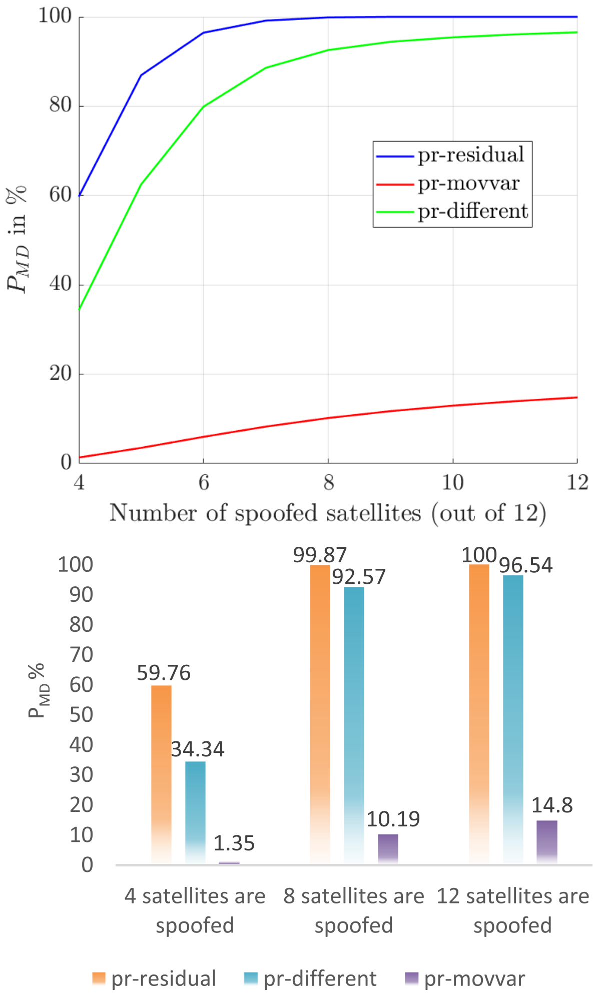


FIGURE 4. Missing detection probability for which pseudo-range deviation is 2m.

As is evident from Figure 3 that for pr-residual, when the number of spoofed satellites is 4, there is less missed detection. while the number of spoofed satellites is 8, the probability of missed detection increases. When all satellites are spoofed, the probability of missing detection is 100 %; For pr-movvar, when the number of spoofed satellites is 4, there is no missing detection, while the number of spoofed satellites is 8, there is less probability of missed detection. when all satellites are spoofed there is a certain degree of missed detection; For the pr-different, there are some missed detections while the number of spoofed satellites is 4, 8 and 12.

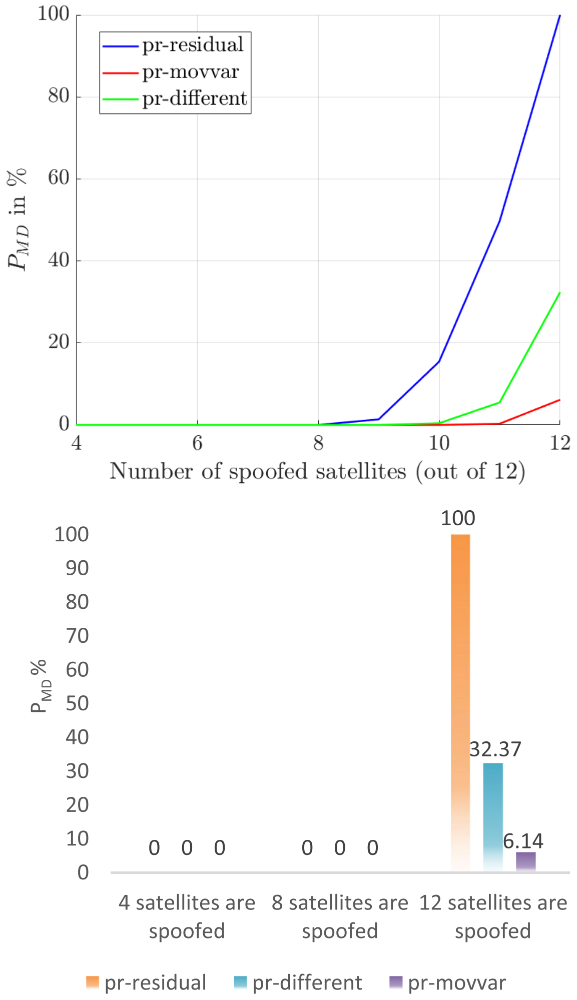


FIGURE 5. The missed detection probability for which pseudorange deviation is 30 m.

Therefore, for spoofing which pseudo-range deviation of 10 m, the pr-movvar has better detection performance.

In order to better observe its detection performance, the pseudo-range deviation is now changed to 2m and 30m.

As shown in Figure 4, the pr-residual and the pr-different have high missed detection probability and poor detection performance in the face of spoofing when the pseudo-range deviation is set to 2m; the missed detection probability of the pr-movvar is significantly reduced. While the number of spoofing satellites is 4, the missed detection probability of the pr-residual is 59.76 %, the missing detection probability of the pr-different is 34.34 %, and the missed detection probability of the pr-movvar is 1.35 %. while the number of spoofing satellites is 8, the missed detection probability of the pr-residual has reached 99.87 %, the missed detection probability of the pr-different is 92.57 %, and the missed detection probability of the pr-movvar is 10.19 %. When all satellites are spoofed, the missed detection probability of the pr-residual has reached 100 %, the missed detection probability of the pr-different is 96.54 %, and the missing detection probability of the pr-movvar is 14.80 %. Therefore, in the face of spoofing with a pseudo-range deviation of 2m, the pr-movvar has better detection performance.

As shown in Figure 5, the pr-residual, the pr-different and the pr-movvar have good detection results in the face of spoofing with a pseudo-range deviation of 30 m. while the number of spoofed satellites is less than 8, the probability of missed detection of three detection algorithms is always maintained at 0 %; while the number of spoofed satellites is higher than 10, pr-movvar is superior to both pr-residual and pr-different algorithms in terms of detection performance. When all satellites are spoofed, the missed detection probability of the pr-movvar is 6.14 %, the missed detection probability of the pr-different is 32.37 %, and the missed detection probability of the pr-residual is 100.00 %. Therefore, in the face of spoofing with large pseudo-range deviation, pr-movvar is still superior to both pr-residual and pr-different algorithms in terms of detection performance.

In summary, the pr-movvar is a more effective GNSS spoofing detection algorithm than the pr-residual and the pr-different. the pr-movvar proposed in this paper does not require anti-spoofing technology equipment, which is easy to implement and reduce the complexity of spoofing detection.

V. CONCLUSION

When the satellite navigation receiver cannot detect spoofing in the tracking and acquisition stage, this paper proposes pr-movvar for satellite navigation spoofing detection based on the pseudo-range calculated by positioning. The algorithm calculates the moving variance of the pseudo-range of different satellites at the same moment, calculates the detection statistic of the moving variance of the pseudo-range using the generalized likelihood ratio satellite navigation spoofing detection model, and detects the pseudo-range spoofing by comparing the statistic with the detection threshold. By using different numbers of spoofed satellites and different degrees of pseudo-range deviation, it is verified that the algorithm can detect spoofing signals well, and the average prediction accuracy rate can reach more than 98 %. The algorithm effectiveness is verified by comparing it with pr-residual and pr-different under the same spoofing situation. The research work in this paper helps to ensure the normal operation of the satellite navigation system and reduce the potential threats and risks, which is of great research significance for maintaining national security, improving the reliability of civil applications, and promoting technological innovation. And it provides theoretical reference for satellite navigation receivers to detect spoofing against pseudorange. Receivers using this spoofing detection algorithm can be used in a wide range of applications such as aviation, vehicle, marine navigation, military, intelligent transportation, emergency rescue, etc. The future research direction is to integrate receiver spoofing detection capabilities with deep learning models such as Transformer, Recurrent Neural Network, and Long Short-Term Memory. This integration aims to achieve intelligent detection, enhance receiver spoofing detection efficiency, and save detection time.

REFERENCES

[1] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," *IEEE Access*, vol. 8, pp. 165444–165496, 2020, doi: 10.1109/ACCESS.2020.3022294.

[2] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016, doi: 10.1109/JPROC.2016.2526658.

[3] T. Hua, X. Zhu, X. Tang, G. Tu, and X. Chen, "Brief review of GNSS spoofing and anti-spoofing technology," in *Proc. Int. Conf. Sens., Meas. Data Anal. Era Artif. Intell. (ICSMD)*, Nanjing, China, Oct. 2021, pp. 1–7, doi: 10.1109/ICSMD53520.2021.9670759.

[4] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins, "GNSS vulnerabilities and existing solutions: A review of the literature," *IEEE Access*, vol. 9, pp. 153960–153976, 2021, doi: 10.1109/ACCESS.2020.2973759.

[5] X. Wang, J. Yang, and M. Huang, "GNSS interference and spoofing detection research status and prospects," *Signal Process.*, pp. 1–21, Nov. 2023.

[6] S. Ni, Q. Fu, and S. Chen, "A review of satellite navigation spoofing interference detection techniques," *Electron. Technol. Softw. Eng.*, no. 7, pp. 147–153, 2023.

[7] N. Spens, D.-K. Lee, and D. Akos, "An application for detecting GNSS jamming and spoofing," in *Proc. 34th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS+)*, Oct. 2021, pp. 1981–1988.

[8] A. Molina-Markham and J. J. Rushanan, "Positioning, navigation, and timing trust inference engine," in *Proc. Int. Tech. Meeting Inst. Navigat.*, Feb. 2020, pp. 1030–1044, doi: 10.33012/2020.17195.

[9] Z. Feng, C. K. Seow, and Q. Cao, "GNSS anti-spoofing detection based on Gaussian mixture model machine learning," in *Proc. IEEE 25th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2022, pp. 3334–3339, doi: 10.1109/ITSC55140.2022.9922109.

[10] X. Zhang, T. Liang, J. Tian, J. Wu, C. Wang, and M. Chen, "Anti-spoofing method for improving GNSS security by jointly monitoring pseudo-range difference and pseudo-range sum sequence linearity," *Sensors*, vol. 23, no. 20, p. 8418, Oct. 2023, doi: 10.3390/s23208418.

[11] S. C. Bose, "GPS spoofing detection by neural network machine learning," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 37, no. 6, pp. 18–31, Jun. 2022, doi: 10.1109/MAES.2021.3100844.

[12] H. Tao, H. Li, and M. Lu, "A method of detections' fusion for GNSS anti-spoofing," *Sensors*, vol. 16, no. 12, p. 2187, Dec. 2016, doi: 10.3390/s16122187.

[13] Z. Chen, J. Li, J. Li, X. Zhu, and C. Li, "GNSS multiparameter spoofing detection method based on support vector machine," *IEEE Sensors J.*, vol. 22, no. 18, pp. 17864–17874, Sep. 2022, doi: 10.1109/JSEN.2022.3193388.

[14] J. Li, X. Zhu, M. Ouyang, D. Shen, Z. Chen, and Z. Dai, "GNSS spoofing detection technology based on Doppler frequency shift difference correlation," *Meas. Sci. Technol.*, vol. 33, no. 9, Sep. 2022, Art. no. 095109.

[15] K. Liu, W. Wu, Z. Wu, L. He, and K. Tang, "Spoofing detection algorithm based on pseudorange differences," *Sensors*, vol. 18, no. 10, p. 3197, Sep. 2018, doi: 10.3390/s18103197.

[16] Z. Wu, Y. Zhang, L. Liu, and M. Yue, "TESLA-based authentication for BeiDou civil navigation message," *China Commun.*, vol. 17, no. 11, pp. 194–218, Nov. 2020, doi: 10.23919/JCC.2020.11.016.

[17] Y. Guo, L. Miao, and X. Zhang, "Spoofing detection and mitigation in a multi-correlator GPS receiver based on the maximum likelihood principle," *Sensors*, vol. 19, no. 1, p. 37, Dec. 2018, doi: 10.3390/s19010037.

[18] Z. Zhang and X. Zhan, "GNSS spoofing network monitoring based on differential pseudorange," *Sensors*, vol. 16, no. 10, p. 1771, Oct. 2016, doi: 10.3390/s16101771.

[19] C. Sun, J. W. Cheong, A. G. Dempster, L. Demicheli, E. Cetin, H. Zhao, and W. Feng, "Moving variance-based signal quality monitoring method for spoofing detection," *GPS Solutions*, vol. 22, no. 3, Jul. 2018, doi: 10.1007/s10291-018-0745-7.

[20] 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, doi: 10.1002/navi.420.

[21] F. Rothmaier, "Optimal sequential spoof detection based on direction of arrival measurements," in *Proc. 33rd Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS+)*, Oct. 2020, pp. 3253–3267, doi: 10.33012/2020.17538.

[22] K. Liu, W. Wu, K. Tang, Z. Wu, and S. Zhang, "GNSS dual-receiver against repeater deception jamming detection algorithm based on pseudo-range information," *Syst. Eng. Electron.*, vol. 39, no. 11, pp. 2393–2398, 2017.

[23] F. Rothmaier, L. Taleghani, Y.-H. Chen, S. Lo, E. Phelts, and T. Walter, "GNSS spoofing detection through metric combinations: Calibration and application of a general framework," in *Proc. 34th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS+)*, Oct. 2021, pp. 4249–4263, doi: 10.33012/2021.18126.

[24] M. Joerger, Y. Zhai, I. Martini, J. Blanch, and B. Pervan, "ARAIM continuity and availability assertions, assumptions, and evaluation methods," in *Proc. Int. Tech. Meeting Inst. Navigat.*, San Diego, CA, USA, Jan. 2020, pp. 404–420, doi: 10.33012/2020.17152.

[25] V. O. Zhilinskiy, "Evaluation of GNSS pseudorange residual error mitigation model," in *Proc. IEEE 23rd Int. Conf. Young Professionals Electron Devices Mater. (EDM)*, Altai, Russia, Jun. 2022, pp. 177–180, doi: 10.1109/EDM55285.2022.9855183.

[26] C. Zhang, X. Lu, and S. Gao, "Residual chi-square test and DAVAR based on fault diagnosis and positioning," *Navigat. Control*, vol. 17, no. 2, pp. 25–31, 2018.

[27] Y. Yang, J. Guo, S. Wang, J. Yang, and H. Liu, "GNSS spoofing detection based correlation and distance for vehicle application," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Xining, China, Aug. 2023, pp. 64–71, doi: 10.1109/smartiot58732.2023.00017.

[28] M. Ö. Demir, G. K. Kurt, and A. E. Pusane, "A pseudorange-based GPS spoofing detection using hyperbola equations," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 10770–10783, Aug. 2023, doi: 10.1109/TVT.2023.3257228.

[29] F. Rothmaier, Y.-H. Chen, S. Lo, and T. Walter, "A framework for GNSS spoofing detection through combinations of metrics," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 6, pp. 3633–3647, Dec. 2021, doi: 10.1109/TAES.2021.3082673.

[30] J. Li, X. Zhu, M. Ouyang, W. Li, Z. Chen, and Z. Dai, "Research on multi-peak detection of small delay spoofing signal," *IEEE Access*, vol. 8, pp. 151777–151787, 2020, doi: 10.1109/ACCESS.2020.3016971.

[31] S. Chen, S. Ni, L. Cheng, T. Lei, Z. Jia, and Q. Fu, "Detection and orientation of GNSS spoofing based on positioning solutions of three receivers," *IEEE Access*, vol. 11, pp. 32365–32379, 2023, doi: 10.1109/ACCESS.2023.3262996.

[32] W. Zhou, Z. Lv, W. Wu, X. Shang, and Y. Ke, "Anti-spoofing technique based on vector tracking loop," *IEEE Trans. Instrum. Meas.*, vol. 72, 2023, Art. no. 8504516, doi: 10.1109/TIM.2023.3289551.

[33] M. Deng, H. Wang, D. Ming, and Y. Chen, "GNSS spoofing detection based on abnormal receiver noise and carrier-to-noise ratio metric," in *Proc. IEEE 22nd Int. Conf. Commun. Technol. (ICCT)*, Nanjing, China, Nov. 2022, pp. 1306–1311, doi: 10.1109/ICCT56141.2022.10072895.

[34] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 23559–23572, Dec. 2022, doi: 10.1109/TITS.2022.3197817.

[35] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 1, pp. 469–475, Feb. 2019, doi: 10.1109/TAES.2018.2848318.

[36] J. Liu, F. Chen, Y. Xie, B. Ge, Z. Lu, and G. Sun, "Robust spoofing detection for GNSS array instrumentation based on C/N$_0$ difference measurements," *IEEE Trans. Instrum. Meas.*, vol. 72, 2023, Art. no. 8507211, doi: 10.1109/TIM.2023.3328684.

PINGPING QU was born in Heilongjiang, China, in 1979. She received the Ph.D. degree in control science and engineering major from Harbin Institute of Technology, China, in 2013.

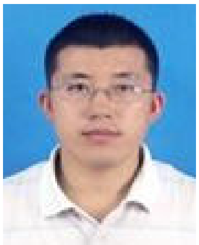
She is currently an Associate Professor with the School of Electronic and Information Engineering, Shenyang Aerospace University, Shenyang, China. Her current research interests include aircraft guidance and control, satellite navigation anti-jamming technology and satellite navigation, and positioning technology.

TIANFENG LIU was born in Liaoning, China, in 1998. He received the B.S.E. degree in communication engineering from the City Institute, Dalian University of Technology, Liaoning, in 2021. He is currently pursuing the M.Eng. degree in electronic information with Shenyang Aerospace University, Shenyang, China.

His current research interest includes satellite navigation anti-spoofing technology.

TENGLI YU was born in Hebei, China, in 1997. She received the B.S.E. degree in geomatics engineering from Shijiazhuang Tiedao University, Shijiazhuang, China, in 2019, and the M.Eng. degree in geomatics engineering from Tianjin Chengjian University, Tianjin, China, in 2022. She is currently pursuing the Ph.D. degree with Shenyang Aerospace University, Shenyang, China.

Her research interests include the global navigation satellite system (GNSS) meteorology and aircraft navigation and positioning algorithms.



ERSHEN WANG was born in Liaoning, China, in 1980. He received the Ph.D. degree in communication and information systems from Dalian Maritime University, China, in 2009.

From January 2014 to December 2016, he was a Postdoctoral Researcher with Beihang University, China. He is currently a Professor with the School of Electronic and Information Engineering, Shenyang Aerospace University, Shenyang, China. He is also a member with Liaoning General Aviation Academy, Shenyang. He is the Lead of the Key Laboratory of Navigation and Surveillance Technology. He has published more than 80 articles in peer-reviewed journals and proceedings and 20 patents/software copyrights. His current research interests include BeiDou navigation satellite systems (BDSs)/global navigation satellite systems (GNSSs) positioning theory and signal processing, integrity monitoring, integrated navigation, target tracking, artificial intelligence, and applications to unmanned systems.

SONG XU was born in Jilin, China, in 1986. He received the M.S. degree in information and communication engineering from Shenyang Aerospace University, Liaoning, China, in 2016.

He is currently the Deputy Director of the Experimental Center, School of Electronic and Information Engineering, Shenyang Aerospace University, Shenyang, China. His current research interests include avionics technology and telecommunication technology.

ZIBO YUAN was born in Hebei, China, in 1998. He received the B.S.E. degree in communication engineering from Tangshan University, Hebei, in 2021. He is currently pursuing the M.Eng. degree in electronic information with Shenyang Aerospace University, Shenyang, China.

His current research interest includes satellite navigation anti-jamming technology.