Received: 9 April 2021 | Revised: 12 October 2021 | Accepted: 11 November 2021

DOI: 10.33012/navi.511

ORIGINAL ARTICLE

A Flexible GNSS Spoofer Localization System: Spoofing Discrimination and Localization Method

Jian Wen | **Hong Li** | **Mingquan Lu**

Department of Electronic Engineering, Beijing National Research Center for Information Science and Technology (BNRist), Tsinghua University, Beijing 100084, China

Correspondence
Hong Li
Room 1002, Weiqing Building, Tsinghua University, Beijing 100084, China
Email: lihongee@tsinghua.edu.cn

Abstract

Global navigation satellite systems (GNSS) are vulnerable to spoofing attacks. To shut down a spoofer, it is necessary to locate the spoofer first. Many spoofer localization systems use long cables for the synchronization of multiple receivers. However, a flexible spoofer localization system free from cables is sometimes essential so the receivers can move freely and are flexible to deploy. This paper solves two major problems in developing such a system: spoofing discrimination without requiring synchronization and having an effective method using asynchronous raw measurements with no other assistance. First, this paper proposes to use the extended pseudorange double-difference method to discriminate spoofing signals. The performance is then analyzed and the effectiveness is verified. Then, a quasi-synchronization spoofer localization method (QSSL) is proposed, and it is verified that its localization performance can attain the Cramer-Rao lower bound. Above all, a field experiment demonstrates the effectiveness of the proposed methods and the feasibility of such system.

Keywords

GNSS, multiple receivers, spoofing discrimination, spoofer localization, TDOA

1 | INTRODUCTION

Global navigation satellite systems (GNSS) can provide position and timing information and is widely utilized in modern life. However, the security and reliability of GNSSs have been challenged by spoofing attacks recently (Humphreys et al., 2008). Civil GNSS signals are very weak when arriving at the surface of the Earth, and their structures are public. These two facts make spoofing attacks feasible. The field tests in Bhatti and Humphreys (2017), Kerns et al. (2014), and Psiaki and Humphreys (2016a) demonstrate that, due to spoofing, GNSS users can derive falsified position and timing solutions without awareness.

1.1 | Spoofing Detection Techniques

In order to alarm victimized GNSS users, spoofing detection techniques have been studied extensively (Günther, 2014; Jafarnia-Jahromi, 2013; Jafarnia-Jahromi et al., 2012; Psiaki & Humphreys, 2016b).

Navigation message authentication (NMA) is a very effective way to defend against spoofing attacks (Borio & Gioia, 2016; Günther, 2014). This technique needs to generate and broadcast cryptographic digital signatures by satellites, making the signal difficult to counterfeit by an unauthorized spoofer (Kerns et al., 2014). Generally, new satellites have to be launched to implement this new function.

While NMA is not yet available, a single-antenna standalone receiver can defend against spoofing by detecting anomalies in signal features, such as abnormal signal power (Akos, 2012), inconsistency between code-based and carrier-based measurements (Chu et al., 2018), distortion of correlation peaks (Pini et al., 2011), or conflict with spatial information from a moving antenna (Broumandan et al., 2016; Wang et al., 2017). Moreover, one can use external information that is not affected by GNSS spoofing. Tanil et al. (2018) proposed a monitor using inertial measurement units (IMUs) to detect GNSS spoofing. Other external information sources include an altimeter, cellular network, ground-based positioning system, and so on (Borio & Gioia, 2016).

Besides single-antenna standalone receivers, researchers also make use of multiple antennas or receivers. In Heng et al. (2015) and Psiaki et al. (2013), the signals from two separated receivers were cross-correlated to detect the absence of encrypted military signals, which would indicate a spoofing attack. Swaszek et al. (2013) monitored if the positioning results of two separated receivers abnormally overlapped each other. In Borio and Gioia (2016), Jafarnia-Jahromi et al. (2014), and Psiaki et al. (2014), double antennas were used to calculate carrier-phase differences for spoofing detection. This method was based on the assumption that spoofing signals come from the same antenna and travel through the same path to a victim receiver, while authentic satellite signals do not. Similarly, Wang et al. (2018) made use of signal power measurements to detect spoofing, and Zhang and Zhan (2018) and our previous work (Wen et al., 2019) utilized code-based measurements.

1.2 | Spoofer Localization

Spoofing detection techniques offer active resistance to spoofing for some users, but leave innocent users exposed to danger. Therefore, for the purpose of shutting down spoofers, research must take a step forward and aim to locate such spoofers.

There are two types of spoofer localization techniques. The first one, proposed by Shang et al. (2020), uses only one receiver, which is a major advantage. However, this technique can only deal with a meaconer, which is supposed to record and replay the satellite signals with relatively unchanged delay to produce unbiased spoofer position estimations. In contrast, the other type is based on a localization system that consists of several distributed sensors and uses received signal strength (RSS), angle of arrival (AOA), time of arrival (TOA), time difference of arrival (TDOA), frequency difference of arrival (FDOA) or a combination of the above to locate a signal source (Dempster & Cetin, 2016). This type is more general and has the potential to deal with various spoofers. Since it is easy to get time information from spoofing signals, related works (Bhamidipati & Gao, 2019; Broumandan et al., 2015; Gamba et al., 2016) adopted GNSS receivers as sensors and TOA or TDOA techniques to achieve spoofer localization.

There are two requirements for TOA or TDOA techniques (Dempster & Cetin, 2016). One is high-quality synchronization of sensors, and in Bhamidipati and Gao (2019) and Gamba et al. (2016), long cables were employed for synchronization. The other requirement is that the positions of sensors must be known. Both Gamba et al. (2016) and Bhamidipati and Gao (2019) used static sensors with

predetermined positions. However, Broumandan et al. (2015) proposed a different method. First, the signals received by sensors were classified into an authentic group or spoofing group. Then, the position and local time of each sensor were estimated using authentic signals, and all sensors could be synchronized with GNSS time using local time estimations. Therefore, the stated two requirements could be fulfilled. However, the signal classification process in Broumandan et al. (2015) was based on the carrier-phase double-difference method and still requires synchronization of sensors with cables according to Broumandan et al. (2015) and Wang et al. (2018).

Although cables provide precise synchronization, they also limit the application of a localization system. In fact, cables are not necessary for locating a spoofer. Without cables, the sensors can move freely, and a flexible spoofer localization system can be built. Such a system has the potential to track a mobile spoofer, or be implemented on cellular networks or future vehicle networks for finding spoofers in a vast area.

The spoofing discrimination methods based on standalone receivers need no cables, but they can hardly judge whether the spoofing signals received by different receivers are from the same spoofer or not. However, the spoofing discrimination methods based on multiple receivers have the potential to fulfill this function, and this function is important for localization. Moreover, although the two requirements for TDOA or TOA techniques can be fulfilled using authentic GNSS signals, both sensor position and synchronization are inaccurate. To deal with the inaccuracy, Wang and Ho (2013) proposed a closed-form multistage weighted least squares (WLS) algorithm when each sensor had at least one synchronous peer. Zou and Liu (2020) used semidefinite programming methods when an emitter for calibration was available. However, both methods remain relatively complicated and need additional assistance like a synchronous peer or calibration emitter. The method proposed by Broumandan et al. (2015) needs no additional assistance, but the measurements from different sensors are asynchronous, which need to be synchronized before they can be used for localization, and Broumandan et al. (2015) can only fulfill measurement synchronization once every sensor receives at least four consistent spoofing signals.

Therefore, to establish a flexible spoofer localization free from long cables, the first problem to deal with is spoofing discrimination without requiring the synchronization of multiple sensors. Then, another problem is the localization method for estimating spoofer position using asynchronous measurements without additional assistance.

For the first problem, a competitive solution is the code-based *pseudorange double difference* (PrDD) method proposed in our previous work (Wen et al., 2019). However, the PrDD method is based on merely two receivers, and authentic signals are easily misjudged as spoofing signals under unfavorable relative geometry. In this paper, since more receivers are available for a spoofer localization system, we propose an extended PrDD method that cross-checks the PrDD results of different receiver pairings. Stenberg et al. (2020) also extended carrier-phase and pseudorange double-difference methods, but they still required synchronous multiple receivers. Our extended PrDD method does not need the synchronization of receivers and shows a greatly improved performance, which makes a flexible spoofer localization system possible. The feasibility and superiority of the extended PrDD method will be demonstrated by simulations and a field experiment.

For the second problem, in this paper, we propose a *quasi-synchronization spoofer localization* (QSSL) method. This method can use asynchronous raw measurements of GNSS signals to form quasi-synchronized TDOA measurements, and then solve

TDOA equations using an iterative WLS algorithm to estimate spoofer position. Theoretical analysis and simulation results verify that its localization performance can attain the Cramer-Rao lower bound (CRLB). Compared with previous works, this method lifts the restriction on spoofing signals in Broumandan et al. (2015) and needs no additional assistance like Wang and Ho (2013) or Zou and Liu (2020).

In summary, the schematic diagram of a flexible spoofer localization system is shown in Figure 1. Several independent GNSS receivers are used as sensors, with one of them designated *central receiver*. All receivers can receive authentic satellite signals, and during a spoofing attack, receivers lying in the affected area will also receive spoofing signals. The receivers obtain raw measurements from both authentic and spoofing signals, including transmit time, pseudorange rate, pseudorandom noise (PRN) code number, carrier phase, and so on. Then, each receiver sends its raw measurements to the central receiver periodically via wireless links. These links are not required to be high-quality in order to be useful for precise synchronization, such as Wi-Fi network communication links, ad hoc peer-to-peer direct communication links, and so on. Afterward, the raw measurements are processed by the central receiver, and the central receiver then uses the extended PrDD method to discriminate spoofing signals from authentic ones, and locate the spoofer using the QSSL method.

This system works on some assumptions. First, as in Borio and Gioia (2016), Broumandan et al. (2015, 2016), Jafarnia-Jahromi et al. (2014), Psiaki et al. (2014), Wang et al. (2017, 2018), Wen et al. (2019), and Zhang and Zhan (2018), a spoofer usually spoofs more than one satellite to successfully deceive others, in which case the spoofing signals contain more than one PRN code and are transmitted by one antenna. Second, a spoofer usually stays stealthy and avoids transmitting signals with overwhelming power, in which case authentic signals are not jammed completely and can be processed by a receiver. Moreover, the total number of received

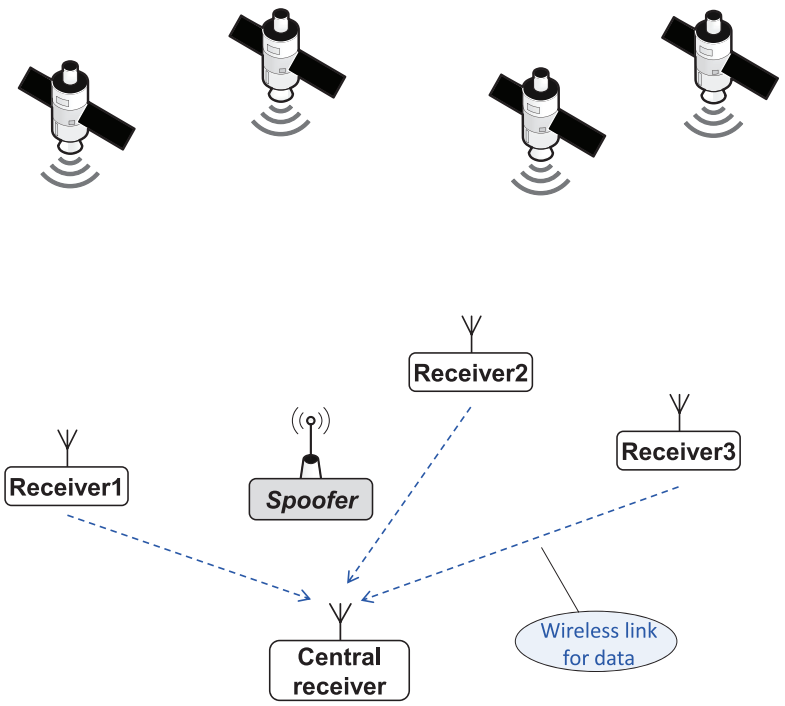


FIGURE 1 A schematic diagram of the spoofer localization system.

authentic signals by a receiver should be at least four. At last, the total number N of receivers that can receive spoofing signals satisfies $N \geq 4$. These assumptions, except the total number of authentic signals, coincide with Bhamidipati and Gao (2019), which also aims to locate spoofers.

1.3 | Our Contributions

In this paper, we aim to solve two major problems of a flexible spoofer localization system: spoofing discrimination without requiring synchronization and finding a localization method using asynchronous raw measurements without additional assistance. Contributions of this paper are summarized below.

- An extended PrDD method is proposed for discriminating spoofing signals. The performance of this method is analyzed, and the effectiveness is validated by simulations.
- A quasi-synchronization spoofer localization (QSSL) method is proposed. We theoretically analyze the spoofer localization performance and verify that the performance can attain the CRLB.
- A field experiment is conducted to demonstrate the effectiveness of the proposed methods and the feasibility of this flexible spoofer localization system.

The rest of this paper is organized as follows. Section 2 introduces the extended PrDD method and its performance analysis. Section 3 introduces the QSSL method and deduces the CRLB of the spoofer position estimator. In Section 4, two requisite functions are emphasized and explained briefly. Section 5 presents the field experiment results with discussion. At last, Section 6 draws some conclusions.

Notations: Throughout the whole paper, matrix and column vectors are denoted by bold uppercase and lowercase letters respectively, while a scalar uses an italic font. $[\cdot]^{\mathrm{T}}$ denotes the transpose of a matrix or vector. $[\cdot]_{n\times m}$ represents a matrix that has n rows and m columns. tr $\{\cdot\}$ stands for the trace of a square matrix. diag $\{\cdot\}$ represents a diagonal or a block diagonal matrix with its argument lying on the main diagonal in order. $||\cdot||$ is the Euclidean norm of its argument. Superscripts i and j denote the corresponding quantities are related to the i-th and j-th signals, and subscripts n and m denote the corresponding quantities are related to the n-th and m-th receivers ($n \geq 1$, $m \geq 1$). A quantity with a tilde represents a raw measurement, and a parameter with a hat represents an estimation or observation of the parameter.

2 | SPOOFING DISCRIMINATION

Before locating a spoofer, we need to discriminate spoofing signals from authentic ones. In this section, following an overview of the previous PrDD method, the extended PrDD method is introduced, and its performance is theoretically analyzed and validated by simulations.

2.1 | Overview of the PrDD Method

Suppose there are two receivers, and each can receive two signals identified by PRN code numbers. When the two receivers are synchronous, they can obtain raw

measurements of the signals at the same instant t' and produce a synchronous PrDD as:

$$\nabla\Delta\rho_{n,m}^{(i,j)}(t') = \left[\rho_n^{(i)}(t') - \rho_m^{(i)}(t')\right] - \left[\rho_n^{(j)}(t') - \rho_m^{(j)}(t')\right] \quad (1)$$

where $\rho(t)$ is pseudorange at the moment t.

If both signals are spoofing signals and transmitted from the same antenna, they have the same propagation path to each receiver, and $\nabla\Delta\rho_{n,m}^{(i,j)}(t')$ will be equal to zero. For example, in Figure 2, $\nabla\Delta\rho_{n,m}^{(i,j)}(t')$ of the two spoofing signals is equal to $[(d_1^{(3)} - d_2^{(3)}) - (d_1^{(4)} - d_2^{(4)})] = 0$, where $d_n^{(i)}$ is the real distance from the n-th receiver to the source of the i-th signal. Otherwise, if the two signals come from different sources, the propagation paths of the signals differ, and $\nabla\Delta\rho_{n,m}^{(i,j)}(t')$ can be other values besides zero. For example, in Figure 2, $\nabla\Delta\rho_{n,m}^{(i,j)}(t')$ of the two satellite signals is equal to $[(d_1^{(1)} - d_2^{(1)}) - (d_1^{(2)} - d_2^{(2)})]$, that of the first satellite signal and one of the spoofing signals is equal to $[(d_1^{(1)} - d_2^{(1)}) - (d_1^{(3)} - d_2^{(3)})]$, and both are not zero. Therefore, spoofing signals can be discriminated by the value of $\nabla\Delta\rho_{n,m}^{(i,j)}(t')$.

However, if the two receivers are asynchronous, they might obtain raw measurements of the signals at two different moments t'' and t', respectively. Then, an asynchronous direct PrDD is:

$$\nabla\Delta\rho_{n,m}^{(i,j)}(t'',t') = \rho_n^{(i)}(t'') - \rho_m^{(i)}(t') - \left[\rho_n^{(j)}(t'') - \rho_m^{(j)}(t')\right] \quad (2)$$

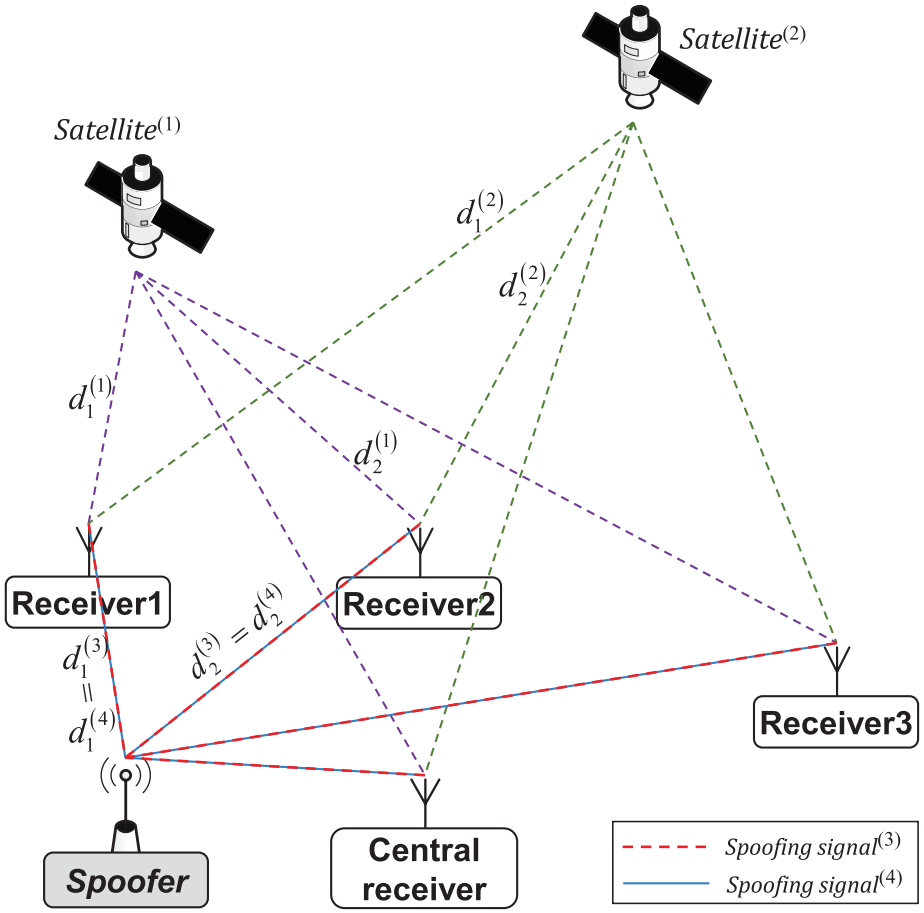


FIGURE 2 Paths of authentic signals and spoofing signals

As explained and demonstrated in our previous work (Wen et al., 2019), $\nabla\Delta\rho_{n,m}^{(i,j)}\left(t'',t'\right)$ needs correction to be useful for discriminating spoofing signals. The correction is approximating $\nabla\Delta\rho_{n,m}^{(i,j)}\left(t'\right)$ using $\nabla\Delta\rho_{n,m}^{(i,j)}\left(t'',t'\right)$ and pseudorange rate.

In practice, pseudoranges are usually measured by signal transmit time and local time as:

$$\hat{\rho}_n^{(i)} = c\cdot\left(t_n + \delta t_n - \tilde{\tau}_n^{(i)}\right) \tag{3}$$

where t_n is real receiver local time, δt_n is the receiver clock bias from reference time, $\tilde{\tau}$ is signal transmit time measurement, and c is the speed of light. Thus, convert pseudorange to signal transmit time, and the corrected asynchronous PrDD can be calculated by:

$$\begin{aligned}\nabla\Delta\hat{\rho}_{n,m}^{(i,j)}\left(t'',t'\right) = c\Big[&\tilde{\tau}_m^{(i)}\left(t'\right) - \tilde{\tau}_n^{(i)}\left(t''\right) - \tilde{\tau}_m^{(j)}\left(t'\right) + \tilde{\tau}_n^{(j)}\left(t''\right)\Big]\\ &+\tilde{\rho}_n^{(i)}\left(t''\right)\Big[\tilde{\tau}_m^{(i)}\left(t'\right) - \tilde{\tau}_n^{(i)}\left(t''\right)\Big]\\ &-\tilde{\rho}_n^{(j)}\left(t''\right)\Big[\tilde{\tau}_m^{(j)}\left(t'\right) - \tilde{\tau}_n^{(j)}\left(t''\right)\Big]\end{aligned} \tag{4}$$

where $\dot{\rho}(t)$ is the pseudorange rate at the moment t, and the last two lines are tire correction to $\nabla\Delta\rho_{n,m}^{(i,j)}\left(t'',t'\right)$. In Equation (4), $\nabla\Delta\hat{\rho}_{n,m}^{(i,j)}\left(t'',t'\right)$ is obtained using two common raw measurements: signal transmit time and pseudorange rate. The latter raw measurement comes from carrier frequency, and the relation between pseudorange rate and carrier Doppler shift is $\dot{\rho} = -c\cdot f_{\mathrm{D}}/(f_{\mathrm{T}} + f_{\mathrm{D}})$, where f_{D} denotes carrier Doppler shift and f_{T} is nominal carrier frequency of signal.

The formation of $\nabla\Delta\hat{\rho}_{n,m}^{(i,j)}\left(t'',t'\right)$ in Equation (4) is the same as Equation (12) of Wen et al. (2019), which is approximately equal to $\nabla\Delta\rho_{n,m}^{(i,j)}\left(t'\right)$ in Equation (1) and can be used to discriminate spoofing signals based on asynchronous receivers. A detailed derivation of Equation (4) can be found in Wen et al. (2019).

However, due to unfavorable relative geometry, a certain pair of authentic signals could be easily misjudged as spoofing signals. An example is shown in Figure 13(a) and explained in Section 5.1. Thus, to improve performance and make the PrDD method more practical, we extend the PrDD method by using more than two receivers.

2.2 | The Proposed Extended PrDD Method

In the spoofer localization system, at least four receivers are available, and it is natural to employ all of them to discriminate spoofing signals. More receivers mean that more spatial information can be obtained, which will improve the performance.

In practice, the central receiver collects periodic raw measurements from each peripheral receiver continuously, and calculates the PrDD for each pair of receivers and each pair of signals using Equation (4). Let $s_{n,m}^{(i,j)}[l] = \nabla\Delta\hat{\rho}_{n,m}^{(i,j)}(l\Delta t + t'', l\Delta t + t')$ for convenience, where l is an integer and Δt is the interval of two successive sets of measurements. As explained in Section 2.1 about Figure 2, for a pair of spoofing signals, the PrDD of all receiver pairings is equal to zero regardless of noise terms.

Consider two signals denoted by i and j. Based on Wen et al. (2019), when the receivers and spoofer are stationary, spoofing discrimination can be viewed as distinguishing between the two hypotheses:

$$\begin{cases} \mathcal{H}_0 : \forall\,(n,m) \in \mathbb{D}^2, s_{n,m}^{(i,j)}[l] = w_{n,m}^{(i,j)}[l] \\ \mathcal{H}_1 : \exists\,(n,m) \in \mathbb{D}^2, s_{n,m}^{(i,j)}[l] = a_{n,m}^{(i,j)} + b_{n,m}^{(i,j)} l + w_{n,m}^{(i,j)}[l] \end{cases} \tag{5}$$

where a and b are uncertain parameters that describe how s changes with time; w is the noise term, a random variable whose probability density function (PDF) is $\mathcal{N}(0, \sigma^2)$ with σ uncertain; $\mathbb{D} = \{1, 2, \cdots, N\}$ is a set of integers used for numbering the receivers; and $\mathbb{D}^2 = \{(n, m) \,|n \in \mathbb{D}, m \in \mathbb{D}, n < m\}$ is the set of all possible two-receiver combinations. $\mathcal{H}_0$ represents that both signals are spoofing signals, and $\mathcal{H}_1$ represents a situation in which at least one of the two signals is authentic. In other words, $\mathcal{H}_0$ means the total absence of authentic signals, and $\mathcal{H}_1$ means the presence of them. A similar design was also adopted by Broumandan et al. (2015), Borio and Gioia (2016), and Wang et al. (2018).

There are two situations under $\mathcal{H}_1$: both signals are authentic, or one signal is authentic and the other is spoofing. Since a satellite keeps moving and the motion is approximately linear in a short period of time, the PrDD under these two situations can be seen as changing linearly with time as described in Equation (5).

According to Kay (1998), given the unknown parameters a, b, and σ, a *generalized likelihood ratio test* (GLRT) approach is suitable to solve the binary hypothesis testing problem. Suppose there are $(2L + 1)$ available s[l] for each combination (n, m, i, j) and $l \in [-L, L]$, $L \geq 1$, a test statistic can be derived as:

$$T_{n,m}^{(i,j)}(\mathbf{s}) = \frac{2L-1}{2} \cdot \frac{\mathbf{s}^{\mathrm{T}}\mathbf{F}\left(\mathbf{F}^{\mathrm{T}}\mathbf{F}\right)^{-1}\mathbf{F}^{\mathrm{T}}\mathbf{s}}{\mathbf{s}^{\mathrm{T}}\left[\mathbf{I} - \mathbf{F}\left(\mathbf{F}^{\mathrm{T}}\mathbf{F}\right)^{-1}\mathbf{F}^{\mathrm{T}}\right]\mathbf{s}} \tag{6}$$

where:

$$\mathbf{s} = \left[s_{n,m}^{(i,j)}[-L], s_{n,m}^{(i,j)}[-L+1], \cdots, s_{n,m}^{(i,j)}[L]\right]^{\mathrm{T}} \tag{7}$$

$$\mathbf{F} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ -L & -L+1 & \cdots & L \end{bmatrix}^{\mathrm{T}} \tag{8}$$

and $\mathbf{I}$ is an identity matrix. To be clear, l is used to number the PrDD measurements, all of which in Equation (7) are from past time but not future. When a decision is to be made, the past $(2L + 1)$ PrDD measurements are collected as in Equation (7) and numbered from $-L$ to L.

For two signals denoted by (i, j), a test statistic is calculated using Equation (6) for each two-receiver combination. Then, for all possible receiver combinations, we compare all the test statistics with a threshold γ to make a decision on $\mathcal{H}_0$ or $\mathcal{H}_1$.

When signals i and j are both spoofing, $\forall(n,m) \in \mathbb{D}^2, T_{n,m}^{(i,j)}(\mathbf{s})$ is distributed as $F_{2,2L-1}$, an F distribution with 2 numerator degrees of freedom and $(2L - 1)$ denominator degrees of freedom. First, consider only two receivers, such as the n-th and m-th receivers. If $T_{n,m}^{(i,j)}(\mathbf{s}) < \gamma$, it will be decided that both signals are spoofing. Otherwise, an error will be made if $T_{n,m}^{(i,j)} \geq \gamma$, which can be seen as a false alarm of the presence of an authentic signal. We define the probability of such error as the probability of false alarm P_{FA}. Therefore, for a given P_{FA}, the threshold can be determined by:

$$\gamma = Q_{F_{2,2L-1}}^{-1}\left(P_{\mathrm{FA}}\right) \tag{9}$$

where $Q_F(\cdot)$ denotes the right-tail probability function of the corresponding F distribution, and $Q_F^{-1}(\cdot)$ is the inverse function. The right-tail probability function

equals one minus the cumulative distribution function (CDF). Then, the measurements provided by other receivers are used following the same rule. Finally, we decide on $\mathcal{H}_0$ if $\forall(n,m)\in\mathbb{D}^2, T_{n,m}^{(i,j)}(\mathbf{s})<\gamma$. Alternatively, an overall test statistic can be expressed as:

$$T^{(i,j)}=\max_{(n,m)\in\mathbb{D}^2}\left\{T_{n,m}^{(i,j)}\left(\mathbf{s}\right)\right\} \tag{10}$$

and decide $\mathcal{H}_0$ if $T^{(i,j)}<\gamma$.

The above rules show how to make a decision about either of the two signals, and the same rules should be followed for all possible signal combinations. Afterwards, all the signal combinations that lead to an $\mathcal{H}_0$ decision should be designated as spoofing signals, while the remainder of signals should be seen as authentic.

Since we need to test every signal combination one by one, it is necessary to evaluate the complexity of this method. For a given L, the matrix $\mathbf{F}$ can be seen as constant, and $\mathbf{F}(\mathbf{F^T F})^{-1}\mathbf{F^T}$ needs to be calculated only once. Besides, each element of $\mathbf{s}$ is calculated by Equation (4), of which the complexity is $\mathcal{O}(1)$. Therefore, the complexity of calculating test statistics using Equation (6) is $\mathcal{O}(L^2)$. Suppose there are in total M_{all} signals of each receiver to be tested, and then to finish the test we need to calculate Equation (6) for $\binom{N}{2}\binom{M_{\text{all}}}{2}=\frac{N(N-1)}{2}\frac{M_{\text{all}}(M_{\text{all}}-1)}{2}$ times. Therefore, the complexity of testing these signals is $\mathcal{O}\left(N^2M_{\text{all}}^2L^2\right)$.

2.3 | Performance Analysis and Simulation Results

Generally, for a given threshold γ, the probability of detection P_{D} can be used to evaluate the performance of the GLRT detector. P_{D} is defined as the probability of deciding $\mathcal{H}_1$ when $\mathcal{H}_1$ is true, which means a successful detection of the presence of an authentic signal. For two signals denoted by (i, j):

$$\begin{aligned}P_{\text{D}}&=1-P\left\{T^{(i,j)}<\gamma\middle|\mathcal{H}_1\right\}\\&=1-P\left\{\forall\left(n,m\right)\in\mathbb{D}^2, T_{n,m}^{(i,j)}\left(\mathbf{s}\right)<\gamma\middle|\mathcal{H}_1\right\}\end{aligned} \tag{11}$$

When $\mathcal{H}_1$ is true, $T_{n,m}^{(i,j)}(\mathbf{s})$ is distributed as $F'_{2,2L-1}(\lambda)$, a non-central F distribution with 2 numerator degrees of freedom, $(2L-1)$ denominator degrees of freedom, noncentrality parameter λ, and:

$$\lambda_{n,m}^{(i,j)}=\frac{\left(a_{n,m}^{(i,j)}\right)^2}{\left(\sigma_{n,m}^{(i,j)}\right)^2}\left(2L+1\right)+\frac{\left(b_{n,m}^{(i,j)}\right)^2}{\left(\sigma_{n,m}^{(i,j)}\right)^2}\sum_{l=-L}^{L}l^2 \tag{12}$$

Therefore, P_{D} is affected by λ and γ. More precisely, according to Equations (9) and (12), it is affected by the total number of used measurements $(2L+1)$, P_{FA}, and the three unknown parameters a, b, and σ. Among these factors, a and b are decided by two factors: time difference $t_{\text{B}}=t'-t''$, and the relative geometry of receivers, satellites, and spoofer. σ denotes the uncertainty of noise term w in Equation (5).

According to the model given in Equation (1), $w_{n,m}^{(i,j)}$ can be modeled as:

$$w_{n,m}^{(i,j)}=w_n^{(i)}-w_m^{(i)}-w_n^{(j)}+w_m^{(j)} \tag{13}$$

where $w_n^{(i)}=\hat{\rho}_n^{(i)}-\rho_n^{(i)}$ and the relatively small random errors in $\tilde{\rho}$ are ignored. Thus, there may be a correlation between two test statistics, such as $T_{1,2}^{(i,j)}(\mathbf{s})$ and

$T_{1,3}^{(i,j)}(\mathbf{s})$, since $w_{1,2}^{(i,j)}$ correlates with $w_{1,3}^{(i,j)}$. In consequence, it is very difficult to determine the probability in Equation (11) analytically or numerically, so we will use simulation results to evaluate P_{D} as proposed in Kay (1998).

First, a simulation is performed to show the influence of correlation. We take the Global Positioning System (GPS) L1 C/A code signal as an example. Suppose four receivers are placed as shown in Figure 3, forming a regular triangle with one of the receivers at the very center. The altitude is 100 meters, and Receiver 1 is placed at 116°E, 40°N. The distance between Receiver 1 and Receiver 2 is denoted by g. Assume the time is 5:30 on June 17, 2020 (GPS time). Ephemeris of a past time is public on the internet, and the positions of satellites in view can be calculated accordingly. We choose two satellites with the PRN code numbers of 1 and 22 and run Monte Carlo simulations for 10^5 times. The model in Equation (13) is used to add Gaussian noise to PrDD measurements, and we assume each term at the right side has independent and identical distribution in the simulation. Thus, when we set $\sigma_{n,m}^{(i,j)}$ to σ', the distribution of $w_n^{(i)}$ will be $\mathcal{N}\left(0,\frac{(\sigma')^2}{4}\right)$. Then, the correct GLRT decisions are counted, and the frequency of them is regarded as empirical P_{D}. The results are shown in Figure 4, and the empirical P_{D} is labeled as *Simulation*. If $T_{n,m}^{(i,j)}(\mathbf{s})$ in Equation (11) is assumed independent of each other, P_{D} will become:

$$\begin{aligned} P_{\mathrm{ind}} &= 1 - \prod_{(n,m)\in\mathbb{D}^2} P\left\{T_{n,m}^{(i,j)}(\mathbf{s}) < \gamma \middle| \mathcal{H}_1\right\} \\ &= 1 - \prod_{(n,m)\in\mathbb{D}^2} \left[1 - Q_{F'_{2,2L-1}\left(\lambda_{n,m}^{(i,j)}\right)}(\gamma)\right] \end{aligned} \tag{14}$$

the values of which are labeled as *Independence* in Figure 4. The results show that the correlation of test statistics would decrease P_{D} in this situation, compared with assumed independent test statistics. However, if at least one of the $\lambda_{n,m}^{(i,j)}$ is large enough, P_{D} will approximate one regardless of the correlation, such as the red dotted line with circle markers in Figure 4.

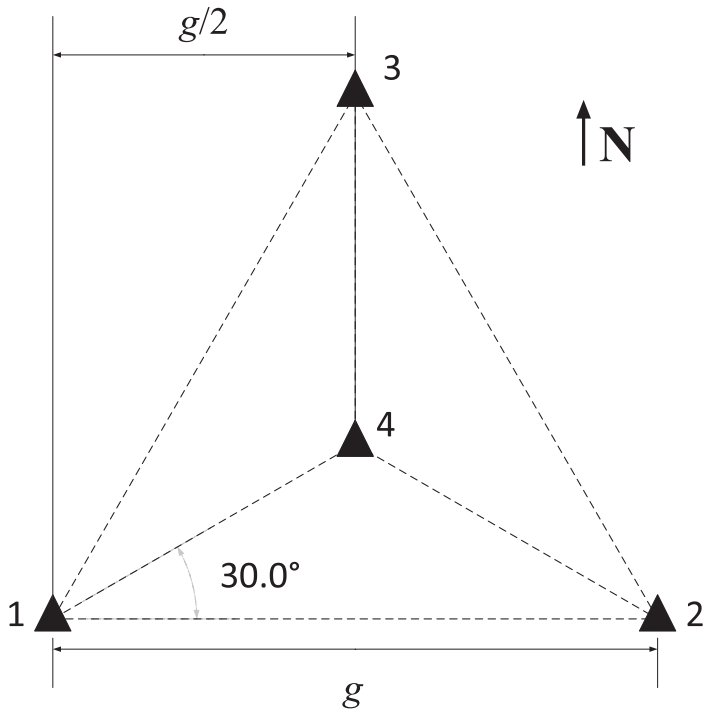


FIGURE 3 Receiver arrangements on the ground in the simulations

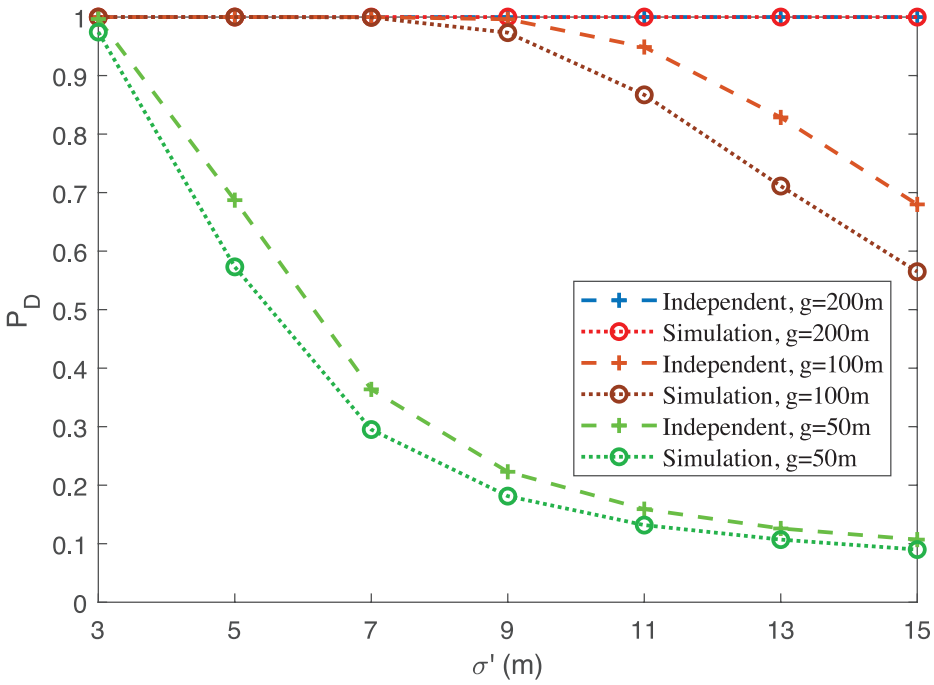


FIGURE 4 Comparison between P_{ind} and empirical P_{D}, when $P_{\text{FA}} = 0.01$, $L = 30$, and $t_{\text{B}} = 100$ ms

It should be noted that the probability P_{FA} in Equation (9) is not about the overall test statistic in Equation (10). It is about a two-receiver combination test statistic, and is used to determine the threshold γ. The overall probability of false alarm can be expressed as:

$$\begin{aligned} P'_{\text{FA}} &= 1 - P\left\{T^{(i,j)} < \gamma \middle| \mathcal{H}_0\right\} \\ &= 1 - P\left\{\forall (n,m) \in \mathbb{D}^2, T^{(i,j)}_{n,m}(\mathbf{s}) < \gamma \middle| \mathcal{H}_0\right\} \end{aligned} \tag{15}$$

Due to the correlation in Equation (13), it is also difficult to determine this probability analytically or numerically. Therefore, another simulation is carried out based on the settings in Figure 4. The model in Equation (13) is also used to produce the noise under $\mathcal{H}_0$, then count the incorrect GLRT decisions on $\mathcal{H}_1$, and use the frequency of these decisions as empirical P'_{FA}. By sliding the threshold γ in a certain range, we can get the results shown in Figure 5, which shows the overall detector operating characteristics in this specific situation.

As can be seen in Equation (11), the more usable receivers $\mathbb{D}$ includes, the more elements $\mathbb{D}^2$ has, and the larger P_{D} will be. Therefore, more simulations are run based on the simulations above to show to what degree an additional receiver can improve performance compared with two receivers, and moreover, how the factors mentioned above affect the performance. For a certain pair of signals, there are two situations under $\mathcal{H}_1$: both are authentic, or one is authentic and the other is spoofing. The simulations are based on these two situations, respectively.

In the following simulations, since P_{D} is affected by the relative geometry between satellites and receivers, we consider all possible signal combinations at a specific time, and the time is set to every 15 minutes from 00:00 through the whole day of June 17, 2020 (GPS time). Thus, there are in total 96 intervals, and each interval generates a group of PrDD measurements. We use the same method as above to add random noise, and run 2×10^5 times simulations for each PrDD measurement. Then, we count the correct GLRT decisions and treat the frequency as P_{D}. At last,

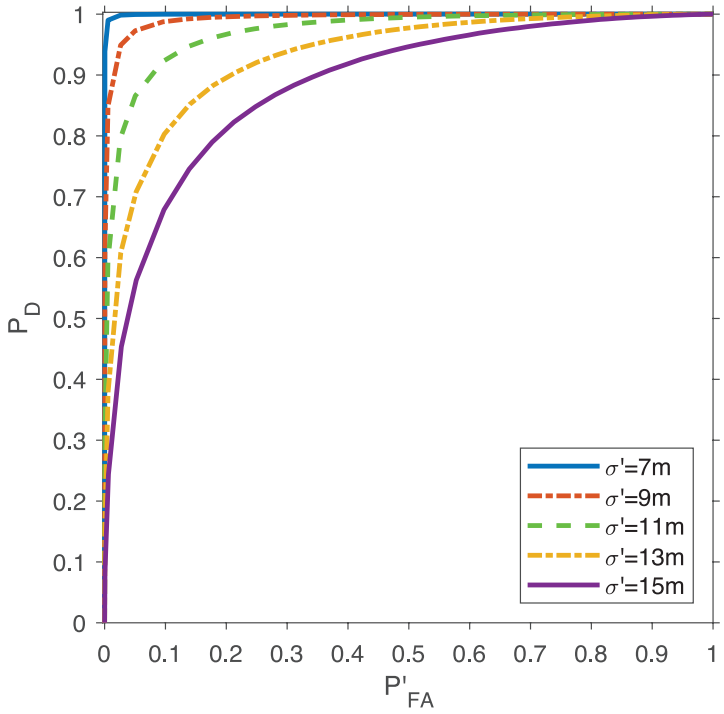


FIGURE 5 Overall detector operating characteristics, when $g = 100$ m, $L = 30$, and $t_B = 100$ ms

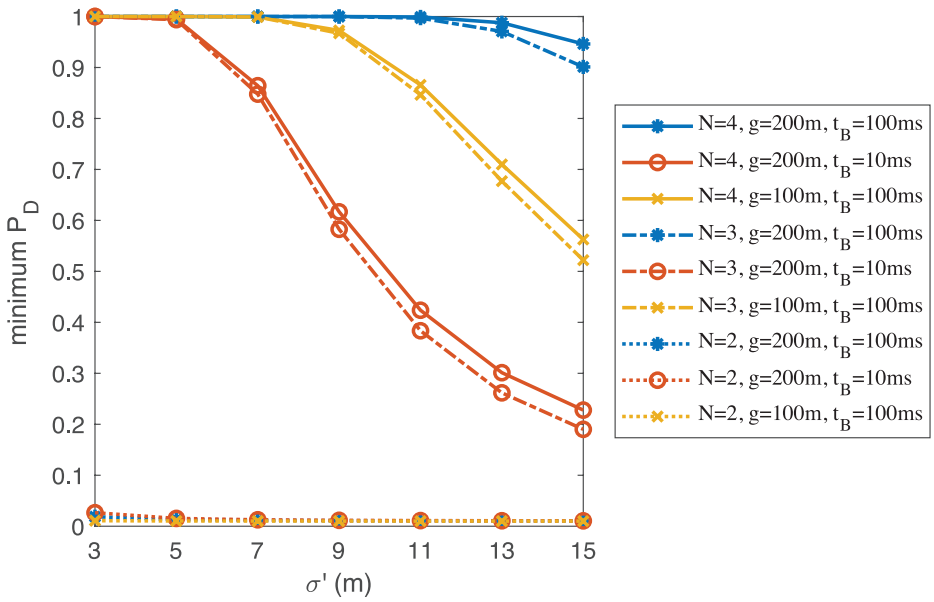


FIGURE 6 Minimum P_D during a whole day, while $P_{FA} = 0.01$ and $L = 30$, without spoofing signals

without loss of generality, we find the minimum P_D of the 96 groups of PrDD measurements to evaluate performance.

First, consider there is no spoofing attack, and all the signals that are received by the receivers are authentic. Under the conditions, set P_{FA} to 0.01 and L to 30, and then we get the results shown in Figure 6. There are nine curves in this figure, in the legend of which $N = 2$ means only Receiver 1 and Receiver 2 are used for simulation, i.e., $\mathbb{D} = \{1, 2\}$, $N = 3$ means $\mathbb{D} = \{1, 2, 3\}$, and $N = 4$ means $\mathbb{D} = \{1, 2, 3, 4\}$.

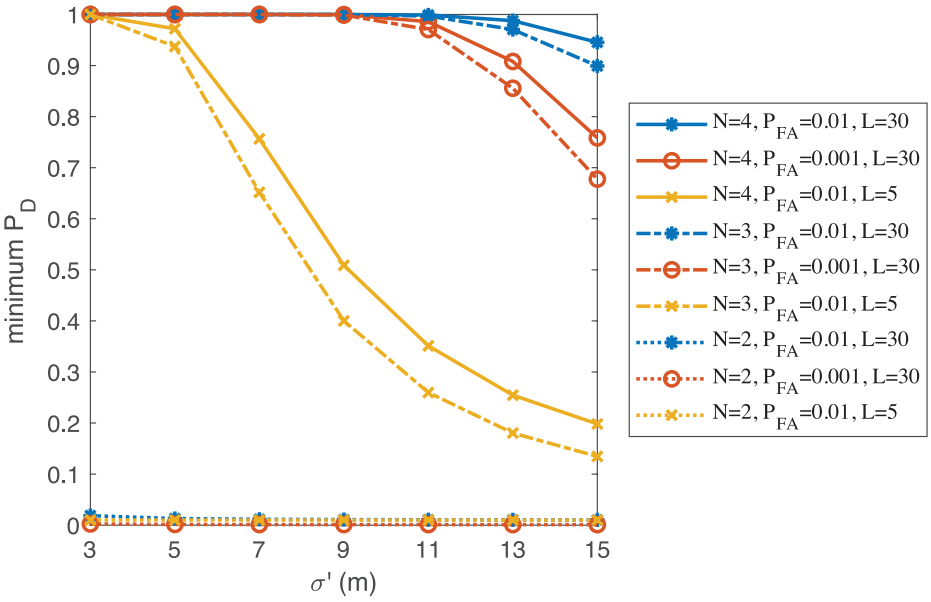


FIGURE 7 Minimum P_D during a whole day, while g = 200 m and t_B = 100 ms, without spoofing signals

While setting g to 200 m and t_B to 100 ms, simulation results are shown in Figure 7. When only two receivers are used, the minimum P_D is close to zero in all cases, which means there are always two authentic signals that will most possibly be misjudged as spoofing signals. However, when three or four receivers are used, the performance can be improved greatly, and especially, the blue curves with an asterisk marker show in that case that authentic signals can be correctly recognized with high confidence during the whole day. Besides, increasing L, g, or t_B is beneficial to improving performance. The influence of t_B is not readily intelligible, and a brief explanation is that, although t_B is usually not controllable, increasing t_B tends to magnify the double difference in satellite distances and thus leads to a bigger absolute value of the PrDD and a better performance.

Next, consider there is one spoofer. Generally, the spoofer position is unpredictable. We simply put the imaginary spoofer at 115.995°E and 39.995°N with an altitude of 150 m. The distance between the spoofer and Receiver 1 is about 700 m, and the elevation angle of the spoofer is about 4.07° from Receiver 1. The spoofer is assumed to replay the signals from GPS satellites without delay. Here, we only consider signal pairings that are composed of one authentic signal and one spoofing signal. Figure 8 shows the simulation results when we set P_{FA} to 0.01 and L to 30, and Figure 9 shows the results when g is set to 250 m and t_B = 100 ms. Similarly, the minimum P_D is also close to zero in all cases when using only two receivers, but using more receivers and increasing L or g still improves performance. However, in this situation, to attain comparable performance to that in Figure 6 and Figure 7, g has to be increased. Sometimes the direction of the spoofer is very similar to that of a certain satellite, and consequently, this method cannot distinguish the signal of this satellite from spoofing signals with full confidence, while two satellites typically do not have similar directions. The influence of g is much more significant in Figure 8, because the spoofer is much closer to the receivers than the satellites and increasing g greatly improves the relative geometry. However, increasing t_B does not yield any benefit for performance at all, because in that case, the difference in distances between this satellite and either of the two receivers is so close to that of the spoofer that there is little double difference to be magnified by t_B.

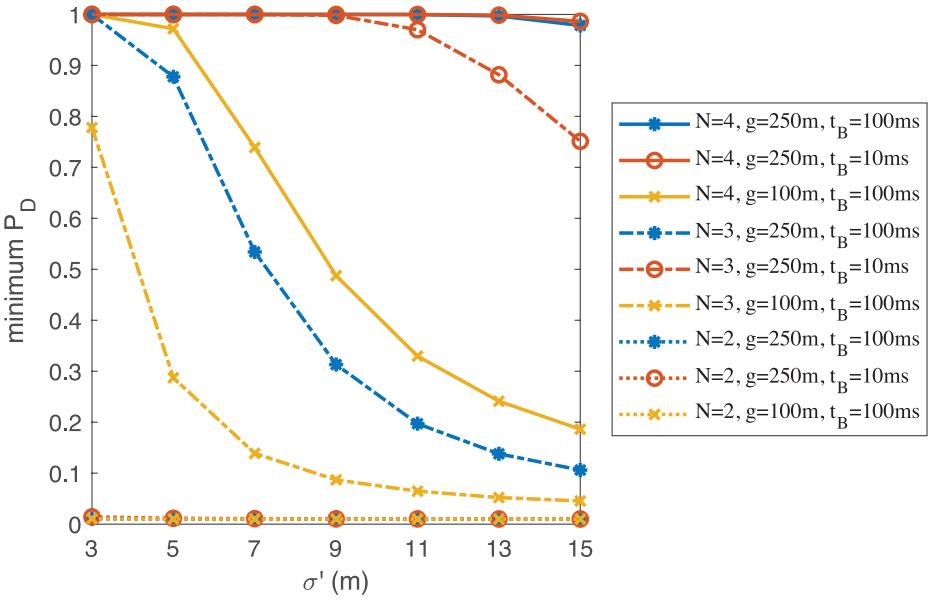


FIGURE 8 Minimum P_D during a whole day, while $P_{FA} = 0.01$ and $L = 30$, with spoofing signals

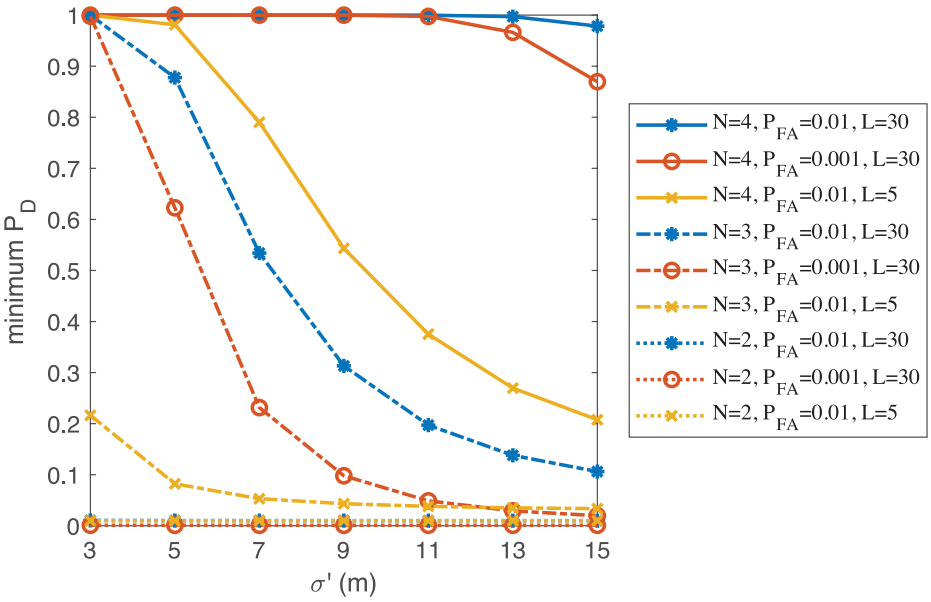


FIGURE 9 Minimum P_D during a whole day, while $g = 250$ m and $t_B = 100$ ms, with spoofing signals

Thus, to make better use of this method, it is suggested to use more receivers and increase the distance between them as much as possible. Besides, improving the accuracy of the measurements, i.e., decreasing σ, is certainly helpful.

In summary, by using multiple receivers, the extended PrDD method is superior to the previous PrDD method based on only two receivers. The simulation results show that this method can discriminate spoofing signals with high confidence at any point in a day. Furthermore, the effectiveness of this method has also been verified by a field experiment described later in Section 5.1.

3 | SPOOFER LOCALIZATION

After successfully discriminating spoofing signals from authentic signals using the extended PrDD method, the central receiver now knows which measurements are from spoofing signals and which measurements are from authentic signals, and then it can calculate spoofer position using the QSSL method.

The QSSL method takes the following steps. Since the position and local time of each receiver are still unknown, the first step of this method is to solve these unknown variables of each receiver using the measurements of authentic GNSS signals. Then, the second step is to estimate quasi-synchronized TDOA measurements using spoofing signals, which is to estimate distance differences from the spoofer to receivers. At last, the spoofer position can be estimated by solving the resulting TDOA equations using an iterative WLS algorithm.

In order to successfully accomplish the first step, each receiver needs to have the ability to process both spoofing and authentic signals, even if they have the same PRN code numbers. More details about this ability can be seen in Section 4. As is assumed at the end of Section 1.2, in the set of measurements from a receiver, at least four authentic signals are included. In other words, a receiver that captures less than four authentic signals is not usable in the following proposed spoofer localization process.

3.1 | The QSSL Method

Suppose there are N usable receivers, the unknown true position of the n-th receiver is $\mathbf{p}_n = [x_n, y_n, z_n]^{\mathrm{T}}$, $n = 1, 2, \cdots, N$, and a spoofer is located at $\mathbf{p}_0 = [x_0, y_0, z_0]^{\mathrm{T}}$. The distance of the spoofer from the n-th receiver is denoted by $r_n = \|\mathbf{p}_n - \mathbf{p}_0\|$, and the difference between r_n and r_m is denoted by $r_{n,m} = r_n - r_m$.

First, we use the raw measurements of authentic GNSS signals to estimate each receiver's position $\mathbf{p}_n$ and local time bias δt_n. According to Kaplan and Hegarty (2005) and later Xie (2009), this can be done by solving the equation:

$$\left\|\mathbf{p}_n - \mathbf{p}^{(i)}\right\| + c\delta t_n = \hat{\rho}_n^{(i)} \quad \left(n = 1, 2, \cdots, N\right) \tag{16}$$

where $\mathbf{p}^{(i)}$ denotes position of the i-th satellite and is regarded as precisely known from GNSS ephemeris. δt_n and $\hat{\rho}_n^{(i)}$ are defined in Equation (3), in which t_n and δt_n are not known, but $t_n + \delta t_n$ is known as biased local time. Thus, after solving Equation (16), we get unbiased estimations $\hat{\mathbf{p}}_n = \left[\hat{x}_n, \hat{y}_n, \hat{z}_n\right]^{\mathrm{T}}$ and $\delta\hat{t}_n$. Then, local time estimation of the n-th receiver is $\hat{t}_n = t_n + \delta t_n - \delta\hat{t}_n$.

Next, we must estimate the range difference $r_{n,m}$ between two receivers and the spoofer, which is to obtain TDOA measurements and transfer that TDOA data into a range difference. Since the receivers are not accurately synchronized, the raw measurements from different receivers may be obtained at different moments, but TDOA techniques require that the raw measurements be obtained at the same time. Thus, two special processes of raw measurements are needed. First, the pseudorange rate should be employed to transfer the difference of transmit time into a difference of distance. Second, the TDOA measurement needs to be synchronized using $\hat{t}_n$, and since $\hat{t}_n$ is inaccurate, the TDOA measurement is quasi-synchronized. Therefore, let the index n of the central receiver be one, and using the measurements of the i-th spoofing signal, $r_{n,1}$ can be estimated by:

$$\begin{aligned}\hat{d}_{n,1}^{(i)} &= \hat{d}_n^{(i)} - \hat{d}_1^{(i)} \\ &= \left[c - \tilde{\rho}_1^{(i)}\left(t_1\right)\right]\left(\hat{t}_n - \hat{t}_1\right) - c\left[\tilde{\tau}_n^{(i)}\left(t_n\right) - \tilde{\tau}_1^{(i)}\left(t_1\right)\right]\end{aligned} \tag{17}$$

The deduction of Equation (17) is given in Appendix A. Then, including the measurements of all the other spoofing signals, the final estimation of $\hat{r}_{n,1}$ is a weighted average of $\hat{d}_{n,1}^{(i)}$ as:

$$\hat{r}_{n,1} = \sum_i \alpha_n^{(i)} \hat{d}_{n,1}^{(i)} \tag{18}$$

where $\alpha_n^{(i)}$ is the positive weight determined by the covariance of all $\hat{d}_{n,1}^{(i)}$, and $\sum_i \alpha_n^{(i)} = 1$.

Here, the estimation $\hat{t}_n$ is seen as inaccurate since it has random errors in it. As is known, $\hat{t}_n$ can be as accurate as tens of nanoseconds. The random errors in $\hat{t}_n$ will go into $\hat{d}_{n,1}^{(i)}$ and then $\hat{r}_{n,1}$. Tens of nanoseconds multiplied by c mean several to more than ten meters in terms of length. Such a level of random errors cannot be neglected, especially when the spoofer is not as far from the receiver. However, an accurate synchronization achieved by long cables would not bring such random errors. Therefore, the TDOA measurement obtained above is called quasi-synchronized.

With all the prior estimations, including receiver positions $\hat{\mathbf{p}}_n$ and range differences $\hat{r}_{n,1}$, TDOA equations can be formed as:

$$\left\|\mathbf{p}_0 - \hat{\mathbf{p}}_n\right\| - \left\|\mathbf{p}_0 - \hat{\mathbf{p}}_1\right\| = \hat{r}_{n,1} \quad (n = 2, 3, \cdots, N) \tag{19}$$

If we have more than three equations, i.e., $N \geq 4$, an estimation $\hat{\mathbf{p}}_0$ of the unknown spoofer position $\mathbf{p}_0$ can be obtained by solving these equations. We make use of an iterative WLS algorithm as follows. First, we decide on an initial guess of spoofer position $\hat{\mathbf{p}}_0$. Second, we linearize Equation (19) by first-order Taylor series expansions about $\hat{\mathbf{p}}_0$, and the $(N-1)$ equations can be expressed in matrix form as $\mathbf{G}_0\Delta\mathbf{p} = \Delta\mathbf{r}$, where $\mathbf{G}_0$ is given in Equation (26), $\Delta\mathbf{r}$ is given in Equation (29), and $\Delta\mathbf{p} = \mathbf{p}_0 - \hat{\mathbf{p}}_0$. Third, estimate $\Delta\mathbf{p}$ as:

$$\Delta\hat{\mathbf{p}} = \left(\mathbf{G}_0^{\mathrm{T}}\mathbf{W}_0\mathbf{G}_0\right)^{-1}\mathbf{G}_0^{\mathrm{T}}\mathbf{W}_0\Delta\mathbf{r} \tag{20}$$

where $\mathbf{W}_0$ is a weighting matrix. Finally, we return to the second step, replace $\hat{\mathbf{p}}_0$ with $(\hat{\mathbf{p}}_0 + \Delta\hat{\mathbf{p}})$, iterate until convergence, at which point an estimation $\hat{\mathbf{p}}_0$ can be obtained. The mean square error (MSE) matrix is $\mathbf{MSE}(\hat{\mathbf{p}}_0) = \left(\mathbf{G}_0^{\mathrm{T}}\mathbf{W}_0\mathbf{G}_0\right)^{-1}$.

By now, the main purpose of locating the spoofer has been achieved. However, due to the existence of the spoofer, the previously obtained $\hat{\mathbf{p}}_n$ and $\delta\hat{t}_n$ can be refined by jointly solving Equation (16) and (19), which means to jointly estimate:

$$\boldsymbol{\theta} = \left[\mathbf{p}_0^{\mathrm{T}}, \boldsymbol{\theta}_{\mathrm{u}}^{\mathrm{T}}\right]^{\mathrm{T}} = \left[\mathbf{p}_0^{\mathrm{T}}, \mathbf{p}_1^{\mathrm{T}}, c\delta t_1, \mathbf{p}_2^{\mathrm{T}}, c\delta t_2, \cdots, \mathbf{p}_N^{\mathrm{T}}, c\delta t_N\right]^{\mathrm{T}} \tag{21}$$

Still, an iterative WLS algorithm is introduced. First, since we have got an estimation $\hat{\mathbf{p}}_0$ as well as $\hat{\mathbf{p}}_n$ and $\delta\hat{t}_n$, which can be denoted by:

$$\hat{\boldsymbol{\theta}} = \left[\hat{\mathbf{p}}_0^{\mathrm{T}}, \hat{\boldsymbol{\theta}}_{\mathrm{u}}^{\mathrm{T}}\right]^{\mathrm{T}} = \left[\hat{\mathbf{p}}_0^{\mathrm{T}}, \hat{\mathbf{p}}_1^{\mathrm{T}}, c\delta\hat{t}_1, \hat{\mathbf{p}}_2^{\mathrm{T}}, c\delta\hat{t}_2, \cdots, \hat{\mathbf{p}}_N^{\mathrm{T}}, c\delta\hat{t}_N\right]^{\mathrm{T}} \tag{22}$$

it is natural to use them as the initial guess. Second, linearize Equation (16) and (19) by first-order Taylor series expansions about $\hat{\boldsymbol{\theta}}$, and the equations can be expressed in matrix form as:

$$\mathbf{G}\Delta\boldsymbol{\theta} = \Delta\mathbf{d} \tag{23}$$

where:

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 & \mathbf{G}_{0,1} & \mathbf{G}_{0,2} & \cdots & \mathbf{G}_{0,N} \\ & \mathbf{G}_1 & & & \\ & & \mathbf{G}_2 & & \\ & & & \ddots & \\ & & & & \mathbf{G}_N \end{bmatrix} \tag{24}$$

$$\Delta\mathbf{d} = \left[\Delta\mathbf{r}^{\mathrm{T}}, \Delta\boldsymbol{\rho}_1^{\mathrm{T}}, \Delta\boldsymbol{\rho}_2^{\mathrm{T}}, \cdots, \Delta\boldsymbol{\rho}_N^{\mathrm{T}}\right]^{\mathrm{T}} \tag{25}$$

and $\Delta\boldsymbol{\theta} = \boldsymbol{\theta} - \hat{\boldsymbol{\theta}}$. Let $[\cdot]_k$ represent the k-th row of a matrix or the k-th element of a column vector. Then, when $1 \le k \le (N-1)$:

$$\left[\mathbf{G}_0\right]_k = \frac{\left(\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_{k+1}\right)^{\mathrm{T}}}{\left\|\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_{k+1}\right\|} - \frac{\left(\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_1\right)^{\mathrm{T}}}{\left\|\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_1\right\|} \tag{26}$$

$$\left[\mathbf{G}_{0,1}\right]_k = \left[\frac{\left(\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_1\right)^{\mathrm{T}}}{\left\|\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_1\right\|}, 0\right] \tag{27}$$

$$\left[\mathbf{G}_{0,n}\right]_k = \begin{cases} \left[-\dfrac{\left(\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_{k+1}\right)^{\mathrm{T}}}{\left\|\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_{k+1}\right\|}, 0\right], & k = n-1, n \ge 2 \\ \mathbf{0}, & k \ne n-1, n \ge 2 \end{cases} \tag{28}$$

$$\left[\Delta\mathbf{r}\right]_k = \hat{r}_{n,1} - \left\|\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_n\right\| + \left\|\hat{\mathbf{p}}_0 - \hat{\mathbf{p}}_1\right\| \tag{29}$$

and when $1 \le k \le M_n$ (M_n is the total number of available authentic signals of the n-th receiver):

$$\left[\mathbf{G}_n\right]_k = \left[\frac{\left(\hat{\mathbf{p}}_n - \mathbf{p}^{(k)}\right)^{\mathrm{T}}}{\left\|\hat{\mathbf{p}}_n - \mathbf{p}^{(k)}\right\|}, 1\right] \tag{30}$$

$$\left[\Delta\boldsymbol{\rho}_n\right]_k = \hat{\rho}_n^{(k)} - \left\|\hat{\mathbf{p}}_n - \mathbf{p}^{(k)}\right\| - c\delta\hat{t}_n \tag{31}$$

Third, estimate $\Delta\boldsymbol{\theta}$ as:

$$\Delta\boldsymbol{\theta} = \left(\mathbf{G}^{\mathrm{T}}\mathbf{W}\mathbf{G}\right)^{-1}\mathbf{G}^{\mathrm{T}}\mathbf{W}\Delta\mathbf{d} \tag{32}$$

where $\mathbf{W}$ is weighting matrix. Fourth, replace $\hat{\boldsymbol{\theta}}$ with $(\hat{\boldsymbol{\theta}} + \Delta\boldsymbol{\theta})$, return to the second step, and iterate until convergence. Now, a refined estimate of $\boldsymbol{\theta}$ can be obtained, and its MSE matrix is $\mathbf{MSE}(\hat{\boldsymbol{\theta}}) = \left(\mathbf{G}^{\mathrm{T}}\mathbf{W}\mathbf{G}\right)^{-1}$. All the estimations in $\hat{\boldsymbol{\theta}}$

can attain the CRLB by selecting the right weighting matrix, which is detailed in Section 3.2.

3.2 | Localization Accuracy Analysis

This subsection will analyze the CRLB of an unbiased spoofer position estimator.

In this problem, unknown parameters, given by $\boldsymbol{\theta}$ in Equation (21), include spoofer position, receiver position, and receiver time. The observations include spoofer range difference $\hat{\mathbf{r}} = \left[\hat{r}_{2,1}, \hat{r}_{3,1}, \cdots, \hat{r}_{N,1}\right]^{\mathrm{T}}$ and pseudorange $\hat{\boldsymbol{\rho}} = \left[\hat{\boldsymbol{\rho}}_1^{\mathrm{T}}, \hat{\boldsymbol{\rho}}_2^{\mathrm{T}}, \cdots, \hat{\boldsymbol{\rho}}_N^{\mathrm{T}}\right]^{\mathrm{T}}$, where $\hat{\boldsymbol{\rho}}_n = \left[\hat{\rho}_n^{(1)}, \hat{\rho}_n^{(2)}, \cdots, \hat{\rho}_n^{(M_n)}\right]^{\mathrm{T}}$. The random errors in $\hat{\mathbf{r}}$ and $\hat{\boldsymbol{\rho}}$ are assumed jointly Gaussian, respectively. $\hat{\mathbf{r}}$ includes measurements of spoofing signals, and $\hat{\boldsymbol{\rho}}$ includes those of real satellite signals. Spoofing signals and real satellite signals come from different sources, and thus we assume the measurement errors of spoofing signals and that of authentic signals are independent. Therefore, the PDF is:

$$\begin{aligned} f(\hat{\mathbf{r}}, \hat{\boldsymbol{\rho}}; \boldsymbol{\theta}) &= f(\hat{\mathbf{r}} \,|\, \hat{\boldsymbol{\rho}}; \boldsymbol{\theta}) \cdot f(\hat{\boldsymbol{\rho}}; \boldsymbol{\theta}) \\ &= C \cdot \exp\left[-\frac{1}{2}\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{Q}_{\mathrm{r}}^{-1}\boldsymbol{\varepsilon}\right] \cdot \exp\left[-\frac{1}{2}(\hat{\boldsymbol{\rho}} - \boldsymbol{\rho})^{\mathrm{T}}\mathbf{Q}_{\rho}^{-1}(\hat{\boldsymbol{\rho}} - \boldsymbol{\rho})\right] \end{aligned} \tag{33}$$

where C is a constant, $\boldsymbol{\varepsilon} = \left[\varepsilon_{2,1}, \varepsilon_{3,1}, \cdots, \varepsilon_{N,1}\right]^{\mathrm{T}}$ is an error vector with its elements being:

$$\varepsilon_{n,1} = \hat{r}_{n,1} - \left(r_n - r_1\right) + c\left(\hat{t}_n - t_n\right) - c\left(\hat{t}_1 - t_1\right) \tag{34}$$

$\boldsymbol{\rho} = \left[\boldsymbol{\rho}_1^{\mathrm{T}}, \boldsymbol{\rho}_2^{\mathrm{T}}, \cdots, \boldsymbol{\rho}_N^{\mathrm{T}}\right]^{\mathrm{T}}$, $\boldsymbol{\rho}_n = \left[\rho_n^{(1)}, \rho_n^{(2)}, \cdots, \rho_n^{(M_n)}\right]^{\mathrm{T}}$, $\mathbf{Q}_{\mathrm{r}}$ is the covariance matrix of $\boldsymbol{\varepsilon}$, and $\mathbf{Q}_{\mathrm{p}}$ is the covariance matrix of $\hat{\boldsymbol{\rho}}$. Then, the log-likelihood function is:

$$\ln f(\hat{\mathbf{r}}, \hat{\boldsymbol{\rho}}; \boldsymbol{\theta}) = \ln C - \frac{1}{2}\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{Q}_{\mathrm{r}}^{-1}\boldsymbol{\varepsilon} - \frac{1}{2}(\hat{\boldsymbol{\rho}} - \boldsymbol{\rho})^{\mathrm{T}}\mathbf{Q}_{\rho}^{-1}(\hat{\boldsymbol{\rho}} - \boldsymbol{\rho}) \tag{35}$$

Thus, the Fisher information matrix (FIM) is:

$$\mathbf{J}(\boldsymbol{\theta}) = -\mathrm{E}\left[\frac{\partial^2 \ln f(\hat{\mathbf{r}}, \hat{\boldsymbol{\rho}}; \boldsymbol{\theta})}{\partial \boldsymbol{\theta} \partial \boldsymbol{\theta}^{\mathrm{T}}}\right] = \begin{bmatrix} \mathbf{A}_{3\times 3} & \mathbf{B}_{3\times 4N} \\ \mathbf{B}^{\mathrm{T}} & \mathbf{C}_{4N\times 4N} \end{bmatrix} \tag{36}$$

where:

$$\begin{cases} \mathbf{A} = \left(\dfrac{\partial \boldsymbol{\varepsilon}}{\partial \mathbf{p}_0}\right)^{\mathrm{T}} \mathbf{Q}_{\mathrm{r}}^{-1} \dfrac{\partial \boldsymbol{\varepsilon}}{\partial \mathbf{p}_0} \\ \mathbf{B} = \left(\dfrac{\partial \boldsymbol{\varepsilon}}{\partial \mathbf{p}_0}\right)^{\mathrm{T}} \mathbf{Q}_{\mathrm{r}}^{-1} \dfrac{\partial \boldsymbol{\varepsilon}}{\partial \boldsymbol{\theta}_{\mathrm{u}}} \\ \mathbf{C} = \left(\dfrac{\partial \boldsymbol{\varepsilon}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\right)^{\mathrm{T}} \mathbf{Q}_{\mathrm{r}}^{-1} \dfrac{\partial \boldsymbol{\varepsilon}}{\partial \boldsymbol{\theta}_{\mathrm{u}}} + \left(\dfrac{\partial \boldsymbol{\rho}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\right)^{\mathrm{T}} \mathbf{Q}_{\rho}^{-1} \left(\dfrac{\partial \boldsymbol{\rho}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\right) \end{cases} \tag{37}$$

When $\mathbf{J}(\boldsymbol{\theta})$ has full rank, the covariance matrix of any unbiased estimation of $\boldsymbol{\theta}$ is bounded below by $\mathbf{J}^{-1}(\boldsymbol{\theta})$.

Since all raw measurements are assumed to be unbiased and have independent Gaussian distributions, the WLS estimation of $\boldsymbol{\theta}$ is also unbiased. Let $\mathbf{W} = \mathrm{diag}\left(\mathbf{Q}_{\mathrm{r}}^{-1}, \mathbf{Q}_{\rho}^{-1}\right)$, and then $\mathbf{MSE}(\hat{\boldsymbol{\theta}}) = \mathbf{J}^{-1}\left(\boldsymbol{\theta}\right)$, which means this estimation attains the CRLB.

According to Shen and Win (2010) and Shen et al. (2010), the equivalent Fisher information matrix (EFIM) of spoofer position is given by:

$$\mathbf{J}_{\mathrm{e}}(\mathbf{p}_0) = \mathbf{A} - \mathbf{B}\mathbf{C}^{-1}\mathbf{B}^{\mathrm{T}} \tag{38}$$

and $\mathbf{J}_{\mathrm{e}}^{-1}(\mathbf{p}_0)$ equals the upper left 3×3 submatrix of $\mathbf{J}^{-1}(\boldsymbol{\theta})$. Thus, the covariance matrix of any unbiased estimation of $\mathbf{p}_0$ is bounded below by $\mathbf{J}_{\mathrm{e}}^{-1}(\mathbf{p}_0)$.

According to Cao et al. (2015) and matrix inversion lemma in Zhang (2017), substitute Equation (37) into (38), and then:

$$\begin{aligned}\mathbf{J}_{\mathrm{e}}(\mathbf{p}_0) &= \left(\frac{\partial \boldsymbol{\varepsilon}}{\partial \mathbf{p}_0}\right)^{\mathrm{T}}\left[\mathbf{Q}_{\mathrm{r}}^{-1} - \mathbf{Q}_{\mathrm{r}}^{-1}\frac{\partial \boldsymbol{\varepsilon}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\mathbf{C}^{-1}\left(\frac{\partial \boldsymbol{\varepsilon}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\right)^{\mathrm{T}}\mathbf{Q}_{\mathrm{r}}^{-1}\right]\frac{\partial \boldsymbol{\varepsilon}}{\partial \mathbf{p}_0} \\ &= \left(\frac{\partial \boldsymbol{\varepsilon}}{\partial \mathbf{p}_0}\right)^{\mathrm{T}}\mathbf{Q}_{\mathrm{e}}^{-1}\frac{\partial \boldsymbol{\varepsilon}}{\partial \mathbf{p}_0}\end{aligned} \tag{39}$$

where:

$$\mathbf{Q}_{\mathrm{e}} = \mathbf{Q}_{\mathrm{r}} + \frac{\partial \boldsymbol{\varepsilon}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\left[\left(\frac{\partial \boldsymbol{\rho}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\right)^{\mathrm{T}}\mathbf{Q}_{\rho}^{-1}\left(\frac{\partial \boldsymbol{\rho}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\right)\right]^{-1}\left(\frac{\partial \boldsymbol{\varepsilon}}{\partial \boldsymbol{\theta}_{\mathrm{u}}}\right)^{\mathrm{T}} \tag{40}$$

Therefore, let $\mathbf{W}_0 = \mathbf{Q}_{\mathrm{e}}^{-1}$, and then the $\mathbf{MSE}(\hat{\mathbf{p}}_0)$ about Equation (20) is equal to $\mathbf{J}_{\mathrm{e}}^{-1}(\mathbf{p}_0)$ regardless of the errors in $\mathbf{G}_0$. As explained in Ho et al. (2007) and Wang and Ho (2013), the decrease in localization accuracy due to errors in $\mathbf{G}_0$ is insignificant. We will verify through simulation in Section 3.4 that, when the errors in $\hat{r}_{n,1}$ and $\hat{\rho}_n^{(i)}$ are not large, the estimation of Equation (20) also attains the CRLB.

3.3 | Localization on the Same Height

This subsection considers a special situation in which all the receivers and the spoofer are of the same height, such as on the surface of the ground or sea. In that case, $\left(\mathbf{G}_0^{\mathrm{T}}\mathbf{W}_0\mathbf{G}_0\right)^{-1}$ in Equation (20) does not exist, and estimating $\mathbf{p}_0$ is impossible.

To successfully estimate spoofer position, the information about height should be made use of, which can be formulated by:

$$h_0 - h_n = 0 \quad (n = 1, 2, \cdots, N) \tag{41}$$

where h_0 denotes the height of spoofer, and h_n denotes the height of the n-th receiver. Then, at first, we determine the geodetic coordinates of both receivers and the spoofer, which means to calculate longitude, latitude, and height $(\hat{\beta}_0, \hat{\phi}_0, \hat{h}_0)$ of $\hat{\mathbf{p}}_0$ and $(\hat{\beta}_n, \hat{\phi}_n, \hat{h}_n)$ of $\hat{\mathbf{p}}_n$ (Hegarty & Kaplan, 2005). Second, linearize Equation (41) about $\hat{\boldsymbol{\theta}}$, and then we have:

$$\begin{aligned}&\left[\cos\hat{\phi}_0\cos\hat{\beta}_0, \cos\hat{\phi}_0\sin\hat{\beta}_0, \sin\hat{\phi}_0\right]\left(\mathbf{p}_0 - \hat{\mathbf{p}}_0\right) \\ &-\left[\cos\hat{\phi}_n\cos\hat{\beta}_n, \cos\hat{\phi}_n\sin\hat{\beta}_n, \sin\hat{\phi}_n\right]\left(\mathbf{p}_n - \hat{\mathbf{p}}_n\right) \\ &= \hat{h}_n - \hat{h}_0\end{aligned} \tag{42}$$

At last, we put Equation (42) together with Equation (23), continue the iterative WLS algorithm until convergence, and then $\boldsymbol{\theta}$ can be estimated.

3.4 | Simulation

In this subsection, another simulation is carried out to compare the performance of the WLS algorithm with the CRLB. Consider the four receivers in Figure 3 while $g = 200$ m. A spoofer is right above Receiver 1 with its altitude at 200 m. The time is assumed 12:00 on June 17, 2020 (GPS time). For convenience, suppose $\mathbf{Q}_\rho = \mathbf{I}$ and $\mathbf{Q}_r = \nu^2\mathbf{I} + \nu^2\mathbf{U}$, where $\mathbf{U}$ is a matrix with all its entries equal to one. According to Shen and Win (2010) and Shen et al. (2010), the trace of MSE matrix can be called *average squared position error* (ASPE) as $\mathrm{E}(\|\hat{\mathbf{p}}_0 - \mathbf{p}_0\|^2) = \mathrm{tr}[\mathbf{MSE}(\hat{\mathbf{p}}_0)]$, and *squared position error bound* (SPEB), an alternate form of the CRLB, is $\mathcal{P}(\mathbf{p}_0) \triangleq \mathrm{tr}[\mathbf{J}_e^{-1}(\mathbf{p}_0)]$. Then, ASPE is bounded below by SPEB based on the properties of matrix trace, and Figure 10 depicts their curves under different values of ν, where ASPE are the results of 10^5 simulations. It can be seen that the performance of the WLS algorithm attains the CRLB in this case.

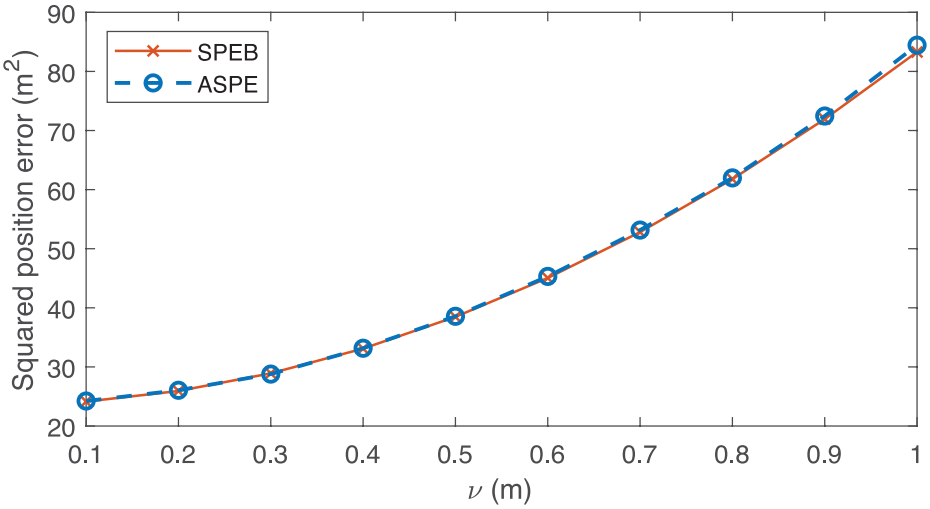


FIGURE 10 Comparison of SPEB and ASPE of spoofer position estimation

4 | REQUISITE SIGNAL PROCESSING

This section emphasizes two special but necessary functions that ensure the feasibility of this spoofer localization system.

First, one of the assumptions introduced in Section 1 is that the receivers can track both authentic and spoofing signals at the same time. However, when a spoofing signal has the same PRN code number of an authentic signal, common receivers usually track only the stronger signal. This problem was analyzed in Section 4.6.2 of Jafarnia-Jahromi (2013), and under the circumstances, there were multiple correlation peaks for a certain PRN code number during acquisition. One solution proposed in He et al. (2017) is to track each correlation peak and obtain raw measurements respectively as usual. Another solution in Humphreys et al. (2008) and Wesson et al. (2011) is to first remove the strong signal and then perform acquisition again for the same PRN code number, so that the weak vestigial signal can be tracked. Using these methods, the receivers should track every signal that they detect and obtain raw measurements of each signal. In this case, a signal is not only identified by PRN code number, but also

by an additional peak number that should be given to it to distinguish different peaks from one another. Then, all the raw measurements, including peak numbers, would be sent to the central receiver for spoofing discrimination and spoofer localization.

The other function is to check the consistency of the code rate and carrier frequency. Under stable ionospheric conditions, the proportion of carrier frequency to code rate remains fixed. For example, the proportion is 1,540 : 1 in terms of GPS L1 C/A code signal. In Equation (4), $\tau(t)$ is a measurement from code, $\dot{\rho}(t)$ is from carrier, and thus the consistency is required for the extended PrDD method to work. If consistency is not kept for a spoofing signal, the solution in Section 5.4.1 of Jafarnia-Jahromi (2013) can be used to discriminate the signal as spoofing.

These two functions should be performed by each receiver before raw measurements are sent to the central receiver.

5 | EXPERIMENT AND RESULTS

To demonstrate the feasibility of this system, we conducted a field experiment in Tsinghua University on February 5, 2021.

Four homemade GPS receivers were deployed as shown in Figure 11. They could receive and process GPS L1 C/A code signals. Receiver 1 was designated as the central receiver, and the distances between Receiver 1 and the others were about 43.2 m, 32.5 m, and 40.4 m, respectively. The receivers worked individually and were equipped with long-term evolution (LTE) wireless communication modules. Every second, each receiver obtained a set of raw measurements and sent them to Receiver 1 via LTE link. Receiver 1 collected the raw measurements from other receivers and undertook the subsequent data processing. A signal generator was used as spoofer. Three signals were simulated by the signal generator and transmitted by a small antenna, with their PRN numbers being 17, 19, and 28. We limited the signal power to a weak level, trying not to make trouble for users beyond this area. The available GPS satellites are shown in Figure 12. There are eight satellites labeled with their PRN numbers, and the small gray arrows designate their moving directions.

5.1 | Results of Spoofing Discrimination

When L is set to 30, Figure 13 shows the test statistics in Equation (6) of four pairs of authentic signals for 500 seconds of continuous time. There were four

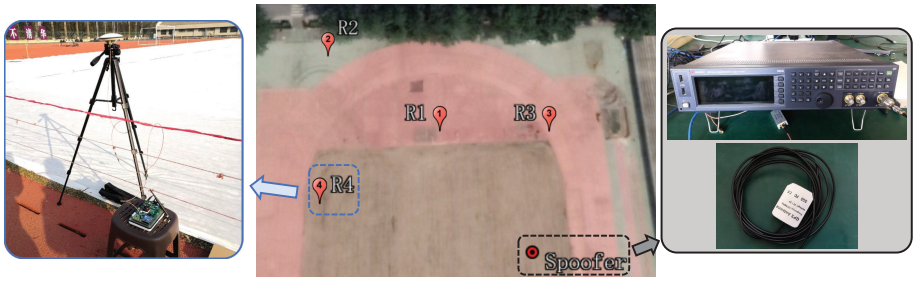


FIGURE 11 Deployment of the GPS receivers in the field experiment

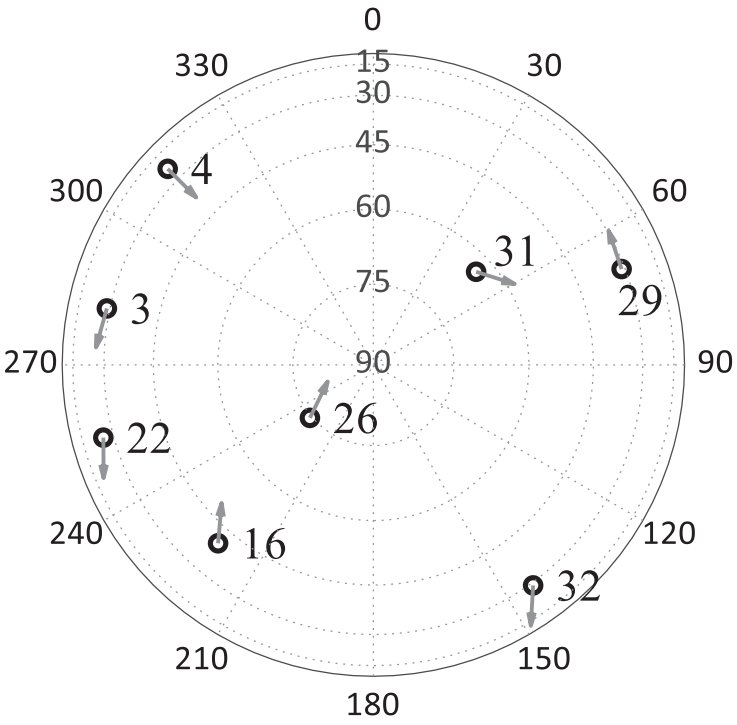


FIGURE 12 Sky plot of available satellites of GPS during the field experiment

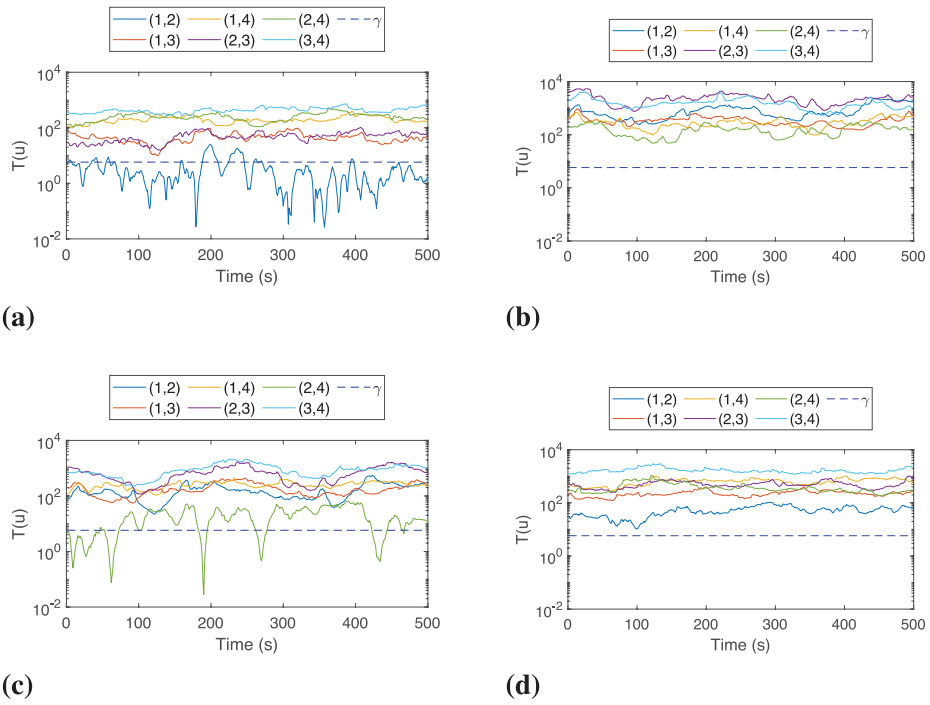


FIGURE 13 Examples of GLRT results of a pair of authentic signals: (a) Test statistics of PRN-16 and PRN-26; (b) Test statistics of PRN-22 and PRN-32; (c) Test statistics of PRN-22 and PRN-26; and (d) Test statistics of PRN-26 and PRN-31

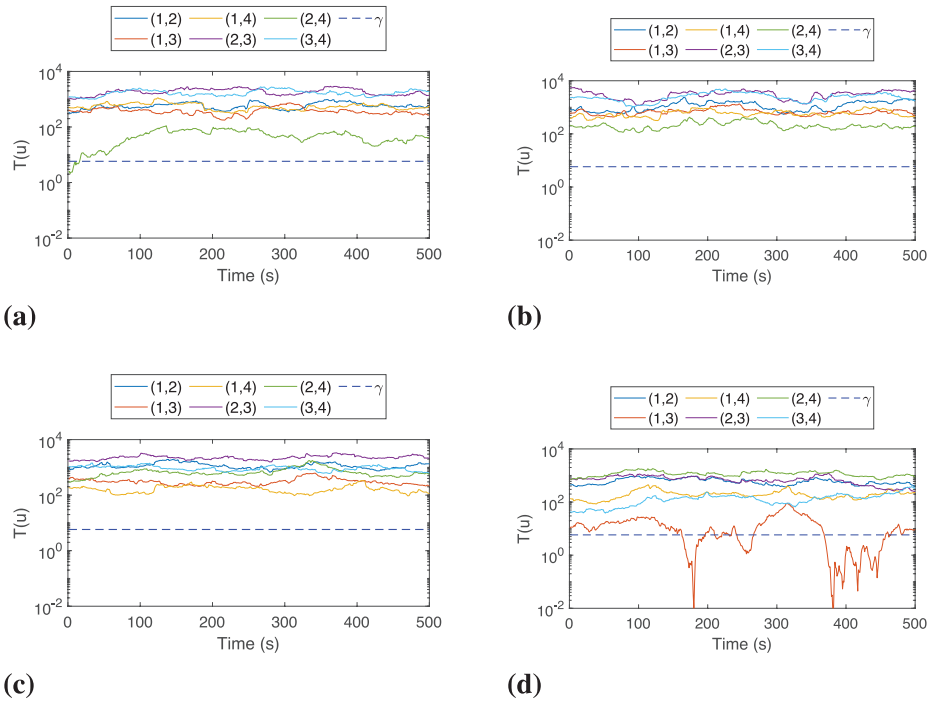


FIGURE 14 Examples of GLRT results of an authentic signal and a spoofing signal: (a) Test statistics of PRN-16 and PRN-28; (b) Test statistics of PRN-22 and PRN-17; (c) Test statistics of PRN-26 and PRN-19; and (d) Test statistics of PRN-31 and PRN-28

receivers, so there were six different combinations of the two receivers. Each receiver combination produced a series of test statistics, so there are six curves in each subfigure, in the legend of which (n, m) represents the combination of the n-th receiver and the m-th receiver. Set P_{FA} to 0.005, and the straight dashed line shows the threshold derived from Equation (9). In Figure 13(a), one of the curves appears beneath the threshold most of the time, which corresponds to the combination of Receiver 1 and Receiver 2. Thus, these two receivers would decide that this pair of signals, PRN-16 and PRN-26, were spoofing signals, while actually they were not. This is because the satellite of PRN-16 had approximately equal distance from Receiver 1 and Receiver 2, and so did the satellite of PRN-26. The relative geometry of the two satellites and the two receivers was thus unfavorable. Therefore, the value of the PrDD was about equal to zero and resulted in incorrect decisions. However, after cross-checking with other receivers, this pair of signals would be correctly recognized, which shows the superiority of the extended PrDD method. As a result, over the duration of the experiment, all pairs of authentic signals were correctly recognized.

When a signal combination is composed of an authentic signal and a spoofing signal, the extended PrDD method can also make correct decisions as shown in Figure 14. In each subfigure, there is at least one curve that stays greater than the threshold the whole time, and thus $\mathcal{H}_1$ is decided for these four pairs of signals. However, there is one exception shown in Figure 15. Since the azimuth of the satellite of PRN-32 is similar to that of the spoofer, the test statistics of all receiver combinations fluctuate near the threshold as shown in Figure 15(a), Figure 15(c), and Figure 15(e). Thus, there were occasional incorrect decisions as shown in Figure 15(b), Figure 15(d), and Figure 15(f), where, in terms of the vertical axis,

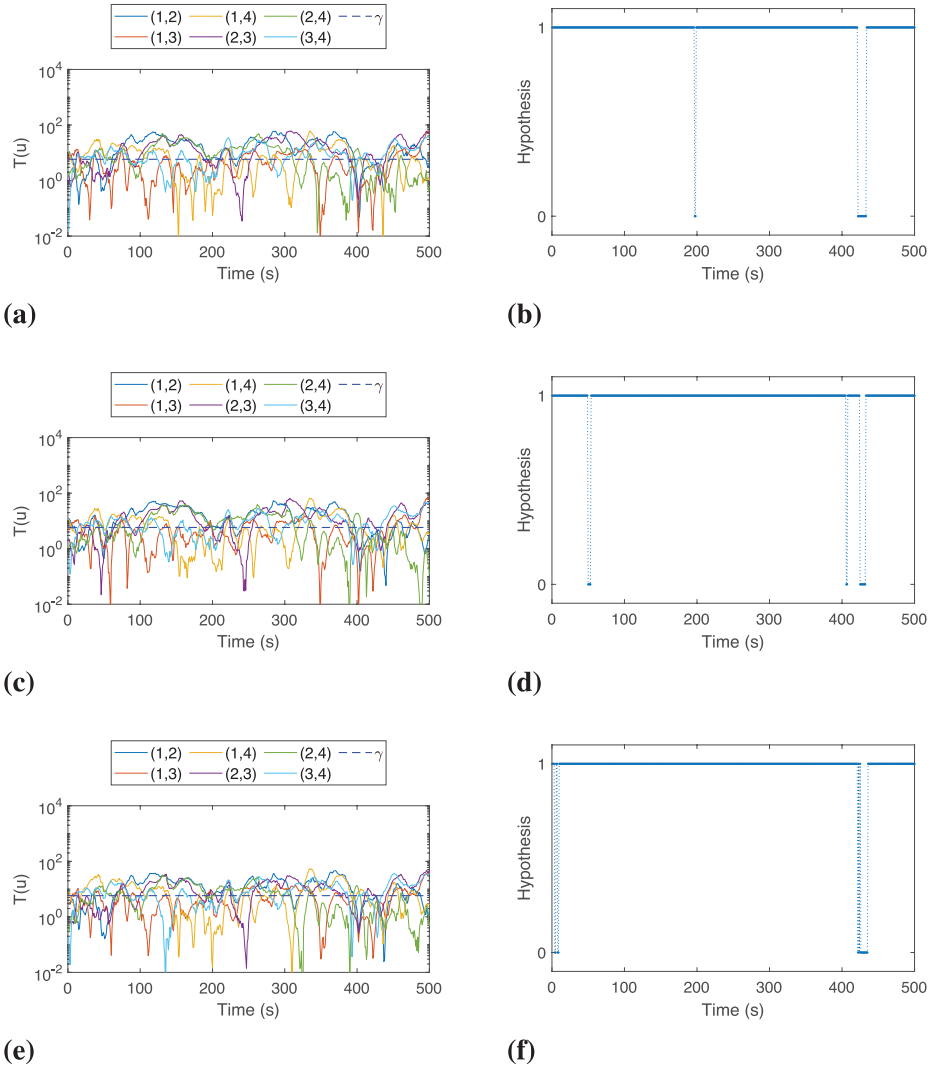


FIGURE 15 GLRT results of PRN-32 and a spoofing signal: (a) depicts the test statistics of PRN-32 and PRN-17 while (b) depicts the test results of PRN-32 and PRN-17; (c) depicts the test statistics of PRN-32 and PRN-19 while (d) depicts the test results of PRN-32 and PRN-19; and (e) depicts the test statistics of PRN-32 and PRN-28 while (f) depicts the test results of PRN-32 and PRN-28.

one means $\mathcal{H}_1$ is decided and zero means $\mathcal{H}_0$ is decided. It is expected that $\mathcal{H}_1$ is decided for these three pairs of signals, but sometimes $\mathcal{H}_0$ is decided by mistake. As a result, all signal combinations of a spoofing signal and an authentic signal (except PRN-32) can be correctly recognized during the experiment, and the signal combinations of PRN-32 and a spoofing signal can be correctly recognized most of the time of the experiment.

For a pair of spoofing signals, the results are shown in Figure 16. Although there are also occasional incorrect decisions, the test statistics remained beneath the threshold most of the time as shown in Figure 16(a), Figure 16(c), and Figure 16(e). In other words, the results show that all spoofing signal combinations were correctly discriminated most of the time of the experiment.

Overall, during the experiment, the extended PrDD method could correctly discriminate spoofing signals from authentic signals most of the time, which verifies the effectiveness of this method.

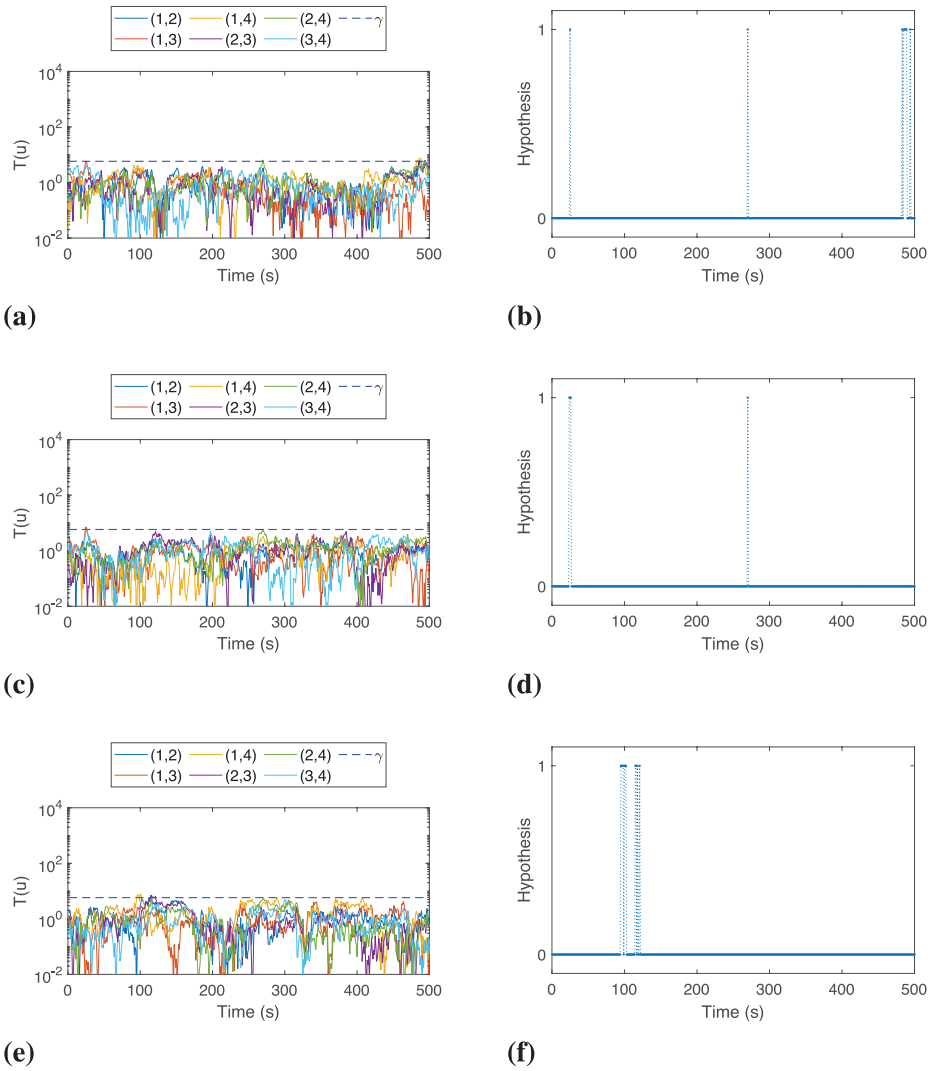
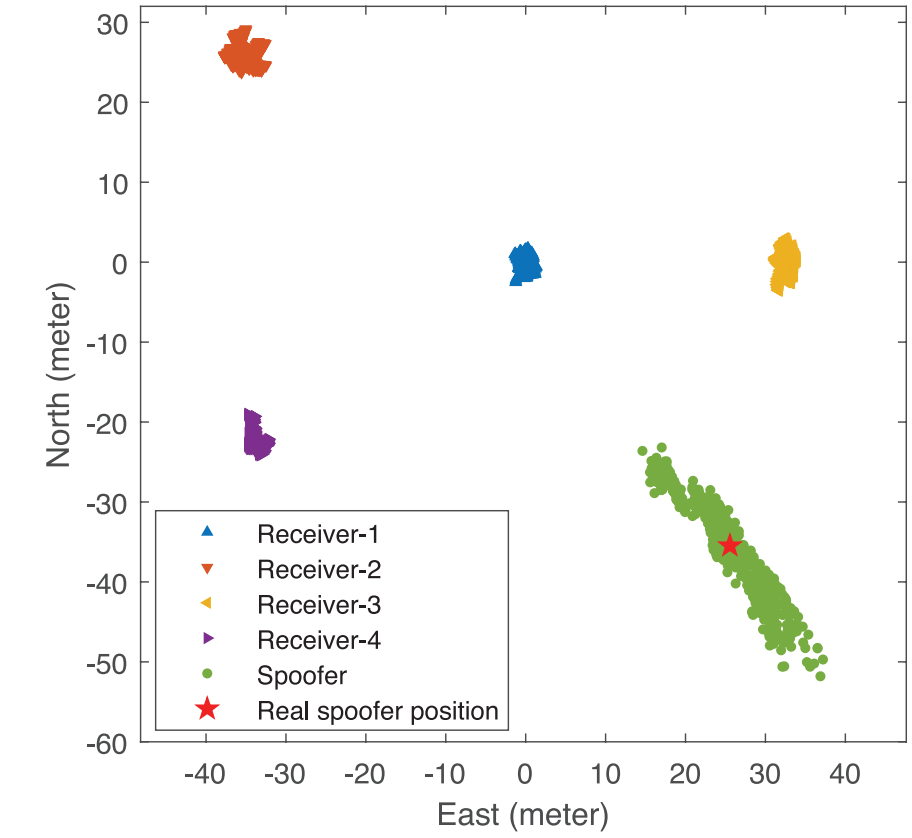


FIGURE 16 GLRT results of a pair of spoofing signals: (a) depicts the test statistics of PRN-17 and PRN-19 while (b) depicts the test results of PRN-17 and PRN-19; (c) depicts the test statistics of PRN-17 and PRN-28 while (d) depicts the test results of PRN-17 and PRN-28; and (e) depicts the test statistics of PRN-19 and PRN-28 while (f) depicts the test results of PRN-19 and PRN-28.

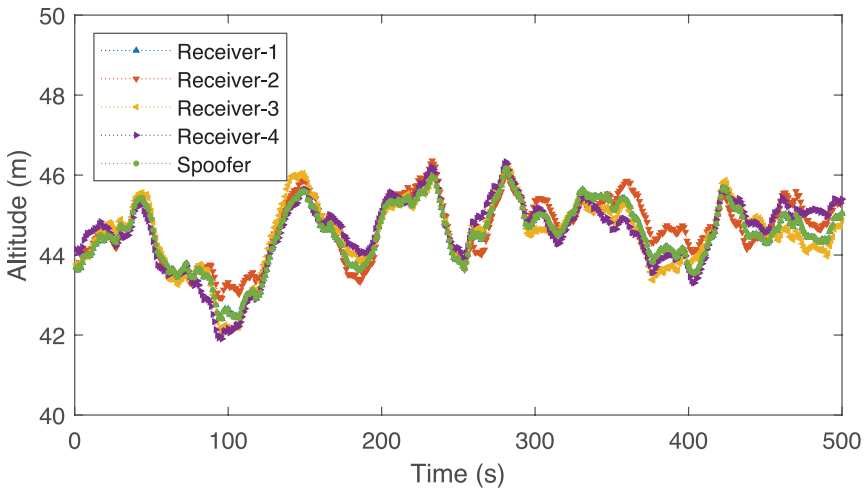
5.2 | Results of Spoofer Localization

After spoofing discrimination, the position of each receiver and spoofer can be estimated using the proposed QSSL method. Since both the receivers and the spoofer are placed on the ground, Equation (42) must be adopted to estimate spoofer position.

The results are shown in Figure 17. The horizontal position estimations are depicted in Figure 17(a), and the altitude estimations are depicted in Figure 17(b). The root mean square error (RMSE) of the position estimations and ASPE of each receiver and the spoofer are given in Table 1. This table lists the RMSE of the position estimations on each axis. All the four receivers have less RMSE on the East axis than that on the North axis. The RMSE of Receiver 2 is a little bigger than those of other receivers, because Receiver 2 can receive only five of all the eight satellite signals shown in Figure 12. As a result, the ASPE of a receiver is no bigger than 6.2 m^2. The ASPE of the spoofer in this experiment was about 43.2 m^2. It can



(a)



(b)

FIGURE 17 Estimated receiver and spoofer positions. (a) Horizontal position estimations. (b) Altitude estimations.

be seen that the spoofer localization results assembled around the real position of the spoofer. All localization results were within 16.7 m from the real spoofer position, and 90% of them were within 9.4 m from the real spoofer position.

The results demonstrate that the QSSL method is effective in this field experiment.

TABLE 1
RMSE and ASPE of position estimations

RMSE	East(m)	North(m)	Up(m)	ASPE(m^2)
Receiver 1	0.529	1.050	0.789	2.006
Receiver 2	1.233	2.004	0.797	6.172
Receiver 3	0.666	1.495	0.836	3.378
Receiver 4	0.656	1.351	0.880	3.031
Spoofer	4.068	5.098	0.790	43.164

6 | CONCLUSION

Spoofer localization is an important anti-spoofing technique. To build a flexible spoofer localization system, two major problems are studied in this paper. One is spoofing discrimination without requiring synchronization of multiple receivers, and the other is using an efficient localization method based on asynchronous raw measurements.

First, this paper proposes an extended PrDD method for spoofing discrimination. This method does not require synchronization of multiple receivers and can judge whether the spoofing signals received by different receivers are from the same spoofer. Simulation results show that this method can discriminate spoofing signals with high confidence at any point in a day. Then, the QSSL method was proposed for estimating spoofer position. This method makes use of asynchronous raw measurements of the signals to locate a spoofer, and requires no additional assistance (such as the synchronous peer or calibration emitter employed by previous works). The CRLB of the localization performance was analyzed, and both theoretical analysis and simulations proved that the spoofer position estimation could attain the CRLB. Above all, the field experiment conducted verified the effectiveness of the proposed methods, and further demonstrated that a flexible spoofer localization system is feasible and practical.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grant No. 61973181) and Tsinghua University Initiative Scientific Research Program (Grant No. 2018Z05JZY004).

REFERENCES

Akos, D. M. (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *NAVIGATION,* 59(4), 281–290. https://doi.org/10.1002/navi.19

Bhamidipati, S., & Gao, G. X. (2019). GPS multireceiver joint direct time estimation and spoofer localization. *IEEE Transactions on Aerospace and Electronic Systems*, *55*(4), 1907–1919. https://doi.org/10.1109/TAES.2018.2879532

Bhatti, J., & Humphreys, T. E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. *NAVIGATION,* 64(1), 51–66. https://doi.org/10.1002/navi.183

Borio, D., & Gioia, C. (2016). A sum-of-squares approach to GNSS spoofing detection. *IEEE Transactions on Aerospace and Electronic Systems,* 52(4), 1756–1768. https://doi.org/10.1109/TAES.2016.150148

Broumandan, A., Jafarnia-Jahromi, A., Daneshmand, S., & Lachapelle, G. (2015). A network-based GNSS structural interference detection, classification, and source localization. *Proc. of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, Tampa, FL, 3358–3369. https://www.ion.org/publications/abstract.cfm?articleID=13034

Broumandan, A., Jafarnia-Jahromi, A., Daneshmand, S., & Lachapelle, G. (2016). Overview of spatial processing approaches for GNSS structural interference detection and mitigation. *Proceedings of the IEEE,* 104(6), 1246–1257. https://doi.org/10.1109/JPROC.2016.2529600

Cao, Y., Li, P., Li, J., Yang, L., & Guo, F. (2015). A new iterative algorithm for geolocating a known altitude target using TDOA and FDOA measurements in the presence of satellite location uncertainty. *Chinese Journal of Aeronautics,* 28(5), 1510–1518. https://doi.org/10.1016/j.cja.2015.08.015

Chu, F., Li, H., Wen, J., & Lu, M. (2018). Statistical model and performance evaluation of a GNSS spoofing detection method based on the consistency of doppler and pseudorange positioning results. *Journal of Navigation,* 72(2), 447–466. https://doi.org/10.1017/S0373463318000747

Dempster, A. G., & Cetin, E. (2016). Interference localization for satellite navigation systems. *Proceedings of the IEEE,* 104(6), 1318–1326. https://doi.org/10.1109/JPR0C.2016.2530814

Gamba, G., Chiara, A. D., Pozzobon, O., & Serant, D. (2016). PROGRESS project: Jamming and spoofing detection and localization system for protection of GNSS ground-based infrastructures. *Proc. of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, OR, 3133–3142. https://doi.org/10.33012/2016.14588

Günther, C. (2014). A survey of spoofing and counter-measures. *NAVIGATION,* 61(3), 159–177. https://doi.org/10.1002/navi.65

He, L., Li, H., & Lu, M. (2017). A fundamental architecture of anti-spoofing GNSS receiver. In J. Sun, J. Liu, Y. Yang, S. Fan, and W. Yu (Eds.), *China Satellite Navigation Conference (CSNC) 2017 Proceedings: Volume I* (pp. 899–909). https://doi.org/10.1007/978-981-10-4588-2_76

Hegarty, C. & Kaplan, E. (2005). *Understanding GPS: Principles and applications* (2nd ed.). Artech house.

Heng, L., Work, D. B., & Gao, G. X. (2015). GPS signal authentication from cooperative peers. *IEEE Transactions on Intelligent Transportation Systems*, *16*(4), 1794–1805. https://doi.org/10.1109/TITS.2014.2372000

Ho, K. C., Lu, X., & Kovavisaruch, L. (2007). Source localization using TDOA and FDOA measurements in the presence of receiver location errors: Analysis and solution. *IEEE Transactions on Signal Processing,* 55(2), 684–696. https://doi.org/10.1109/TSP.2006.885744

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner Jr., P. M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proc. of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008)*, Savannah, GA, 2314–2325. https://www.ion.org/publications/abstract.cfm?articleID=8132

Jafarnia-Jahromi, A. (2013). *GNSS signal authenticity verification in the presence of structural interference* [Unpublished doctoral dissertation, University of Calgary]. http://doi.org/10.11575/PRISM/26310

Jafarnia-Jahromi, A., Broumandan, A., Daneshmand, S., Sokhandan, N., & Lachapelle, G. (2014). A double antenna approach toward detection, classification, and mitigation of GNSS structural interference *Proc. of the 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Noordwijk, The Netherlands. https://schulich.ucalgary.ca/labs/position-location-and-navigation/files/position-location-and-navigation/jafarnia2014_conference.pdf

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation.* https://doi.org/10.1155/2012/127072

Kay, S. M. (1998). *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory.* Prentice-Hall.

Kerns, A. J., Wesson, K. D., & Humphreys, T. E. (2014). A blueprint for civil GPS navigation message authentication. *2014 IEEE/ION Position, Location and Navigation Symposium,* Monterey, CA, 262–269. https://doi.org/10.1109/PLANS.2014.6851385

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics,* 31(4), 617–636. https://doi.org/10.1002/rob.21513

Pini, M., Fantino, M., Cavaleri, A., Ugazio, S., & Lo Presti, L. (2011). Signal quality monitoring applied to spoofing detection. *Proc. of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011),* Portland, OR, 1888–1896. https://www.ion.org/publications/abstract.cfm?articleID=9738

Psiaki, M. L., & Humphreys, T. E. (2016a). Attackers can spoof navigation signals without our knowledge: Here's how to fight back GPS lies. *IEEE Spectrum,* 53(8), 26–53. https://doi.org/10.1109/MSPEC.2016.7524168

Psiaki, M. L., & Humphreys, T. E. (2016b). GNSS spoofing and detection. *Proceedings of the IEEE,* 104(6), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013). GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems,* 49(4), 2250–2267. https://doi.org/10.1109/ TAES.2013.6621814

Psiaki, M. L., O'Hanlon, B. W., Powell, S. P., Bhatti, J. A., Wesson, K. D., Humphreys, T. E., & Schofield, A. (2014). GNSS spoofing detection using two-antenna differential carrier phase. *Proc. of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, Tampa, FL, 2776–2800. https://www.ion.org/publications/abstract.cfm?articleID=12530

Shang, S., Li, H., Peng, C., & Lu, M. (2020). A novel method for GNSS meaconer localization based on a space-time double-difference model. *IEEE Transactions on Aerospace and Electronic Systems, 56*(5), 3432–3449. https://doi.org/10.1109/TAES.2020.2974034

Shen, Y., & Win, M. Z. (2010). Fundamental limits of wideband localization—Part I: A general framework. *IEEE Transactions on Information Theory, 56*(10), 4956–4980. https://doi.org/10.1109/TIT.2010.2060110

Shen, Y., Wymeersch, H., & Win, M. Z. (2010). Fundamental limits of wideband localization - Part II: Cooperative networks. *IEEE Transactions on Information Theory, 56*(10), 4981–5000. https://doi.org/10.1109/TIT.2010.2059720

Stenberg, N., Axell, E., Rantakokko, J., & Hendeby, G. (2020). GNSS spoofing mitigation using multiple receivers. *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Portland, OR, 555–565. https://doi.org/10.1109/PLANS46316.2020.9109958

Swaszek, P. F., Hartnett, R. J., Kempe, M. V., & Johnson, G. W. (2013). Analysis of a simple, multi-receiver GPS spoof detector. *Proc. of the 2013 International Technical Meeting of the Institute of Navigation,* San Diego, CA, 884–892. https://www.ion.org/publications/abstract.cfm?articleID=10877

Tanil, C., Khanafseh, S., Joerger, M., & Pervan, B. (2018). An INS monitor to detect GNSS spoofers capable of tracking vehicle position. *IEEE Transactions on Aerospace and Electronic Systems, 54*(1), 131–143. https://doi.org/10.1109/TAES.2017.2739924

Wang, F., Li, H., & Lu, M. (2017). GNSS spoofing countermeasure with a single rotating antenna. *IEEE Access*, *5*, 8039–8047. https://doi.org/10.1109/ACCESS.2017.2698070

Wang, F., Li, H., & Lu, M. (2018). GNSS spoofing detection based on unsynchronized double-antenna measurements. *IEEE Access, 6,* 31203–31212. https://doi.org/10.1109/ACCESS.2018.2845365

Wang, Y., & Ho, K. C. (2013). TDOA source localization in the presence of synchronization clock bias and sensor position errors. *IEEE Transactions on Signal Processing*, *61*(18), 4532–4544. https://doi.org/10.1109/TSP.2013.2271750

Wen, J., Li, H., Wang, Z., & Lu, M. (2019). Spoofing discrimination using multiple independent receivers based on code-based pseudorange measurements. *Proc. of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2019)*, Miami, FL, 3892–3903. https://doi.org/10.33012/2019.17075

Wesson, K. D., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2011). An evaluation of the vestigial signal defense for civil GPS anti-spoofing. *Proc. of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011),* Portland, OR, 2646–2656. https://www.ion.org/publications/abstract.cfm?articleID=9816

Xie, G. (2009). *Principles of GPS and Receiver Design.* Publishing House of Electronics Industry.

Zhang, X.-D. (2017). *Matrix analysis and applications*. Cambridge University Press. https://doi.org/10.1017/9781108277587

Zhang, Z., & Zhan, X. (2018). Statistical analysis of spoofing detection based on TDOA. *IEEJ Transactions on Electrical and Electronic Engineering*, *13*(6), 840–850. https://doi.org/10.1002/tee.22637

Zou, Y., & Liu, H. (2020). Semidefinite programming methods for alleviating clock synchronization bias and sensor position errors in TDOA localization. *IEEE Signal Processing Letters, 27,* 241–245. https://doi.org/10.1109/LSP.2020.2965822

How to cite this article: Wen, J., Li, H., & Lu, M. (2022) A flexible GNSS spoofer localization system: Spoofing discrimination and localization method. *NAVIGATION, 69*(1). https://doi.org/10.33012/navi.511

APPENDIX

A DEDUCTION OF QUASI-SYNCHRONIZED TDOA MEASUREMENTS

Since $d_n^{(i)} = \rho_n^{(i)} - c\delta t_n = c\cdot\left(t_n - \tau_n^{(i)}\right)$, we have

$$\begin{aligned} d_{n,1}^{(i)} &= d_n^{(i)} - d_1^{(i)} \\ &= \left[\rho_n^{(i)}\left(t_n\right) - c\delta t_n\right] - \left[\rho_1^{(i)}\left(t_n\right) - c\delta t_1\right] \\ &\approx \rho_n^{(i)}\left(t_n\right) - \left[\rho_1^{(i)}\left(t_1\right) + \dot{\rho}_1^{(i)}\left(t_1\right)\cdot\left(t_n - t_1\right)\right] - c\delta t_n + c\delta t_1 \\ &= c\left[t_n - \tau_n^{(i)}\left(t_n\right)\right] - c\left[t_1 - \tau_1^{(i)}\left(t_1\right)\right] - \dot{\rho}_1^{(i)}\left(t_1\right)\cdot\left(t_n - t_1\right) \\ &= \left[c - \dot{\rho}_1^{(i)}\left(t_1\right)\right]\left(t_n - t_1\right) - c\left[\tau_n^{(i)}\left(t_n\right) - \tau_1^{(i)}\left(t_1\right)\right]. \end{aligned} \tag{A1}$$

Note that an assumption in Equation (A1) is that δt_n and δt_1 keep unchanged during the short period of time from t_1 to t_n. Also, an approximation is made as $\rho_1^{(i)}\left(t_n\right) \approx \rho_1^{(i)}\left(t_1\right) + \dot{\rho}_1^{(i)}\left(t_1\right)\cdot\left(t_n - t_1\right)$. Here, $d_n^{(i)}$ is not the distance of spoofer from the n-th receiver, but an imaginary distance between the n-th receiver and the imaginary satellite that is simulated by the spoofer. However, the difference of the real spoofer distances is equal to that of the imaginary satellite distances, so we can use the result in Equation (A1) to estimate spoofer position. The second line of Equation (A1) means the desired range difference should be calculated using raw measurements that are measured at the same time. However, only asynchronous raw measurements are available, so we have the form as the last line of Equation (A1), i.e., the form in Equation (17).