

Article

Anti-Spoofing Method for Improving GNSS Security by Jointly Monitoring Pseudo-Range Difference and Pseudo-Range Sum Sequence Linearity

Xinran Zhang, Taotao Liang, Jie Tian , Junwei Wu, Chuan Wang and Maolin Chen *

Institute of Electronic Engineering, China Academy of Engineering Physics, Mianyang 621999, China; zhang-xr15@tsinghua.org.cn (X.Z.); oldphoto522121@163.com (T.L.); tianjie@caep.cn (J.T.); wjwcaep@163.com (J.W.); wch_eml@126.com (C.W.)

* Correspondence: maolin66@126.com

Abstract: Spoofing interference is one of the most emerging threats to the Global Navigation Satellite System (GNSS); therefore, the research on anti-spoofing technology is of great significance to improving the security of GNSS. For single spoofing source interference, all the spoofing signals are broadcast from the same antenna. When the receiver is in motion, the pseudo-range of spoofing signals changes nonlinearly, while the difference between any two pseudo-ranges changes linearly. Authentic signals do not have this characteristic. On this basis, an anti-spoofing method is proposed by jointly monitoring the linearity of the pseudo-range difference (PRD) sequence and pseudo-range sum (PRS) sequence, which transforms the spoofing detection problem into the sequence linearity detection problem. In this paper, the model of PRD and PRS is derived, the hypothesis based on the linearity of PRD sequence and PRS sequence is given, and the detection performance of the method is evaluated. This method uses the sum of squares of errors (SSE) of linear fitting of the PRD sequence and PRS sequence to construct detection statistics, and has low computational complexity. Simulation results show that this method can effectively detect spoofing interference and distinguish spoofing signals from authentic signals.



Citation: Zhang, X.; Liang, T.; Tian, J.; Wu, J.; Wang, C.; Chen, M.

Anti-Spoofing Method for Improving GNSS Security by Jointly Monitoring Pseudo-Range Difference and Pseudo-Range Sum Sequence Linearity. *Sensors* **2023**, *23*, 8418.

<https://doi.org/10.3390/s23208418>

Academic Editor: Baocheng Zhang

Received: 28 August 2023

Revised: 8 October 2023

Accepted: 10 October 2023

Published: 12 October 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: Global Navigation Satellite System (GNSS); security; spoofing interference; pseudo-range difference (PRD); pseudo-range sum (PRS); linearity; sum of squares of errors (SSE)

1. Introduction

Global Navigation Satellite System (GNSS) has the unique technical characteristics of all-weather, all-day, and global coverage and has become the most widely used space-based radio positioning system at present [1,2]. While it is widely used, the security of GNSS has been paid more attention [3]. Due to the inherent vulnerability of GNSS, such as weak signal power, publicly known civil signal structure, slow message update, etc., GNSS is vulnerable to external interference, and its security is seriously threatened [4,5]. In its current form, the main types of GNSS interference include suppression interference and spoofing interference. Suppression interference interferes with the target receiver by transmitting high-power signals, which reduces its positioning performance and even makes it impossible to locate [6]. However, the effect of suppressing interference is dominant. It is easy for the attacked receiver to find out that it has been suppressed and take countermeasures accordingly. The more covert spoofing interference induces the receiver to output wrong positioning results by broadcasting false signals with the same structural characteristics and different parameters as GNSS signals [7]. Compared with suppression interference, spoofing interference does not require high power, and its interference effect is more concealed, so its potential harm is higher [8]. The research on anti-spoofing technology is of great significance to improving the security of GNSS, which has gradually been widely valued by academic circles and has become a new research hotspot [9,10].

According to the number of spoofing sources, spoofing interference can be divided into two modes: single spoofing source interference and multiple spoofing sources interference [11]. Single spoofing source interference means that a spoofing source transmits multiple spoofing signals, which is the most common spoofing interference mode at present. In this way, the spoofing signals can be consistent without knowing the target receiver position [12]. Multiple spoofing sources interference means that each spoofing source produces a spoofing signal, and all the spoofing signals are transmitted to the receiver from different directions. This way is closer to the actual scene. Nevertheless, to make the spoofing signals meet the consistency, the receiver position should be known, and the spoofing sources need to synchronize accurately through the communication link, which requires high implementation cost and technical level. Up to now, the interference mode of multiple spoofing sources cooperative spoofing is still in the theoretical research stage, and there is no public report in the literature.

Because of the complexity of spoofing interference, the principles of anti-spoofing methods are quite different. The anti-spoofing method based on C/N_0 monitoring assumes that the C/N_0 of spoofing signals exceeds the normal range, but if the spoofing signals are broadcast together with noise, this method will be invalidated [13]. The signal quality monitoring method can detect the traction spoofing interference based on the fact that overlapping correlation peaks in the traction process will lead to distortion of the autocorrelation function but is ineffective when correlation peaks are separated [14]. The receiver autonomous integrity monitoring method detects spoofing interference according to the consistency of authentic signals, but it will fail when spoofing signals tend to be consistent [15].

For single spoofing source interference, an important feature is that all spoofing signals are broadcast from the same antenna. Therefore, the incidence angles of all spoofing signals are the same, while those of authentic signals are different. According to this, methods based on multiple antennas or multiple receivers can effectively detect spoofing interference [16–21]. However, these methods not only need to synchronize the observations of all antennas or receivers but also need to add extra hardware, which leads to high complexity and cost. In addition, methods based on mobile receivers are also effective [22–24]. All spoofing signals have the same propagation path, while the authentic signals from different satellites have different propagation paths. Therefore, when the receiver moves, some observations of the authentic signals and the spoofing signals will show different changes. Previous studies assumed that the channel gains or carrier Doppler shifts of all the spoofing signals are correlated, so spoofing interference can be detected by monitoring the correlation of channel gains or carrier Doppler shifts between different signals. However, the change in channel gain is related to the distance between the spoofing source and the receiver. The farther the distance, the less obvious the channel gain variation caused by the receiver motion [11]. In addition, the change in carrier Doppler shift is related to the velocity change in the receiver. The smaller the velocity change, the less obvious the carrier Doppler shift variation caused by the receiver motion.

Based on the above considerations, this paper proposes an anti-spoofing method for single spoofing source interference, which jointly monitors the linearity of the pseudo-range difference (PRD) sequence and pseudo-range sum (PRS) sequence. In a short time, the pseudo-range variation caused by the satellite motion is linear. For spoofing signals, although the variations in pseudo-ranges caused by the receiver motion are nonlinear, these variations are the same. Consequently, the pseudo-range of spoofing signals changes nonlinearly, while the difference between any two pseudo-ranges changes linearly. For authentic signals, it does not have this characteristic. Therefore, we can detect spoofing interference by monitoring the linearity of the PRD sequence and PRS sequence and distinguishing between authentic signals and spoofing signals. Compared with the existing research, the proposed method can effectively solve the problem of spoofing detection even when the distance between the spoofing source and the receiver is far away or the

velocity of the receiver changes slowly, which shows that the performance of the method is more robust.

Subsequent sections of this paper are arranged as follows. In Section 2, the models of PRD and PRS are derived, and their linear problems are analyzed. In Section 3, hypothesis testing is given, linearity detection statistics are constructed, and false alarm probability and detection probability are analyzed. Section 4 shows the simulation results. Section 5 summarizes the content of this paper.

2. Linearity Analysis

2.1. Pseudo-Range Sequence Linearity Analysis

The pseudo-range measurement value ρ of the authentic signal is as shown in Equation (1):

$$\rho = r + c(\delta t_u - \delta t_s + I + T) + \varepsilon, \quad (1)$$

where r represents the geometric distance between satellite and receiver; c represents the speed of light; δt_u and δt_s represent receiver clock error and satellite clock error, respectively; I is ionospheric delay; T is tropospheric delay; and ε represents pseudo-range measurement noise, which can be considered as Gaussian white noise.

Define the pseudo-range sequence $\vec{\rho}_i = [\rho_i(0), \dots, \rho_i(k), \dots, \rho_i(K-1)]$. $\rho_i(k)$ denotes the pseudo-range measurement value of the signal i at the k -th measurement time. The measurement time interval is Δt , and the sequence length is K . In a short time, the changes in ionospheric delay, tropospheric delay, and satellite clock error are very small and can be ignored. In addition, since the distance between the satellite and receiver is far enough, the position change of the satellite and receiver in a short time is very small relative to the distance between them. Therefore, the unit observation vector $\vec{l}_i$ of the satellite at the receiver can be considered constant. Thus, $\rho_i(k)$ can be approximately expressed as

$$\rho_i(k) \approx \Delta \vec{r}_{s,i}(k) \cdot \vec{l}_i - \Delta \vec{r}_u(k) \cdot \vec{l}_i + c \cdot \delta t_u(k) + \varepsilon_i(k) + Cn_i. \quad (2)$$

In Equation (2), $Cn_i = \rho_i(0) - c \cdot \delta t_u(0) - \varepsilon_i(0)$ is a constant; $\Delta \vec{r}_{s,i}(k)$ and $\Delta \vec{r}_u(k)$ represent the position vectors of the satellite and the receiver from time 0 to time k , respectively.

$\Delta \vec{r}_{s,i}(k) \cdot \vec{l}_i$ means the radial projection component of the satellite position change. The radial acceleration of the satellite is less than $2 \times 10^{-5} \text{ m/s}^3$ [11]. The radial acceleration is so small that it has little effect on radial velocity. Therefore, in a short time, it can be considered that the radial velocity is constant, which means that $\Delta \vec{r}_{s,i}(k) \cdot \vec{l}_i$ varies linearly. The receiver is driven by a stable clock, and its clock drift does not change obviously with time [25]. Therefore, the receiver clock difference $\delta t_u(k)$ can also be considered to vary linearly in a short time. When the receiver velocity is constant, $\Delta \vec{r}_u(k) \cdot \vec{l}_i$ changes linearly with time. When its velocity changes, $\Delta \vec{r}_u(k) \cdot \vec{l}_i$ changes nonlinearly. According to the above analysis, the elements in $\vec{\rho}_i$ are linear when the receiver moves at a uniform velocity, and nonlinear when the receiver moves at a variable velocity.

In case of spoofing signal, under the assumption that the position of the spoofing source is unchanged, $\rho_i(k)$ can be approximately expressed as

$$\rho_i(k) \approx \Delta \vec{r}_{s,i}(k) \cdot \vec{l}_i^p - \Delta \vec{r}_u(k) \cdot \vec{l}^u(k) + \Delta \rho_{p,i}(k) + c \cdot \delta t_u(k) + \varepsilon_i(k) + Cn_i, \quad (3)$$

where $\vec{l}_i^p$ represents the unit observation vector of the satellite at the spoofing source, $\vec{l}^u(k)$ represents the unit observation vector of the spoofing source at the receiver, and $\Delta \rho_{p,i}(k)$ represents the difference between the additional component of the spoofing source at time k and time 0. It should be emphasized that in addition to the assumption that the spoofing source is stationary, we also need to assume that the additional component of the spoofing

source to any signal changes linearly, which is the prerequisite for the effectiveness of the proposed method. Thus, $\Delta\rho_{p,i}(k)$ can be considered to vary linearly.

Since the distance between the satellite and the spoofing source is far enough, $\vec{l}_i^p$ can be considered to be constant in a short time, so that $\Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i^p$ varies linearly with time. While for $\vec{l}^u(k)$, due to the distance between the spoofing source and the receiver being relatively close, $\vec{l}^u(k)$ will change continuously with the movement of the receiver. Therefore, whether the receiver is moving at a uniform velocity or not, $\Delta\vec{r}_u(k) \cdot \vec{l}^u(k)$ is nonlinear with time, and then the elements in $\vec{\rho}_i$ are nonlinear.

2.2. PRD Sequence Linearity Analysis

Defining $\Delta\vec{\rho}_{ij} = [\Delta\rho_{ij}(0), \dots, \Delta\rho_{ij}(k), \dots, \Delta\rho_{ij}(K-1)]$ is the sequence of measured pseudo-range differences between the signal i and the signal j , where $\Delta\rho_{ij}(k)$ can be denoted as

$$\Delta\rho_{ij}(k) = \rho_i(k) - \rho_j(k). \quad (4)$$

If the two signals are authentic signals, $\Delta\rho_{ij}(k)$ can be derived as

$$\Delta\rho_{ij}(k) \approx \Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i - \Delta\vec{r}_{s,j}(k) \cdot \vec{l}_j - \Delta\vec{r}_u(k) \cdot (\vec{l}_i - \vec{l}_j) + \varepsilon_i(k) - \varepsilon_j(k) + \Delta\text{Cn}_{ij}, \quad (5)$$

where $\Delta\text{Cn}_{ij} = (\rho_i(0) - \varepsilon_i(0)) - (\rho_j(0) - \varepsilon_j(0))$ is a constant. The pseudo-range variation $c \cdot \delta t_u(k)$ caused by the change in the receiver clock difference is eliminated in the calculation process. In a short time, $\Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i$ and $\Delta\vec{r}_{s,j}(k) \cdot \vec{l}_j$ change linearly, and $\vec{l}_i - \vec{l}_j$ can be considered unchanged. Therefore, it is not difficult to conclude that the elements in $\Delta\vec{\rho}_{ij}$ are linear when the receiver moves at a uniform velocity and nonlinear when the receiver moves at a variable velocity.

If the two signals are spoofing signals, $\Delta\rho_{ij}(k)$ can be derived as

$$\Delta\rho_{ij}(k) \approx \Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i^p - \Delta\vec{r}_{s,j}(k) \cdot \vec{l}_j^p + \Delta\rho_{p,i}(k) - \Delta\rho_{p,j}(k) + \varepsilon_i(k) - \varepsilon_j(k) + \Delta\text{Cn}_{ij}. \quad (6)$$

The pseudo-range change $\Delta\vec{r}_u(k) \cdot \vec{l}^u(k)$ caused by the change in receiver position is eliminated in the calculation process. In this case, the elements in $\Delta\vec{\rho}_{ij}$ are linear regardless of whether the receiver is moving at a uniform velocity or a variable velocity.

If one of the two signals is an authentic signal and the other is a spoofing signal, $\Delta\rho_{ij}(k)$ can be derived as

$$\Delta\rho_{ij}(k) \approx \Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i - \Delta\vec{r}_{s,j}(k) \cdot \vec{l}_j^p - \Delta\vec{r}_u(k) \cdot (\vec{l}_i - \vec{l}^u(k)) - \Delta\rho_{p,j}(k) + \varepsilon_i(k) - \varepsilon_j(k) + \Delta\text{Cn}_{ij}. \quad (7)$$

Since $\vec{l}^u(k)$ will change during the motion of the receiver, $\Delta\vec{r}_u(k) \cdot \vec{l}^u(k)$ changes nonlinearly with time regardless of whether the receiver moves at a uniform velocity, which means that the elements in $\Delta\vec{\rho}_{ij}$ are nonlinear.

2.3. PRS Sequence Linearity Analysis

Defining $\Sigma\vec{\rho}_{ij} = [\Sigma\rho_{ij}(0), \dots, \Sigma\rho_{ij}(k), \dots, \Sigma\rho_{ij}(K-1)]$ is the sequence of measured pseudo-range sums between the signal i and the signal j , where $\Sigma\rho_{ij}(k)$ can be denoted as

$$\Sigma\rho_{ij}(k) = \rho_i(k) + \rho_j(k). \quad (8)$$

If the two signals are authentic signals, $\Sigma\rho_{ij}(k)$ can be derived as

$$\Sigma\rho_{ij}(k) \approx \Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i + \Delta\vec{r}_{s,j}(k) \cdot \vec{l}_j - \Delta\vec{r}_u(k) \cdot \left(\vec{l}_i + \vec{l}_j\right) + 2c \cdot \delta t_u(k) + \varepsilon_i(k) + \varepsilon_j(k) + \Sigma\text{Cn}_{ij}, \quad (9)$$

where $\Sigma\text{Cn}_{ij} = (\rho_i(0) - c \cdot \delta t_u(0) - \varepsilon_i(0)) + (\rho_j(0) - c \cdot \delta t_u(0) - \varepsilon_j(0))$ is a constant. In a short time, $\Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i$ and $\Delta\vec{r}_{s,j}(k) \cdot \vec{l}_j$ change linearly, and $\vec{l}_i + \vec{l}_j$ can be considered unchanged. Therefore, it is not difficult to conclude that the elements in $\Sigma\vec{\rho}_{ij}$ are linear when the receiver moves at a uniform velocity and nonlinear when the receiver moves at a variable velocity.

If the two signals are spoofing signals, $\Sigma\rho_{ij}(k)$ can be derived as

$$\Sigma\rho_{ij}(k) \approx \Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i^p + \Delta\vec{r}_{s,j}(k) \cdot \vec{l}_j^p - 2\Delta\vec{r}_u(k) \cdot \vec{l}^u(k) + \Delta\rho_{p,i}(k) + \Delta\rho_{p,j}(k) + 2c \cdot \delta t_u(k) + \varepsilon_i(k) + \varepsilon_j(k) + \Sigma\text{Cn}_{ij}. \quad (10)$$

If one of the two signals is an authentic signal and the other is a spoofing signal, $\Sigma\rho_{ij}(k)$ can be derived as

$$\Sigma\rho_{ij}(k) \approx \Delta\vec{r}_{s,i}(k) \cdot \vec{l}_i + \Delta\vec{r}_{s,j}(k) \cdot \vec{l}_j^p - \Delta\vec{r}_u(k) \cdot \left(\vec{l}_i + \vec{l}^u(k)\right) + \Delta\rho_{p,j}(k) + 2c \cdot \delta t_u(k) + \varepsilon_i(k) + \varepsilon_j(k) + \Sigma\text{Cn}_{ij}. \quad (11)$$

For the two cases, since $\vec{l}^u(k)$ will change during the motion of the receiver, $\Delta\vec{r}_u(k) \cdot \vec{l}^u(k)$ will change with time regardless of whether the receiver moves at a uniform velocity, which means that the elements in $\Sigma\vec{\rho}_{ij}$ are nonlinear.

2.4. Analysis Summary

Based on all the above analysis, we can draw a conclusion, as shown in Table 1. Case 1 indicates that the two signals are authentic signals. Case 2 indicates that the two signals are spoofing signals. Case 3 indicates that one of the two signals is an authentic signal and the other is a spoofing signal.

Table 1. Linearity analysis results of PRD sequence and PRS sequence.

	Case 1		Case 2		Case 3	
	Constant	Variational	Constant	Variational	Constant	Variational
$\Delta\vec{\rho}_{ij}$	linear	nonlinear	linear	linear	nonlinear	nonlinear
$\Sigma\vec{\rho}_{ij}$	linear	nonlinear	nonlinear	nonlinear	nonlinear	nonlinear

3. Anti-Spoofing Method

From the analysis in Section 2, it can be seen that when the two signals are spoofing signals, the PRD sequence $\Delta\vec{\rho}_{ij}$ is linear, while the PRS sequence $\Sigma\vec{\rho}_{ij}$ is nonlinear. In other cases, this characteristic is not satisfied. Accordingly, the detection result $\Delta\vec{\rho}_{ij}$ is linear and $\Sigma\vec{\rho}_{ij}$ is nonlinear, indicating that the signal i and the signal j are spoofing signals from the same spoofing source. Although no definite conclusion can be obtained from other detection results, all authentic signals and spoofing signals can still be distinguished with traversal detection.

The specific detection process includes the following two steps.

- ✧ Step 1: Randomly select two signals and use the proposed method to detect whether they are both spoofing signals. If yes, proceed to Step 2. If not, we will reselect two signals for detection until two spoofing signals are selected.
- ✧ Step 2: For the other signals, except the two spoofing signals, one of them is selected in turn to be jointly detected with any one of the spoofing signals.

For Step 2, on the premise that one signal is a spoofing signal, the proposed method can directly determine whether the other signal is an authentic signal or a spoofing signal. As a result, all authentic signals and spoofing signals can be judged.

The above spoofing detection process is represented with a flowchart, as shown in Figure 1. Next, this section will introduce the detection method of the linearities of PRD sequence $\Delta\vec{\rho}_{ij}$ and PRS sequence $\Sigma\vec{\rho}_{ij}$ involved in the spoofing detection process.

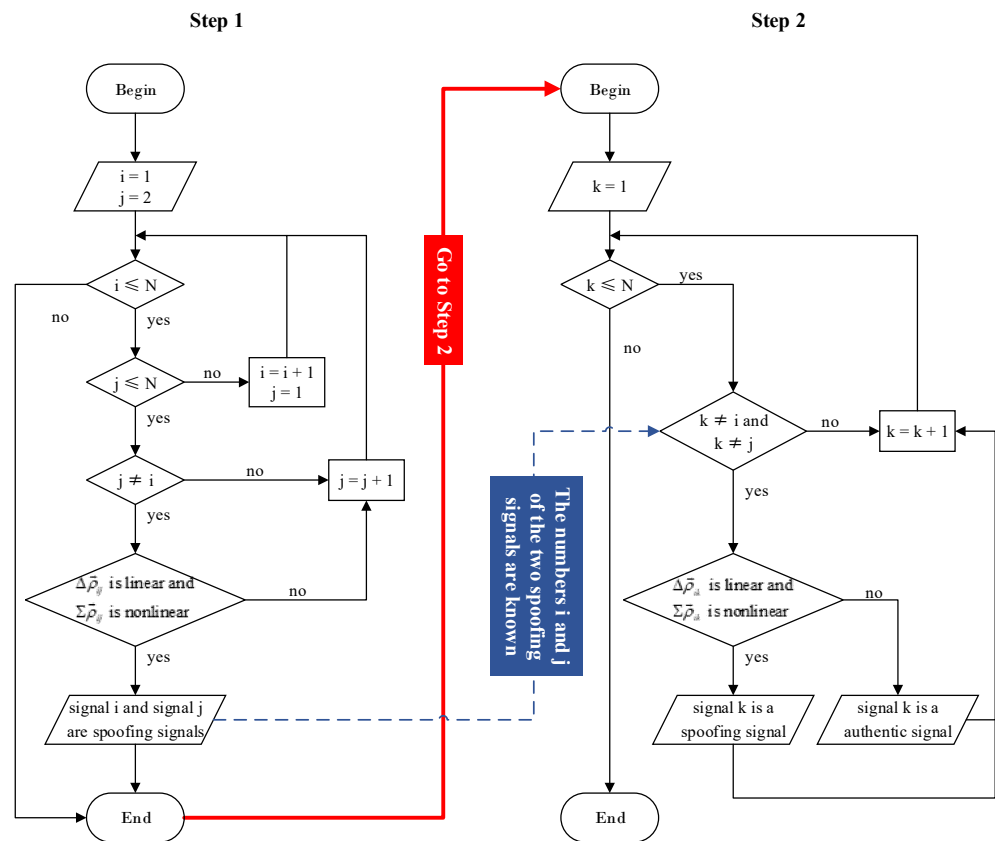


Figure 1. Flowchart corresponding to spoofing detection process.

3.1. PRD Sequence Linearity Detection

In the linearity detection of the PRD sequence, two hypotheses for PRD sequence $\Delta\vec{\rho}_{ij}$ are as follows:

$$\begin{cases} H_{\Delta,0} : \Delta\vec{\rho}_{ij} \text{ is nonlinear} \\ H_{\Delta,1} : \Delta\vec{\rho}_{ij} \text{ is linear} \end{cases} \quad (12)$$

For $\Delta\vec{\rho}_{ij}$, we can calculate its least square linear regression model:

$$\Delta\hat{\rho}_{ij}(k) = \hat{a}_{\Delta,ij} \times k + \hat{b}_{\Delta,ij}, \quad (13)$$

where $\hat{a}_{\Delta,ij}$ and $\hat{b}_{\Delta,ij}$ are the estimated model parameters and $\Delta\hat{\rho}_{ij}(k)$ represents the estimated value of $\Delta\rho_{ij}(k)$ obtained with a linear model.

Under the $H_{\Delta,0}$ hypothesis, $\Delta\rho_{ij}(k)$ can be expressed as

$$\Delta\rho_{ij}(k) = g_{\Delta,ij}(k) + w_{\Delta,0}(k), \quad (14)$$

where $g_{\Delta,ij}(k)$ represents a nonlinear equation and $w_{\Delta,0}(k)$ is Gaussian white noise. The variance of $w_{\Delta,0}(k)$ is σ_{ij}^2 :

$$\sigma_{ij}^2 = \sigma_i^2 + \sigma_j^2. \quad (15)$$

σ_i^2 and σ_j^2 denote the pseudo-range measurement noise variance of the signal i and the signal j , respectively. In this case, the difference between the actual value and the estimated value $\Delta x_{ij}(k)$ can be deduced as follows:

$$\begin{aligned} \Delta x_{ij}(k) &= \Delta\rho_{ij}(k) - \widehat{\Delta\rho}_{ij}(k) \\ &= (g_{\Delta,ij}(k) + w_{\Delta,0}(k)) - \left(\widehat{a}_{\Delta,ij} \times k + \widehat{b}_{\Delta,ij} \right) \\ &= \mu_{\Delta,ij}(k) + w_{\Delta,0}(k) \end{aligned} \quad (16)$$

Therefore, $\Delta x_{ij}(k)$ obeys the Gaussian distribution with mean value $\mu_{\Delta,ij}(k)$ and variance σ_{ij}^2 .

Under the $H_{\Delta,1}$ hypothesis, $\Delta\rho_{ij}(k)$ can be expressed as

$$\Delta\rho_{ij}(k) = a_{\Delta,ij} \times k + b_{\Delta,ij} + w_{\Delta,1}(k), \quad (17)$$

where $a_{\Delta,ij}$ and $b_{\Delta,ij}$ are model parameters, $w_{\Delta,1}(k)$ is Gaussian white noise, and its variance is also σ_{ij}^2 . Thus, the difference between the actual value and the estimated value $\Delta x_{ij}(k)$ can be deduced as follows:

$$\begin{aligned} \Delta x_{ij}(k) &= \Delta\rho_{ij}(k) - \widehat{\Delta\rho}_{ij}(k) \\ &= (a_{\Delta,ij} \times k + b_{\Delta,ij} + w_{\Delta,1}(k)) - \left(\widehat{a}_{\Delta,ij} \times k + \widehat{b}_{\Delta,ij} \right) \\ &= (a_{\Delta,ij} - \widehat{a}_{\Delta,ij}) \times k + (b_{\Delta,ij} - \widehat{b}_{\Delta,ij}) + w_{\Delta,1}(k) \\ &\approx w_{\Delta,1}(k) \end{aligned} \quad (18)$$

Compared with $w_{\Delta,1}(k)$, $a_{\Delta,ij} - \widehat{a}_{\Delta,ij}$ and $b_{\Delta,ij} - \widehat{b}_{\Delta,ij}$ are very small and can be ignored. Therefore, $\Delta x_{ij}(k)$ obeys the Gaussian distribution with zero mean and σ_{ij}^2 variance.

$\vec{\Delta x}_{ij} = [\Delta x_{ij}(0), \dots, \Delta x_{ij}(k), \dots, \Delta x_{ij}(K-1)]$ is called the fitting error sequence of the PRD sequence. The effect of linear fitting can be evaluated using the sum of squares of errors (SSE) between actual data and estimated data. The smaller the SSE, the better the linear fitting effect. Based on this, we construct the linearity detection statistic ΔT_{ij} corresponding to the PRD sequence:

$$\Delta T_{ij} = \frac{1}{K} \sum_{k=0}^{K-1} \Delta x_{ij}(k)^2 = \sum_{k=0}^{K-1} \left(\frac{\Delta x_{ij}(k)}{\sqrt{K}} \right)^2. \quad (19)$$

It can be proved that under the hypothesis of $H_{\Delta,0}$, ΔT_{ij} obeys the non-central chi-square distribution with the degree of freedom K and the non-central parameter $\lambda_{\Delta,ij}$. And under the $H_{\Delta,1}$ hypothesis, ΔT_{ij} obeys the central chi-square distribution with the degree of freedom K .

$$\begin{cases} H_{\Delta,0} : \Delta T_{ij} \sim \chi^2 \left(K, \lambda_{\Delta,ij}, \frac{\sigma_{ij}^2}{K} \right) \\ H_{\Delta,1} : \Delta T_{ij} \sim \chi^2 \left(K, 0, \frac{\sigma_{ij}^2}{K} \right) \end{cases}. \quad (20)$$

The non-central parameter $\lambda_{\Delta,ij}$ is as follows:

$$\lambda_{\Delta,ij} = \sum_{k=0}^{K-1} \left(\frac{\mu_{\Delta,ij}(k)}{\sqrt{K}} \right)^2 = \frac{1}{K} \sum_{k=0}^{K-1} (\mu_{\Delta,ij}(k))^2. \quad (21)$$

When the degree of freedom is large enough, the chi-square distribution can be approximately Gaussian distribution [26]. According to this characteristic of chi-square distribution, the distribution of ΔT_{ij} under the $H_{\Delta,0}$ hypothesis and the $H_{\Delta,1}$ hypothesis can be approximately expressed as

$$\begin{cases} H_{\Delta,0} : \Delta T_{ij} \sim \mathbb{N} \left(\sigma_{ij}^2 + \lambda_{\Delta,ij}, \frac{2\sigma_{ij}^4}{K} + \frac{4\sigma_{ij}^2}{K} \lambda_{\Delta,ij} \right) \\ H_{\Delta,1} : \Delta T_{ij} \sim \mathbb{N} \left(\sigma_{ij}^2, \frac{2\sigma_{ij}^4}{K} \right) \end{cases}. \quad (22)$$

Figure 2 shows the probability density function of the linearity detection statistic ΔT_{ij} under different hypotheses, where the solid lines are the theoretical curves calculated according to the Equation (22), and the star points are the statistical results obtained through 10,000 Monte Carlo random experiments. Figure 2a,b correspond to the $H_{\Delta,0}$ hypothesis, where their central parameters are $\lambda_{\Delta,ij} = 100$ and $\lambda_{\Delta,ij} = 200$, respectively, while Figure 2c corresponds to the $H_{\Delta,1}$ hypothesis. It can be found that the simulation results are very close to the theoretical results. Under the $H_{\Delta,1}$ hypothesis, ΔT_{ij} is closer to zero, and the smaller the noise variance and the longer the sequence length, the more concentrated the distribution of ΔT_{ij} . Under the $H_{\Delta,0}$ hypothesis, the mean and variance of ΔT_{ij} increase with the increase in central parameters.

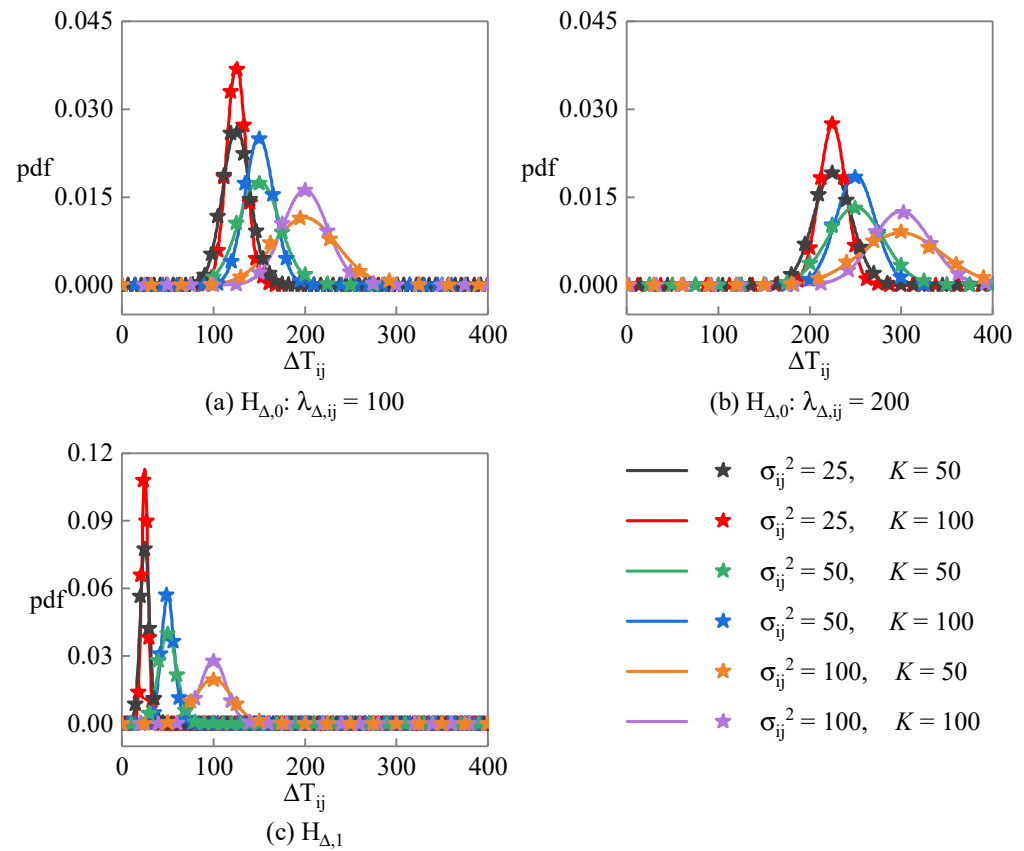


Figure 2. Probability density function of the linearity detection statistic corresponding to PRD sequence under different hypotheses.

3.2. PRS Sequence Linearity Detection

In the linearity detection of the PRS sequence, two hypotheses for PRS sequence $\vec{\rho}_{ij}$ are as follows:

$$\begin{cases} H_{\Sigma,0} : \vec{\rho}_{ij} \text{ is linear} \\ H_{\Sigma,1} : \vec{\rho}_{ij} \text{ is nonlinear} \end{cases} \quad (23)$$

Similarly, the difference between the actual value and the estimated value obtained with linear fitting $\vec{\rho}_{ij}$ is represented by $\Sigma x_{ij}(k)$. Under the $H_{\Sigma,0}$ hypothesis, $\Sigma x_{ij}(k)$ obeys the Gaussian distribution with zero mean and σ_{ij}^2 variance. Under the $H_{\Sigma,1}$ hypothesis, $\Sigma x_{ij}(k)$ obeys the Gaussian distribution with mean value $\mu_{\Sigma,ij}(k)$ and variance σ_{ij}^2 . $\Sigma \vec{x}_{ij} = [\Sigma x_{ij}(0), \dots, \Sigma x_{ij}(k), \dots, \Sigma x_{ij}(K-1)]$ is called the fitting error sequence of the PRS sequence. Constructing the linearity detection statistic ΣT_{ij} corresponding to the PRS sequence:

$$\Sigma T_{ij} = \frac{1}{K} \sum_{k=0}^{K-1} \Sigma x_{ij}(k)^2 = \sum_{k=0}^{K-1} \left(\frac{\Sigma x_{ij}(k)}{\sqrt{K}} \right)^2. \quad (24)$$

It can be proved that under the hypothesis of $H_{\Sigma,0}$, ΣT_{ij} obeys the central chi-square distribution with the degree of freedom K . And under the $H_{\Delta,1}$ hypothesis, ΣT_{ij} obeys the non-central chi-square distribution with the degree of freedom K and the non-central parameter $\lambda_{\Sigma,ij}$.

$$\begin{cases} H_{\Sigma,0} : \Sigma T_{ij} \sim \chi^2 \left(K, 0, \frac{\sigma_{ij}^2}{K} \right) \\ H_{\Sigma,1} : \Sigma T_{ij} \sim \chi^2 \left(K, \lambda_{\Sigma,ij}, \frac{\sigma_{ij}^2}{K} \right) \end{cases} \quad (25)$$

The non-central parameter $\lambda_{\Sigma,ij}$ is as follows:

$$\lambda_{\Sigma,ij} = \sum_{k=0}^{K-1} \left(\frac{\mu_{\Sigma,ij}(k)}{\sqrt{K}} \right)^2 = \frac{1}{K} \sum_{k=0}^{K-1} (\mu_{\Sigma,ij}(k))^2. \quad (26)$$

Combined with the previous analysis, when the degree of freedom is large enough, the chi-square distribution can be approximately Gaussian distribution. Therefore, the distribution of ΣT_{ij} under different hypotheses can be derived:

$$\begin{cases} H_{\Sigma,0} : \Sigma T_{ij} \sim \mathbb{N} \left(\sigma_{ij}^2, \frac{2\sigma_{ij}^4}{K} \right) \\ H_{\Sigma,1} : \Sigma T_{ij} \sim \mathbb{N} \left(\sigma_{ij}^2 + \lambda_{\Sigma,ij}, \frac{2\sigma_{ij}^4}{K} + \frac{4\sigma_{ij}^2}{K} \lambda_{\Sigma,ij} \right) \end{cases} \quad (27)$$

Figure 3 shows the probability density function of the linearity detection statistic ΣT_{ij} under different hypotheses, where the solid lines are the theoretical curves calculated according to the Equation (27), and the star points are the statistical results obtained through 10,000 Monte Carlo random experiments. Figure 3a corresponds to the $H_{\Sigma,0}$ hypothesis, while Figure 3b,c correspond to the $H_{\Sigma,1}$ hypothesis, where their central parameters are $\lambda_{\Sigma,ij} = 100$ and $\lambda_{\Sigma,ij} = 200$, respectively. It can be found that the simulation results are very close to the theoretical results. Under the $H_{\Sigma,0}$ hypothesis, ΣT_{ij} is closer to zero, and the smaller the noise variance and the longer the sequence length, the more concentrated the distribution of ΣT_{ij} . Under the $H_{\Sigma,0}$ hypothesis, the mean and variance of ΣT_{ij} increase with the increase in central parameters.

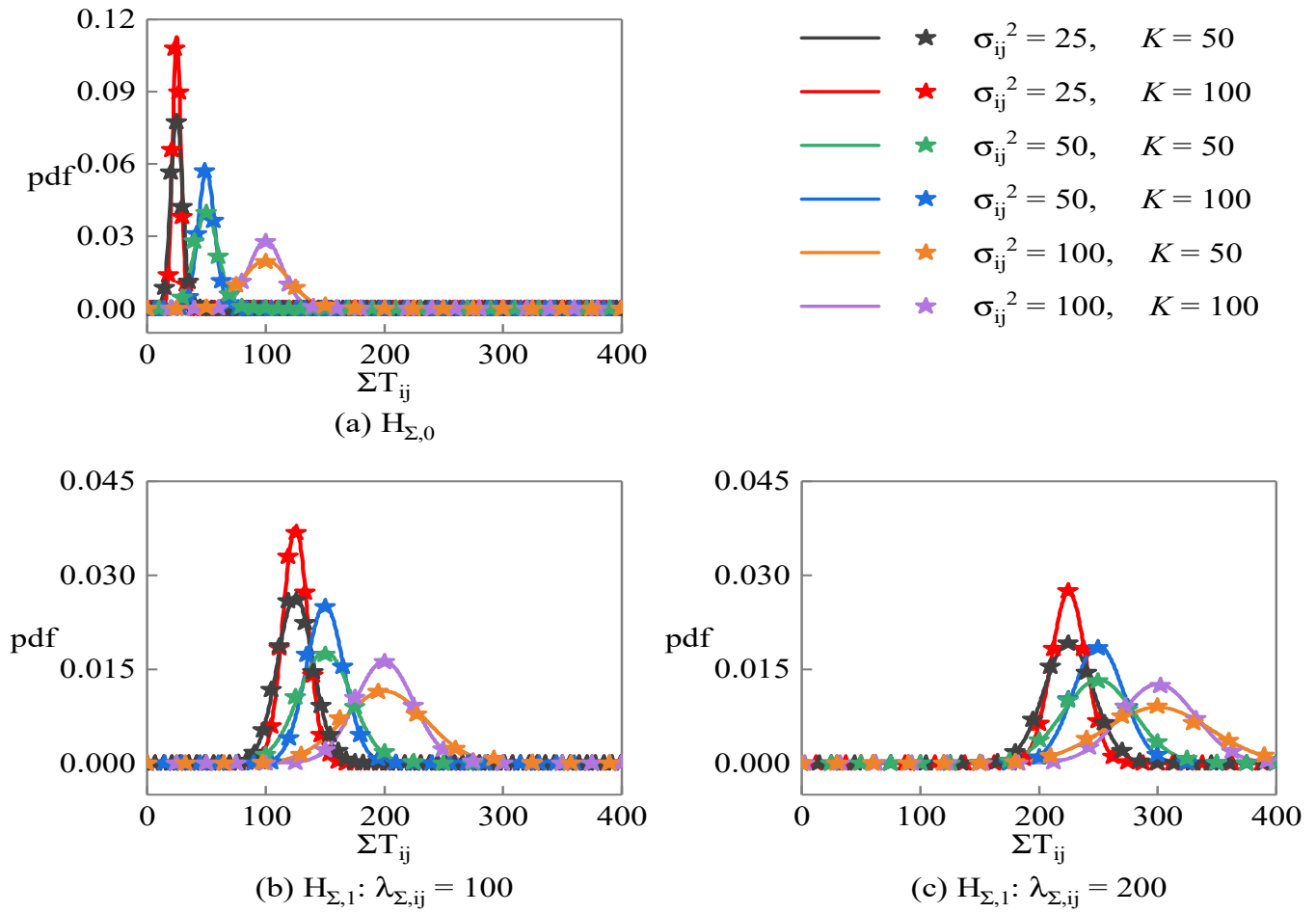


Figure 3. Probability density function of the linearity detection statistic corresponding to PRS sequence under different hypotheses.

3.3. Detection Performance Analysis

From the analysis in Section 2, it can be seen that the noise contained with the PRD $\Delta\rho_{ij}(k)$ is $\varepsilon_i(k) - \varepsilon_j(k)$, and the noise contained with PRS $\Sigma\rho_{ij}(k)$ is $\varepsilon_i(k) + \varepsilon_j(k)$. $\varepsilon_i(k)$ and $\varepsilon_j(k)$ are not correlated. Therefore, the variance of $\varepsilon_i(k) - \varepsilon_j(k)$ and $\varepsilon_i(k) + \varepsilon_j(k)$ is $\sigma_{ij}^2 = \sigma_i^2 + \sigma_j^2$. The correlation coefficient η_{ij} between them can be derived as

$$\eta_{ij} = \frac{\text{cov}(\varepsilon_i(k) - \varepsilon_j(k), \varepsilon_i(k) + \varepsilon_j(k))}{\sqrt{\text{var}(\varepsilon_i(k) - \varepsilon_j(k)) \cdot \text{var}(\varepsilon_i(k) + \varepsilon_j(k))}} = \frac{\sigma_i^2 - \sigma_j^2}{\sigma_i^2 + \sigma_j^2}. \quad (28)$$

When the pseudo-range measurement noise variances σ_i^2 and σ_j^2 are equal, the correlation coefficient is $\eta_{ij} = 0$, which means that the PRD sequence $\Delta\vec{\rho}_{ij}$ is not correlated with the noise contained in the PRS sequence $\Sigma\vec{\rho}_{ij}$. When $\sigma_i^2 \neq \sigma_j^2$, $\Delta\vec{\rho}_{ij}$ is correlated with the noise contained in $\Sigma\vec{\rho}_{ij}$, and the greater the difference between the two noise variances, the higher the correlation. Considering that the spoofing signals broadcast by the same spoofing source have similar power, to simplify the problem, it is assumed that the noises contained in $\Delta\vec{\rho}_{ij}$ and $\Sigma\vec{\rho}_{ij}$ are not correlated. That is to say, the detection of PRD sequence linearity is independent of the detection of PRS sequence linearity.

For the PRD sequence and PRS sequence linearity detection, since the noise variance is σ_{ij}^2 and the detection length is K , the same detection threshold γ can be set. In the linearity detection of the PRD sequence, the $H_{\Delta,0}$ hypothesis is considered to be valid when $\Delta T_{ij} > \gamma$,

and the $H_{\Delta,1}$ hypothesis is considered to be valid when $\Delta T_{ij} \leq \gamma$. Combined with the Equation (22), the false alarm probability $P_{\Delta,fa}$ and the detection probability $P_{\Delta,d}$ can be derived as follows:

$$\begin{cases} P_{\Delta,fa} = P(\Delta T_{ij} \leq \gamma | H_{\Delta,0}) \approx 1 - Q\left(\frac{\gamma - (\sigma_{ij}^2 + \lambda_{\Delta,ij})}{\sqrt{\frac{2\sigma_{ij}^4}{K} + \frac{4\sigma_{ij}^2}{K}\lambda_{\Delta,ij}}}\right) \\ P_{\Delta,d} = P(\Delta T_{ij} \leq \gamma | H_{\Delta,1}) \approx 1 - Q\left(\frac{\gamma - \sigma_{ij}^2}{\sqrt{\frac{2\sigma_{ij}^4}{K}}}\right) \end{cases} \quad (29)$$

where $Q(\cdot)$ is the right tail probability function. In the linearity detection of the PRS sequence, the $H_{\Sigma,0}$ hypothesis is considered to be valid when $\Sigma T_{ij} \leq \gamma$, and the $H_{\Sigma,1}$ hypothesis is considered to be valid when $\Sigma T_{ij} > \gamma$. Combined with the Equation (27), the false alarm probability $P_{\Sigma,fa}$ and the detection probability $P_{\Sigma,d}$ can be derived as follows:

$$\begin{cases} P_{\Sigma,fa} = P(\Sigma T_{ij} > \gamma | H_{\Sigma,0}) \approx Q\left(\frac{\gamma - \sigma_{ij}^2}{\sigma_{ij}^2 \sqrt{\frac{2}{K}}}\right) \\ P_{\Sigma,d} = P(\Sigma T_{ij} > \gamma | H_{\Sigma,1}) \approx Q\left(\frac{\gamma - (\sigma_{ij}^2 + \lambda_{\Sigma,ij})}{\sqrt{\frac{2\sigma_{ij}^4}{K} + \frac{4\sigma_{ij}^2}{K}\lambda_{\Sigma,ij}}}\right) \end{cases} \quad (30)$$

For the method proposed in this paper, the false alarm probability P_{fa} and detection probability P_d of joint detection can be expressed as

$$\begin{cases} P_{fa} = P(\Delta T_{ij} \leq \gamma \text{ and } \Sigma T_{ij} > \gamma | (H_{\Delta,0} \text{ or } H_{\Sigma,0})) \\ P_d = P(\Delta T_{ij} \leq \gamma \text{ and } \Sigma T_{ij} > \gamma | (H_{\Delta,1} \text{ and } H_{\Sigma,1})) \end{cases} \quad (31)$$

Since it is assumed that the PRD sequence linearity detection is independent of the PRS sequence linearity detection, P_{fa} and P_d can be further derived:

$$\begin{aligned} P_{fa} &= P(\Delta T_{ij} \leq \gamma | H_{\Delta,0}) \cdot P(\Sigma T_{ij} > \gamma | H_{\Sigma,0}) + P(\Delta T_{ij} \leq \gamma | H_{\Delta,1}) \cdot P(\Sigma T_{ij} > \gamma | H_{\Sigma,0}) \\ &\quad + P(\Delta T_{ij} \leq \gamma | H_{\Delta,0}) \cdot P(\Sigma T_{ij} > \gamma | H_{\Sigma,1}) \\ &= P_{\Delta,fa} \cdot P_{\Sigma,fa} + P_{\Delta,d} \cdot P_{\Sigma,fa} + P_{\Delta,fa} \cdot P_{\Sigma,d} \end{aligned} \quad (32)$$

$$P_d = P(\Delta T_{ij} \leq \gamma | H_{\Delta,1}) \cdot P(\Sigma T_{ij} > \gamma | H_{\Sigma,1}) = P_{\Delta,d} \cdot P_{\Sigma,d} \quad (33)$$

The false alarm probability P_{fa} and detection probability P_d of joint detection corresponding to the detection threshold γ in different scenes are shown in Figure 4. Compared with the Figure 4a,b, the increase in noise variance makes P_{fa} higher and P_d lower. Compared with the Figure 4a,c, the reduction in sequence length makes P_{fa} higher and P_d lower. Compared with the Figure 4a,d, the decrease in non-central parameter $\lambda_{\Delta,ij}$ makes P_{fa} increase, and P_d remains unchanged. Compared with the Figure 4a,e, the decrease in non-central parameter $\lambda_{\Sigma,ij}$ reduces P_{fa} and P_d .

The lower the false alarm probability and the higher the detection probability, the better the detection performance. Furthermore, we count the difference $P_d - P_{fa}$ between the detection probability and the false alarm probability corresponding to the detection threshold γ in different scenes, as shown in Figure 5. It is not difficult to find from the figure that the smaller the noise variance, the longer the sequence length, and the larger the non-central parameters $\lambda_{\Delta,ij}$ and $\lambda_{\Sigma,ij}$, the better the detection performance.

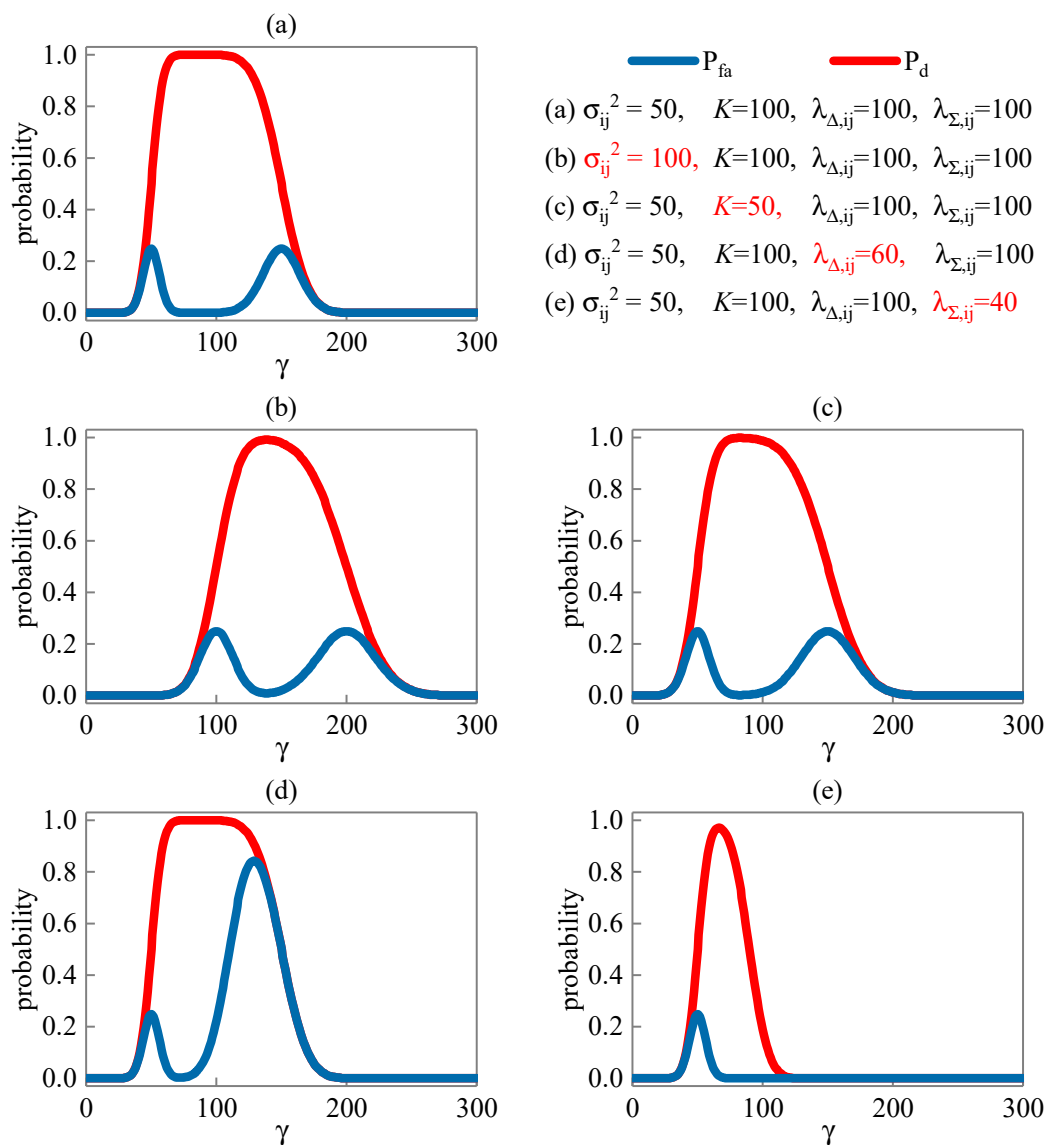


Figure 4. False alarm probability and detection probability corresponding to detection threshold.

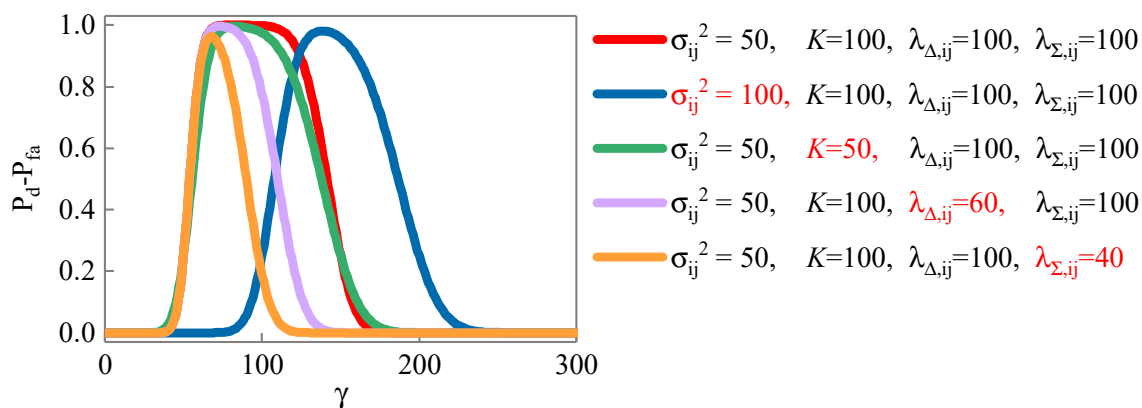


Figure 5. Difference between detection probability and false alarm probability corresponding to detection threshold.

4. Simulation Results and Analysis

In this section, the feasibility of the method will be verified with simulation tests. Simulation scenes are divided into the uniform motion scene and the circular motion scene, as shown in Figure 6. The authentic signals and spoofing signals in the two scenes are generated with the GNSS signal source simulator, sampled and stored in signal memory, and then processed with the GNSS software receiver.

The number of test signals is 8, in which the PRNs of authentic signals are 2, 11, 14, and 21, and the PRNs of spoofing signals are 5, 10, 16, and 33. The standard deviation of the pseudo-range measurement error of all signals is set to 3 m. This assumption implies that the noise variance of PRD and PRS for any two signals is 18. The receiver tracks the collected signals and obtains the measured pseudo-range sequence with the sequence length $K = 120$ and the time interval $\Delta t = 0.1$ s. The difference between two measurement pseudo-range sequences is selected to form a PRD sequence, and the sum forms a PRS sequence. Each PRD sequence and PRS sequence is linearly fitted to obtain fitting error sequences, and the detection statistics are obtained by statistics. The detection threshold $\gamma = 30$. For this threshold, the probability that the sequence is linear but the detection result is nonlinear will be less than 0.001%.

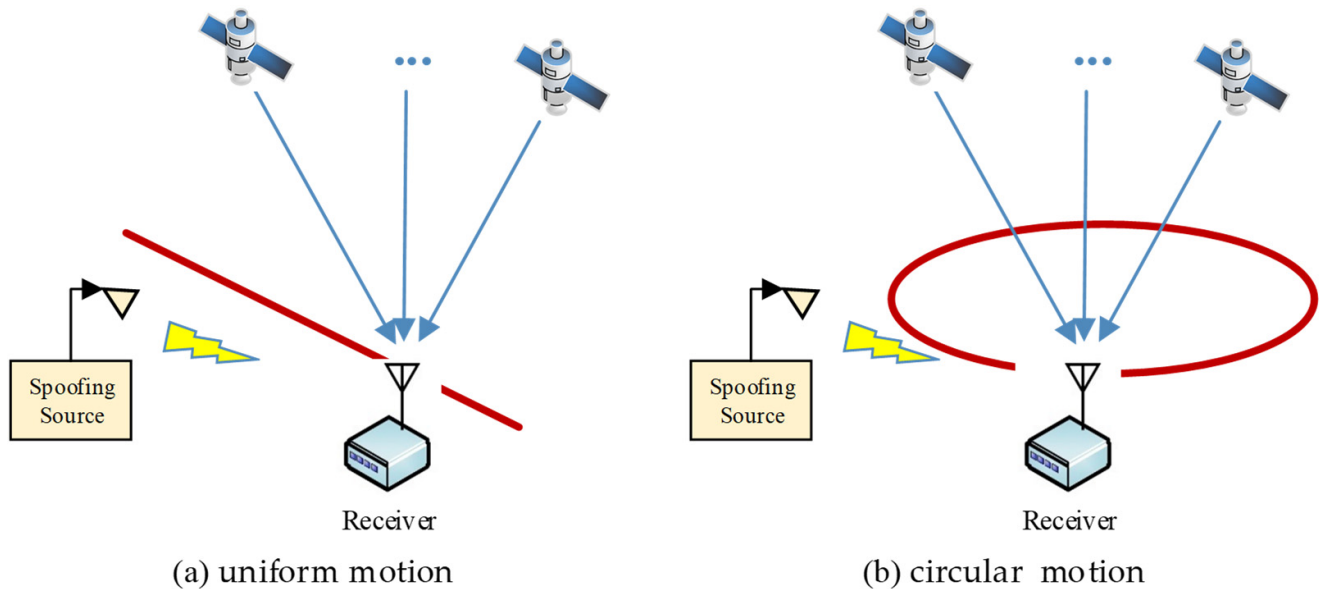


Figure 6. Two simulation scenes.

4.1. Uniform Motion Scene Test

In the uniform motion scene test, the distance between the spoofing source and the target receiver is 1000 m at 0 time, and the speed of the receiver is 40 m/s. The fitting error sequences $\Delta \vec{x}_{ij}$ and $\Sigma \vec{x}_{ij}$ correspond to the PRD sequence and the PRS sequence, and the linearity detection statistics ΔT_{ij} and ΣT_{ij} obtained by statistics are shown in Figure 7. In the case of two authentic signals, as shown in Figure 7a, both ΔT_{ij} and ΣT_{ij} are below the threshold. For the case of one authentic signal and one spoofing signal, as shown in Figure 7c, both ΔT_{ij} and ΣT_{ij} are above the threshold. For the case of two spoofing signals, as shown in Figure 7b, $\Delta T_{ij} \leq \gamma$ and $\Sigma T_{ij} > \gamma$ are satisfied. The simulation results are consistent with the analysis results, which show that the proposed method can detect spoofing signals in uniform motion scenes.

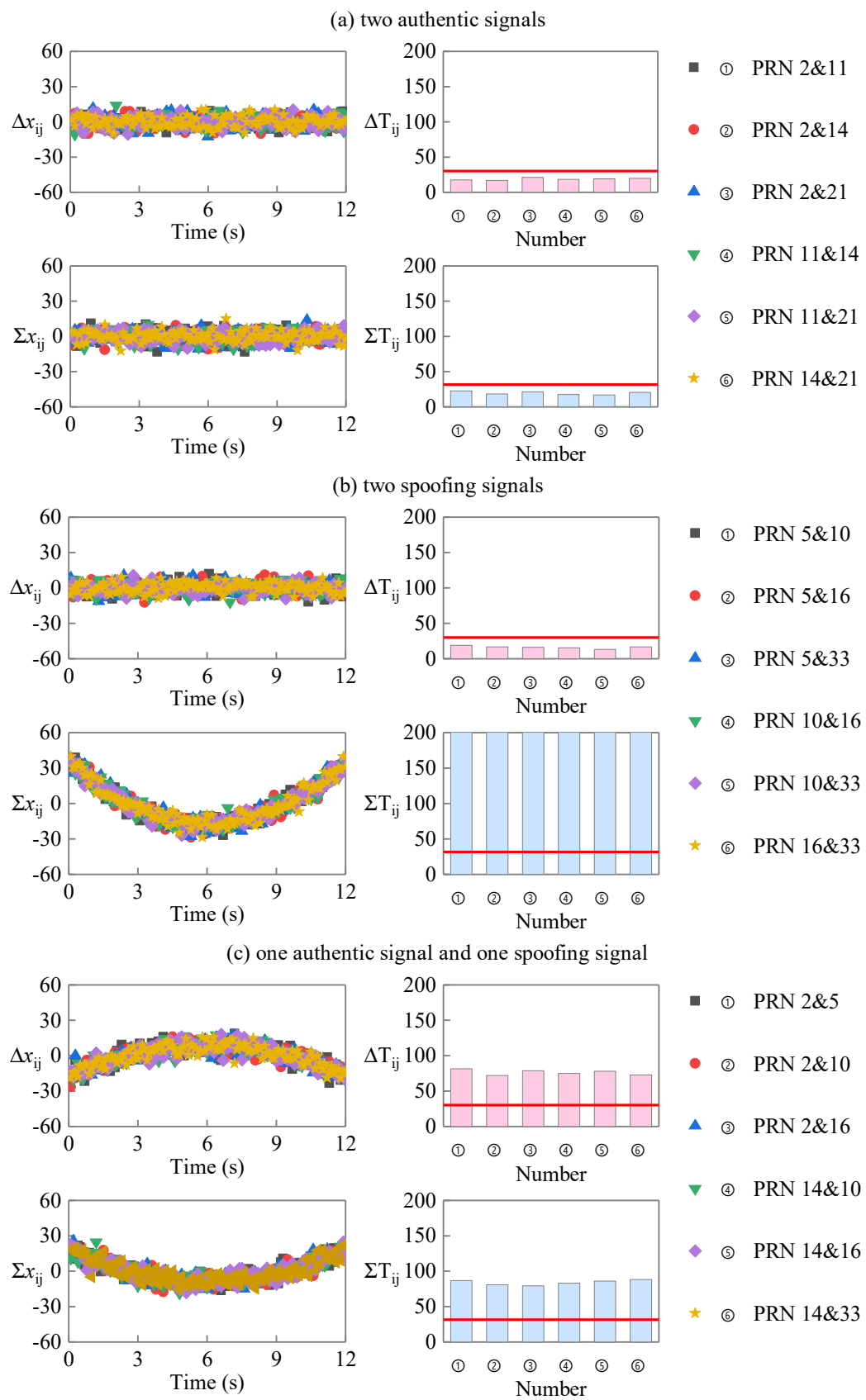


Figure 7. Fitting error sequences and detection statistics in the uniform motion scene.

4.2. Circular Motion Scene Test

In the circular motion scene test, the distance between the spoofing source and the target receiver is 1000 m at 0 time, the speed of the receiver is 40 m/s, and the circumference radius is 300 m. The fitting error sequences $\Delta \vec{x}_{ij}$ and $\Sigma \vec{x}_{ij}$ correspond to the PRD sequence and the PRS sequence, and the linearity detection statistics ΔT_{ij} and ΣT_{ij} obtained with the test are shown in Figure 8. In the case of two authentic signals, as shown in Figure 8a, both ΔT_{ij} and ΣT_{ij} are above the threshold. For the case of one authentic signal and one spoofing signal, as shown in Figure 8c, both ΔT_{ij} and ΣT_{ij} are above the threshold. For the case of two spoofing signals, as shown in Figure 8b, $\Delta T_{ij} \leq \gamma$ and $\Sigma T_{ij} > \gamma$ are satisfied. The simulation results are consistent with the analysis results, which show that the proposed method can detect spoofing signals in variable motion scenes.

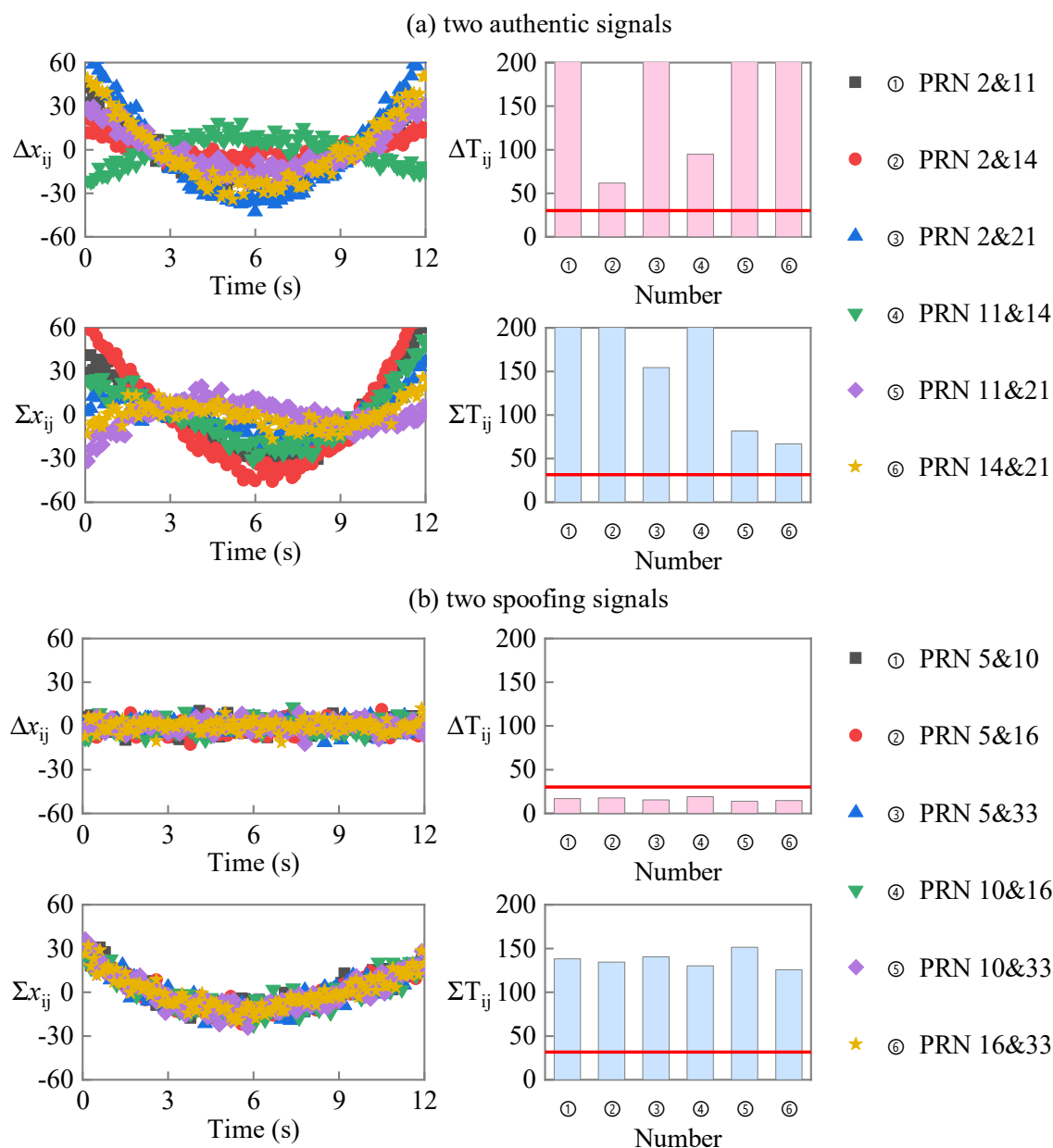


Figure 8. Cont.

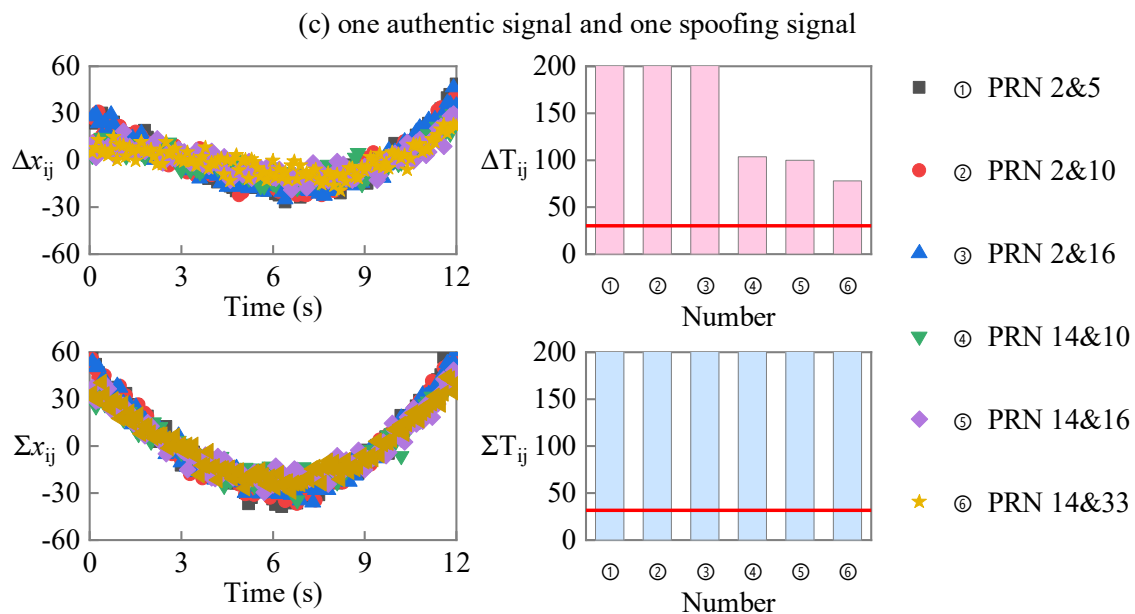


Figure 8. Fitting error sequences and detection statistics in the circular motion scene.

5. Conclusions

Aiming at single spoofing interference, this paper proposes an anti-spoofing method based on the joint monitoring of the PRD sequence and the PRS sequence linearity, which changes the spoofing detection problem into the sequence linearity detection problem. The detection statistics are constructed based on the SSE of linear fitting of the PRD sequence and PRS sequence. When the sequence length is large enough, the detection statistics approximately obey the Gaussian distribution. The influence of noise variance, sequence length, and non-central parameters on the detection performance of the method is analyzed. It can be concluded that the smaller the noise variance, the longer the sequence length, and the larger the non-central parameters, the better the detection performance. In addition, the feasibility of the method is verified by simulation tests. Simulation results show that this method can detect spoofing interference and distinguish authentic signals from spoofing signals in both uniform motion scenes and variable motion scenes. This is the premise of improving the security and availability of GNSS in the presence of spoofing interference.

The proposed method is low complexity because it only requires pseudo-range information and does not need to modify the baseband processing of the receiver. Nevertheless, the precondition for the effectiveness of the method is that the spoofing source is stationary, and the additional component of the spoofing source to any signal is linearly varying. In addition, this paper lacks an exploration of the influence of receiver motion on non-central parameters, which makes it impossible to establish a direct relationship between receiver motion and detection performance. Our future work will focus on these two aspects to improve.

Author Contributions: Conceptualization, X.Z. and T.L.; methodology, X.Z.; software, T.L., J.W. and C.W.; validation, X.Z.; formal analysis, X.Z.; investigation, X.Z. and M.C.; resources, J.T.; data curation, X.Z.; writing, X.Z.; visualization, M.C.; supervision, J.T.; project administration, T.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the CAEP Foundation under Grant CX20200010.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned aircraft capture and control via GPS spoofing. *J. Field Robot.* **2014**, *31*, 617–636. [\[CrossRef\]](#)
2. Bhatti, J.; Humphreys, T.E. Hostile control of ships via false GPS signals: Demonstration and detection. *Navigation* **2017**, *64*, 51–66. [\[CrossRef\]](#)
3. Han, S.; Chen, L.; Meng, W.; Li, C. Improve the Security of GNSS Receivers Through Spoofing Mitigation. *IEEE Access* **2017**, *5*, 21057–21069. [\[CrossRef\]](#)
4. Grant, A.; Williams, P.; Ward, N.; Basker, S. GPS Jamming and the Impact on Maritime Navigation. *J. Navig.* **2009**, *62*, 173–187. [\[CrossRef\]](#)
5. Ioannides, T.; Pany, T.; Gibbons, G. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. *Proc. IEEE* **2016**, *104*, 1174–1194. [\[CrossRef\]](#)
6. Chen, F.; Nie, J.; Ni, S.; Li, Z.; Wang, F. Combined algorithm for interference suppression and signal acquisition in GNSS receivers. *Electron. Lett.* **2017**, *53*, 274–275. [\[CrossRef\]](#)
7. Warner, J.S.; Johnston, R.G. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. *J. Secur. Adm.* **2002**, *25*, 19–27.
8. Shepard, D.P.; Humphreys, T.E.; Fansler, A.A. Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 146–153. [\[CrossRef\]](#)
9. Schmidt, D.; Radke, K.; Camtepe, S. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Comput. Surv.* **2016**, *48*, 1–31. [\[CrossRef\]](#)
10. Yang, H.; Jin, R.; Xu, W.; Che, L.; Zhen, W. Satellite Navigation Spoofing Interference Detection and Direction Finding Based on Array Antenna. *Sensors* **2023**, *23*, 1604. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Tu, J.; Zhan, X.; Zhang, X.; Zhang, Z.; Jing, S. Low-complexity GNSS anti-spoofing technique based on Doppler frequency difference monitoring. *IET Radar Sonar Navig.* **2018**, *12*, 1058–1065. [\[CrossRef\]](#)
12. Tao, H.; Wu, H.; Li, H.; Lu, M. GNSS Spoofing Detection Based on Consistency Check of Velocities. *Chin. J. Electron.* **2019**, *28*, 218–225. [\[CrossRef\]](#)
13. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 observables. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 181–191. [\[CrossRef\]](#)
14. Ali, P.; Ali, B.; Lachapelle, G. Characterization of Signal Quality Monitoring Techniques for Multipath Detection in GNSS Applications. *Sensors* **2017**, *17*, 1579.
15. Psiaki, M.L.; Humphreys, T.E. GNSS spoofing and detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [\[CrossRef\]](#)
16. Montgomery, P.Y.; Humphreys, T.E.; Ledvina, B.M. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In Proceedings of the International Technical Meeting of The Institute of Navigation, Anaheim, CA, USA, 26–28 January 2009; pp. 124–130.
17. Montgomery, P.Y.; Humphreys, T.E.; Ledvina, B.M. A multi-antenna defense: Receiver autonomous GPS spoofing detection. *Inside GNSS* **2009**, *4*, 40–46.
18. Swaszek, P.F.; Hartne, R.J. Spoof detection using multiple COTS receivers in safety critical applications. In Proceedings of the ION GNSS+, Nashville, TN, USA, 16–20 September 2013; pp. 2921–2930.
19. Swaszek, P.F.; Richard, J.H. A multiple COTS receiver GNSS spoof detector-extensions. In Proceedings of the International Technical Meeting of The Institute of Navigation, San Diego, CA, USA, 27–29 January 2014; pp. 316–326.
20. Axell, E.; Larsson, E.G.; Persson, D. GNSS spoofing detection using multiple mobile COTS receivers. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Process (ICASSP), Brisbane, Australia, 19–24 April 2015; pp. 3192–3196.
21. Radin, S.D.; Swaszek, P.F.; Seals, K.C. GNSS spoof detection based on pseudo-ranges from multiple receivers. In Proceedings of the International Technical Meeting of The Institute of Navigation, Dana Point, CA, USA, 26–28 January 2015; pp. 657–671.
22. Nielsen, J.; Broumandan, A.; Lachapelle, G. GNSS spoofing detection for single antenna handheld receivers. *Navigation* **2011**, *58*, 335–344. [\[CrossRef\]](#)
23. Broumandan, A.; Jafarnia-Jahromi, A.; Dehghanian, V. GNSS spoofing detection in handheld receivers based on signal spatial correlation. In Proceedings of the IEEE/ION Position Location and Navigation Symposium (PLANS), Myrtle Beach, SC, USA, 24–26 April 2012; pp. 479–487.
24. Broumandan, A.; Jafarnia-Jahromi, A.; Lachapelle, G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solut.* **2014**, *19*, 475–487. [\[CrossRef\]](#)
25. Hesselbarth, A.; Wanninger, L. Short-term stability of GNSS satellite clocks and its effects on precise point positioning. In Proceedings of the ION GNSS, Savannah, GA, USA, 16–19 September 2008; pp. 1855–1863.
26. Szilárd, A.; Árpád, B. Properties of the probability density function of the non-central chi-squared distribution. *J. Math. Anal. Appl.* **2008**, *346*, 395–402.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.