sensors

MDPI

Article

GNSS Spoofing Network Monitoring Based on Differential Pseudorange

Zhenjun Zhang and Xingqun Zhan *

School of Aeronautics and Astronautics, Shanghai Jiao Tong University, Shanghai 200240, China; zj.zhang@sjtu.edu.cn

* Correspondence: xqzhan@sjtu.edu.cn; Tel.: +86-136-2181-7248

Academic Editor: Xue-Bo Jin

Received: 14 September 2016; Accepted: 17 October 2016; Published: 23 October 2016

Abstract: Spoofing is becoming a serious threat to various Global Navigation Satellite System (GNSS) applications, especially for those that require high reliability and security such as power grid synchronization and applications related to first responders and aviation safety. Most current works on anti-spoofing focus on spoofing detection from the individual receiver side, which identifies spoofing when it is under an attack. This paper proposes a novel spoofing network monitoring (SNM) mechanism aiming to reveal the presence of spoofing within an area. Consisting of several receivers and one central processing component, it keeps detecting spoofing even when the network is not attacked. The mechanism is based on the different time difference of arrival (TDOA) properties between spoofing and authentic signals. Normally, TDOAs of spoofing signals from a common spoofer are identical while those of authentic signals from diverse directions are dispersed. The TDOA is measured as the differential pseudorange to carrier frequency ratio (DPF). In a spoofing case, the DPFs include those of both authentic and spoofing signals, among which the DPFs of authentic are dispersed while those of spoofing are almost overlapped. An algorithm is proposed to search for the DPFs that are within a pre-defined small range, and an alarm will be raised if several DPFs are found within such range. The proposed SNM methodology is validated by simulations and a partial field trial. Results show 99.99% detection and 0.01% false alarm probabilities are achieved. The SNM has the potential to be adopted in various applications such as (1) alerting dedicated users when spoofing is occurring, which could significantly shorten the receiver side spoofing cost; (2) in combination with GNSS performance monitoring systems, such as the Continuous Operating Reference System (CORS) and GNSS Availability, Accuracy, Reliability anD Integrity Assessment for Timing and Navigation (GAARDIAN) System, to provide more reliable monitoring services.

Keywords: GNSS; spoofing and anti-spoofing; spoofing network monitoring; TDOA; differential pseudorange to carrier frequency ratio

1. Introduction

The GNSS's vulnerability to spoofing was first officially identified by the U.S. government in 2001 [1]. Recently, the situation has become more critical. An experiment conducted by the research team led by Dr. Humphreys illustrates the threat of spoofing, where an unmanned aerial vehicle (UAV) was captured and then forced to crash down [2].

Although many effective spoofing detection techniques have been developed to protect individual receivers, there is little discussion in the literature focusing on spoofing monitoring that aims to monitor the presence of spoofing within an area. Actually, spoofing monitoring could be promising and valuable in various applications. For instance, when equipped with spoofing monitoring, one could alert dedicated users when spoofing is occurring. This is attractive because the users can be made aware of spoofing without having to continuously perform spoofing detection themselves. Also, it could

be combined with the GNSS performance monitoring systems to provide more reliable services. Nowadays, many systems have been developed for GNSS performance monitoring, such as CORS and GAARDIAN [3]. However, few of them are reported to be equipped with spoofing monitoring techniques. Unfortunately, a performance monitoring service may not be reliable without taking spoofing into consideration. One may doubt the necessity of spoofing monitoring because these systems are equipped with the receiver autonomous integrity monitoring (RAIM) technique, which can detect counterfeit signals, and they tend to have accurate knowledge of their three-dimensional positions so that they can easily detect spoofing based on unexpected position, velocity and time (PVT) outputs. However, this is not always the case. In a spoofing scenario, there are three cases for the status of the monitoring system: (1) The system adopts only the spoofing signals for PVT so that it is spoofed; (2) The system adopts only the authentic signals for PVT, and therefore it is not spoofed and its reported position is not affected by the spoofing. This is likely to happen. For examples, a spoofer is placed somewhat far away from the system so that the received spoofing strength may be weaker than the authentic one. In this scenario, the receiver tends to adopt stronger authentic signals for PVT and ignore the weaker spoofing. In addition, some spoofing technologies are able to spoof only a particular receiver [4]. In this scenario, although other receivers can still receive spoofing signals, their reported PVT will not be influenced; (3) The system adopts a combination of spoofing and authentic signals for PVT. To detect the presence of spoofing, the monitoring mechanism is required to be effective in all three cases. However, the RAIM and the prior known PVT information are not sufficient to satisfy such a requirement. The RAIM cannot be workable for the first two cases because either authentic or spoofing signals tend to be self-consistent with a small pseudorange residual [5], while the prior known PVT information cannot be applied in the second case as the system's reported PVT is not affected by spoofing.

Hence, in order to perform spoofing monitoring, one is required to continue detecting spoofing even when not affected by spoofing. Among the proposed spoofing detection techniques, several methods could satisfy such a requirement: (1) Cryptographic based methods [6–8] meant to make parts of civil GNSS codes or navigation messages unpredictable to a spoofer. Based on such methods, one can easily find non-authentic signals. Though effective, this requires a modification to the signal structure and may not be available in the near future; (2) The moving receiver-based techniques given by [9–12]. They assume spoofing signals are transmitted from a common spoofer so that the spoofing parameters, such as signal strengths and Dopplers, are highly correlated. The spoofing detection is developed based on searching for the correlated signals among all the received signals. These techniques are effective, but they require the motion of the receivers, while spoofing monitoring systems/networks tend to be stationary; (3) Redundant signal detection based methods introduced by [4,13–16] aiming to detect unexpected 'GNSS-like' signals. Such methods can be easy to implement as they are software-defined, but they may have trouble distinguishing spoofing from multipath [14,17].

Although the aforementioned methods can be effective in spoofing monitoring, they are either difficult to implement or unsuitable for monitoring a network that consists of multiple static receivers. Several anti-spoofing methods based on multiple receivers were proposed in [18–22]. These works assume the multiple receivers adopt only the spoofing signals for PVT and therefore that they will give nearly identical position solutions and pseudorange measurements. Some works [18–20] aim to check whether the position solutions reported from multiple spatially separated receivers match their known physical formation; [21] aims to check whether the reported position solutions are almost identical. One study [22] takes advantage of different pseudorange properties between spoofing and non-spoofing cases. In a spoofing case, the pseudoranges of each satellite signal observed at multiple receivers are almost identical, while in a non-spoofing case they are varied. Although these methods are promising as they are effective and can be easily implemented, they can hardly be applied for spoofing monitoring purposes. As discussed before, the PVT solutions from monitoring receivers may not be influenced in the spoofing case and therefore their reported position and pseudorange measurements might not be 'almost identical'.

Based on these considerations, a spoofing network monitoring (SNM) mechanism consisting of multiple (more than one) receivers and a central processing component is proposed in this paper. As opposed to the previous works on multi-receiver-based anti-spoofing [18–22], the SNM is able to detect the presence of spoofing signals no matter whether the PVT solutions are influenced by spoofing. The essence of the SNM is to search for the spoofing signals among all the received signals. The use of multiple receivers rather than one receiver is mainly because the SNM mechanism is based on the differing TDOA properties between spoofing and authentic signals. Like many spoofing detection techniques [9–12,17–20,22,23], the SNM assumes that the spoofing signals are transmitted from a common spoofer. Hence, the TDOAs of spoofing signals transmitted from a common spoofer are identical, while those of authentic signals from diverse directions are dispersed. The TDOA is measured as the differential pseudorange to carrier frequency ratio (DPF). In a non-spoofing case where only authentic signals are received, the DPFs of the received signals are dispersed. In a spoofing case, both authentic and spoofing signals are received and therefore the DPFs will include those of both authentic and spoofing signals. Among these, the DPFs of authentic are dispersed while those of spoofing are almost overlapped. Hence, an algorithm is designed to search for the DPFs that are within a predefined small range, and an alarm will be raised if several DPFs are found within such a range. Simulations and real-data experiments are conducted to validate spoofing monitoring performance. Results show the detection and false alarm probabilities could reach 99.99% and 0.01%, respectively.

The SNM is relatively low-cost and can be easily implemented and deployed for three reasons: (1) It consists of at least two monitoring receivers, and most commercial receivers could be adopted with only a slightly modification in software; (2) The monitoring receivers do not require either clock synchronization or the knowledge of their 3-D positions. This implies the SNM could be a 'plug and play' option; (3) The methodology is totally software-defined and is of low computational complexity.

The rest of the paper consists of 8 sections. Section 2 gives the architecture of the SNM. Section 3 gives differential pseudorange (DP) models, based on which the DPF models are given in Section 4. Section 5 introduces the spoofing monitoring methodology. Its performance is then tested based on simulations in Section 6. The real-data experiments are conducted in Section 7 to validate the proposed SNM. Section 8 provides some discussion and recommends future work. Section 9 concludes the paper.

2. Spoofing Network Monitoring Architecture

The architecture given by Figure 1 consists of at least two monitoring receivers and a central processing component (CPC). The monitoring receivers are used to provide pseudorange and Doppler measurements of all the received signals. These measurements are then fed into the CPC for spoofing monitoring purposes. The rest of this section introduces the 4-step spoofing network monitoring architecture, and a detailed analysis is given in the successive sections.

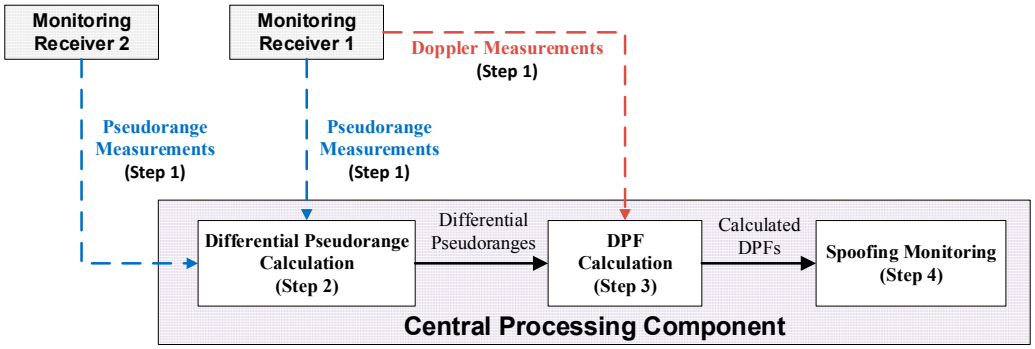


Figure 1. Spoofing network monitoring architecture.

2.1. Raw Measurements

Since the spoofing monitoring is based on the DPF, the first step is to estimate the pseudorange and Doppler measurements of all the received signals. This step is performed by the monitoring receivers. The receiver architecture given by Figure 2 is almost the same as the normal commercial receivers except for the acquisition block. The modified acquisition block searches for all the signals and then passes all those that are above the predetermined acquisition threshold to the tracking block. Hence, if spoofing exists, both the authentic and spoofing signals will be acquired [10–12]. This modified acquisition process has already been introduced and adopted by references [10–12] for spoofing detection purposes. The tracking block aims to estimate the Doppler and code phase measurements of these acquired signals. The Doppler measurements are fed into the CPC and the code phases are used to measure the pseudorange. It is measured as the product of the speed of light and the signal's propagation time that is the difference between its generation and received time. The generation time is determined based on the decoded navigation message and the code phase [24] while the received time is read from the receiver's clock. Though the GNSS cannot be trusted for timing as there may exist a spoofing, many other cheap ways could be adopted. For example, there is the Network Time Protocol (NTP)-based clock synchronization technology, which is widely used for internet time synchronization and can achieve a precision of tens of milliseconds [25]. This precision is sufficient for spoofing monitoring.

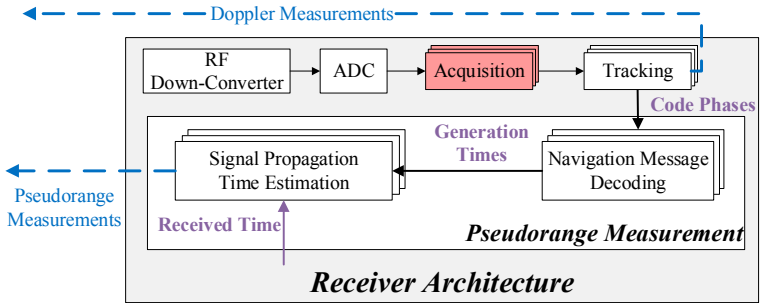


Figure 2. Monitoring Receiver Architecture.

Note the following:

- In a spoofing case, although both authentic and spoofing signals are processed by the receiver, the receiver itself does not know the types of the signals (spoofing or authentic), and it does not even know whether there are spoofing signals or not.
- The monitoring receiver does not need to perform the PVT process because its only function is to provide raw measurements. Hence, the PVT block is not given in the monitoring receiver architecture.

2.2. Differential Pseudorange Calculation

The differential pseudorange (DP) is calculated based on the pseudorange measurements from receivers. In a spoofing case, the pseudoranges of both spoofing and authentic signals are provided by each receiver, so the calculated DPs would consist of 2 or 3 DP types: (1) DP between spoofing signals; (2) DP between authentic signals; and possibly (3) the DP between spoofing and authentic signals if the two have some common PRNs. These three types are introduced in Section 3.3, where the corresponding DP models are also given.

2.3. DPF Calculation

The DPF is calculated as the ratio between the differential pseudorange and the received carrier frequency. The received carrier frequency is a combination of the signal frequency generated at the

satellite (e.g., 1.57542 GHz for GPS L1) and the Doppler measurement provided by either of the two receivers. Based on the DPs given by step 2, the calculated DPFs in a spoofing case also include 2 or 3 types: (1) DPF between spoofing signals; (2) DPF between authentic signals; and possibly (3) the DPF between spoofing and authentic signals.

These three types are discussed in Section 4, where the corresponding DPF models are also given. It shows the DPF consists of the TDOA, multipath error difference, clock difference and estimation noise. Considering spoofing signals are from a common spoofer, the first three parts of spoofing DPFs are identical. Hence, the spoofing DPFs are almost overlapped. By contrast, the authentic DPFs are dispersed as authentic signals come from various directions.

2.4. Spoofing Monitoring

In a non-spoofing case, only dispersed authentic DPFs are present. In a spoofing case, as discussed before, besides dispersed authentic DPFs, the overlapped spoofing DPFs will also be present. Hence the monitoring algorithm is designed to search for the DPFs that are within a predefined small range, and the presence of spoofing is determined when several DPFs are found within such range. The monitoring methodology, including the hypothesis test, the determination of the pre-defined range and the algorithm, is introduced in Section 5.

3. Differential Pseudorange Models

This section firstly gives the spoofing scenario, based on which the pseudorange models are then given. Finally, the differential pseudorange models are formulated.

3.1. Spoofing Scenario

Figure 3 illustrates a typical spoofing scenario consisting of two monitoring receivers, a spoofer and several GNSS satellites. It is assumed each of the two monitoring receivers, noted as rcv_1 and rcv_2, are able to receive both spoofing and authentic signals. The clock bias for rcv_x is as Δt_x. The receiver time t' of rcv_x is modelled as a combination of true time t_x and the clock bias Δt_x:

$$t' = t_x + \Delta t_x \tag{1}$$

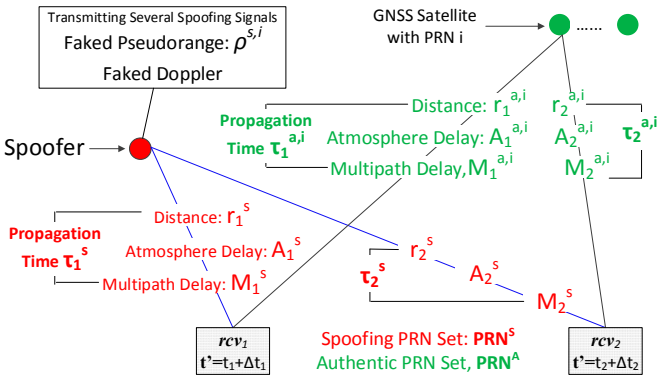


Figure 3. Spoofing Scenario.

The spoofer is transmitting several fake GNSS signals with faked Doppler and code phase, and the faked code phase will result in the faked pseudorange $\rho^{s,i}$. Like many other spoofing detection methods assuming all spoofing signals transmitted from a common spoofer, the number of spoofing signals is assumed to be at least 4 so that victim receivers could be spoofed to a wrong location via adopting

spoofing signals for PVT calculation. The PRN sets of spoofing and authentic signals are noted as $\mathbf{PRN^S}$ and $\mathbf{PRN^A}$, respectively. The relationships between the two sets are as follows:

$$\mathbf{PRN^{A\cap S}} = \mathbf{PRN^A} \cap \mathbf{PRN^S}, \quad \mathbf{PRN^{A-S}} = \mathbf{PRN^A} - \mathbf{PRN^S}, \quad \mathbf{PRN^{S-A}} = \mathbf{PRN^S} - \mathbf{PRN^A}$$

where $\mathbf{PRN^{A\cap S}}$ is the intersection of $\mathbf{PRN^A}$ and $\mathbf{PRN^S}$, $\mathbf{PRN^{A-S}}$ belongs to $\mathbf{PRN^A}$ but not $\mathbf{PRN^S}$, and $\mathbf{PRN^{S-A}}$ belongs to $\mathbf{PRN^S}$ but not $\mathbf{PRN^A}$.

3.2. Pseudorange Measurement

After all the signals are processed, the pseudorange measurements at rcv_x are:

$$\widetilde{\boldsymbol{\rho}}_{\mathbf{x}} = \begin{bmatrix} \widetilde{\rho}_x^{a,i}, \widetilde{\rho}_x^{s,i} | i \in \mathbf{PRN^{A\cap S}} \\ \widetilde{\rho}_x^{a,i} | i \in \mathbf{PRN^{A-S}} \\ \widetilde{\rho}_x^{s,i} | i \in \mathbf{PRN^{S-A}} \end{bmatrix} \tag{2}$$

wherein $\widetilde{\rho}_x^{s,i}$ and $\widetilde{\rho}_x^{a,i}$ are respectively the authentic and spoofing pseudorange measurements at rcv_x. The superscript i denotes the PRN index. Note that both $\widetilde{\rho}_x^{s,i}$ and $\widetilde{\rho}_x^{a,i}$ are available for $i \in \mathbf{PRN^{A\cap S}}$ because the spoofing and authentic have the common PRN i. $\widetilde{\rho}_x^{s,i}$ and $\widetilde{\rho}_x^{a,i}$ measured at receiver time t' is derived in Appendix A, and the result is:

$$\widetilde{\rho}_x^{s,i}\left(t'\right) = \frac{\lambda f^{s,i}}{c}\left[r_x^s + A_x^s + M_x^s + c\Delta t_x\right] + \rho^{s,i}\left(t'\right) + \xi_x^{s,i} \tag{3}$$

$$\widetilde{\rho}_x^{a,i}\left(t'\right) = \frac{\lambda f^{a,i}}{c}\left[r_x^{a,i}\left(t'\right) + A_x^{a,i} + M_x^{a,i} + c\Delta t_x\right] + \xi_x^{a,i} \tag{4}$$

wherein λ is the carrier wavelength and c is the speed of light. $f^{s,i}$ ($f^{a,i}$) is the received carrier frequency, which is a combination of the GNSS carrier frequency (e.g., 1.57542 GHz for GPS L1) and Doppler. r_x^s ($r_x^{a,i}$) is the distance between the spoofer (satellite) and rcv_x. A denotes the atmosphere induced delay, including troposphere and ionosphere. M is the multipath induced error. $\rho^{s,i}\left(t'\right)$ is the faked pseudorange measurements simulated at the spoofer at t'. The measurement noise $\xi_x^{s,i}$ ($\xi_x^{a,i}$) is usually modelled as an identical and independently distributed (IID) Gaussian random variable with zero mean and the variance of σ^2 [24].

3.3. Differential Pseudorange

The differential pseudorange (DP) is calculated as the difference of the pseudorange measurements with the same PRN, which are respectively provided by two receivers. The result is given as below:

$$\boldsymbol{\Delta\rho} = \begin{bmatrix} \Delta\rho^{a,i}, \Delta\rho^{s,i}, \Delta\rho^{a-s,i}, \Delta\rho^{s-a,i} | i \in \mathbf{PRN^{A\cap S}} \\ \Delta\rho^{a,i} | i \in \mathbf{PRN^{A-S}} \\ \Delta\rho^{s,i} | i \in \mathbf{PRN^{S-A}} \end{bmatrix} \tag{5}$$

where

$$\Delta\rho^{s,i} = \widetilde{\rho}_1^{s,i} - \widetilde{\rho}_2^{s,i}, \quad \Delta\rho^{a,i} = \widetilde{\rho}_1^{a,i} - \widetilde{\rho}_2^{a,i}, \quad \Delta\rho^{a-s,i} = \widetilde{\rho}_1^{a,i} - \widetilde{\rho}_2^{s,i}, \quad \Delta\rho^{s-a,i} = \widetilde{\rho}_1^{s,i} - \widetilde{\rho}_2^{a,i} \tag{6}$$

In a spoofing case, the calculated DPs will include 3 DP types: (1) DP between authentic signals: $\Delta\rho^{a,i}$; (2) DP between spoofing signals $\Delta\rho^{s,i}$; (3) DP between authentic and spoofing signals: $\Delta\rho^{a-s,i}$ and $\Delta\rho^{s-a,i}$. This type exists if and only if $\mathbf{PRN^{A\cap S}}$ is a nonempty set. By substituting Equations (3) and (4) into Equation (6), the $\Delta\rho^{s,i}$ and $\Delta\rho^{a,i}$ becomes:

$$\Delta\rho^{s,i} = \lambda f^{s,i}\left(\Delta\tau^s + \Delta M^s + \Delta t\right) + \Delta\xi^{s,i} \tag{7}$$

$$\Delta\rho^{a,i} = \lambda f^{a,i}\left(\Delta\tau^{a,i} + \Delta M^{a,i} + \Delta t\right) + \Delta\xi^{a,i} \tag{8}$$

where

$$\Delta\tau^{s} = \left[r_1^s - r_2^s\right]/c, \quad \Delta M^{s} = M_1^s - M_2^s, \quad \Delta\xi^{s,i} = \xi_1^{s,i} - \xi_2^{s,i}, \quad \Delta t = \Delta t_1 - \Delta t_2$$
$$\Delta\tau^{a,i} = \left[r_1^{a,i} - r_2^{a,i}\right]/c, \quad \Delta M^{a,i} = M_1^{a,i} - M_2^{a,i}, \quad \Delta\xi^{a,i} = \xi_1^{a,i} - \xi_2^{a,i}$$

In $\Delta\rho^{s,i}$ ($\Delta\rho^{a,i}$), the $\Delta\tau^{s}$ ($\Delta\tau^{a,i}$) is actually the TDOA of a spoofing signal (authentic signal). The difference of atmosphere delay is negligible for short baseline (e.g., <10 km) differential pseudorange [26], therefore it is neglected in both $\Delta\rho^{s,i}$ and $\Delta\rho^{a,i}$ as the SNM is short baseline based. Also, given that the IID Gaussian distributed measurement noise at different receivers ($\xi_1^{s,i}$ and $\xi_2^{s,i}$) are uncorrelated [26], the $\Delta\xi^{s,i}$ ($\Delta\xi^{a,i}$) can be modelled as an IID Gaussian random variable with zero mean and the variance of $2\sigma^2$ (the standard deviation of the pseudorange measurement noise σ was defined in Section 3.2):

$$\Delta\xi^{s,i} \sim \mathbf{N}\left[0, \sqrt{2}\sigma\right], \quad \Delta\xi^{a,i} \sim \mathbf{N}\left[0, \sqrt{2}\sigma\right] \tag{9}$$

wherein $\mathbf{N}[a,b]$ denotes the Gaussian distribution with the mean of a and standard deviation of b.

4. Differential Pseudorange to Carrier Frequency Ratio

The DPF of each signal is calculated as the ratio between the differential pseudorange and the received carrier frequency. The received carrier frequency measurement is a combination of the standard GNSS frequency and the Doppler measurement. The Doppler can be provided by either of the two receivers. Note that received carrier frequency measurement includes the pure carrier frequency and the Doppler measurement error, and the Doppler measurement error is negligible as it is way smaller than the carrier frequency. Based on the calculated differential pseudoranges given by Equation (5), the calculated DPFs are given as:

$$\mathbf{k} = \begin{bmatrix} k^{a,i}, k^{s,i}, k^{a-s,i}, k^{s-a,i} | i \in \mathbf{PRN}^{\mathbf{A}\cap\mathbf{S}} \\ k^{a,i} | i \in \mathbf{PRN}^{\mathbf{A}-\mathbf{S}} \\ k^{s,i} | i \in \mathbf{PRN}^{\mathbf{S}-\mathbf{A}} \end{bmatrix} \tag{10}$$

where $k^{s,i} = \frac{\Delta\rho^{s,i}}{\lambda f^{s,i}}$, $k^{a,i} = \frac{\Delta\rho^{a,i}}{\lambda f^{a,i}}$, $k^{a-s,i} = \frac{\Delta\rho^{a-s,i}}{\lambda f^{a,i}}$, $k^{s-a,i} = \frac{\Delta\rho^{s-a,i}}{\lambda f^{s,i}}$.

In a spoofing case, the calculated DPF include three DPF types: (1) DPF between the authentic signals (authentic DPF): $k^{a,i}$; (2) DPF between spoofing signals (spoofing DPF): $k^{s,i}$; and (3) DPF between authentic and spoofing signals (AS DPF): $k^{s\text{-}a,i}$ and $k^{a\text{-}s,i}$. By substituting Equations (7) and (8), the $k^{s,i}$ and $k^{a,i}$ are given as:

$$k^{s,i} = \underbrace{\Delta\tau^{s} + \Delta M^{s} + \Delta t}_{\text{Identical Among Spoofing Signals}} + \delta^{s,i} \tag{11}$$

$$k^{a,i} = \underbrace{\Delta\tau^{a,i} + \Delta M^{a,i}}_{\text{Various for authentic signals}} + \Delta t + \delta^{a,i} \tag{12}$$

where

$$\delta^{s,i} = \Delta\xi^{s,i}/\left(\lambda f^{s,i}\right), \quad \delta^{a,i} = \Delta\xi^{a,i}/\left(\lambda f^{a,i}\right) \tag{13}$$

The DPF noises $\delta^{s,i}$ and $\delta^{a,i}$ are further derived in Appendix B, and the results are:

$$\begin{aligned} \delta^{s,i} &= \Delta\xi^{s,i}/c, \quad \delta^{s,i} \sim \mathbf{N}\left[0, \sigma_\delta\right] \\ \delta^{a,i} &= \Delta\xi^{a,i}/c, \quad \delta^{a,i} \sim \mathbf{N}\left[0, \sigma_\delta\right] \end{aligned} \tag{14}$$

where

$$\sigma_\delta = \sqrt{2}\sigma/c \tag{15}$$

As can be seen, both the spoofing and authentic DPFs consist of four parts: TDOA, multipath difference, clock difference and the DPF estimation noise. The first three parts are identical among spoofing DPFs as spoofing signals are transmitted from the common source. Hence, the spoofing DPFs would almost overlay each other within a small range. Note that the spoofing DPFs do not completely overlay due to the random DPF estimation noise. By contrast, the TDOAs and multipath differences of authentic signals are dispersed because they are transmitted from diverse directions. Hence, the authentic DPFs are dispersed.

Note that the AS DPFs $k^{s\text{-}a,i}$ and $k^{a\text{-}s,i}$ are not given because they are irrelevant for the spoofing monitoring methodology introduced in the following section. This is because in a non-spoofing case, these AS DPFs will not even exist. In a spoofing case, though they might be present, the spoofing monitoring technique is based on the overlapped spoofing DPFs rather than the AS DPFs.

Following gives the distribution of the $k^{s,i}$, which will be used for detection probability analysis given in the following section. Since $\Delta\xi^{s,i}$ given by Equation (9) is an IID Gaussian random variable, the spoofing DPF noise $\delta^{s,i}$ given by Equation (14) is also IID. Hence, the spoofing DPFs $k^{s,i}$ consisting of identical $\Delta\tau^s$, ΔM^s and Δt, and IID Gaussian random variables $\delta^{s,i}$, are identically and independently Gaussian distributed:

$$k^{s,i} \sim \mathbf{N}\left[\Delta\tau^s + \Delta M^s + \Delta t, \sigma_\delta\right] \tag{16}$$

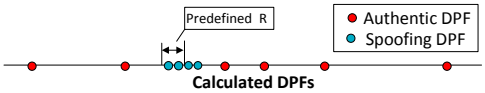
5. Monitoring Methodology

5.1. Hypothesis Test

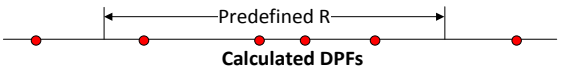
The spoofing monitoring is based on the calculated DPFs. In a non-spoofing case, the calculated DPFs include only dispersed authentic DPFs. In a spoofing case, however, the calculated DPFs include not only authentic, but also overlapped spoofing DPFs. Furthermore, it is assumed in Section 3.1 that the number of spoofing signals is at least 4. Hence, in a spoofing case, there must present at least 4 DPFs that almost overlay each other but with different PRNs. Hence, the spoofing monitoring is designed to search for the DPFs that are within a predefined small range and the existence of spoofing can be identified if at least 4 DPFs (with different PRNs) are found within such a range. The null hypothesis H_0 stating the absence of spoofing and alternate hypothesis H_1 stating the existence of spoofing are given as:

$$\begin{aligned} \mathrm{H}_0 &: \; N(R) < 4 \\ \mathrm{H}_1 &: \; N(R) \geq 4 \end{aligned} \tag{17}$$

wherein $N(R)$ represents the number of DPFs (with different PRNs) that are within the predefined range of R. A proper R is crucial to the monitoring performance. As is seen in Figure 4, the improper R would result in either low detection or high false alarm probability. Hence, Section 5.2 determines the minimum R required to achieve a desired detection probability. After the R is determined, an algorithm is developed in Section 5.3 to search for the DPFs that are within the R.



(**a**) R is set too small so that only 2 DPFs are within the R in a spoofing case, leading to low detection probability.



(**b**) R is set too large so that 4 DPFs are within R in the non-spoofing case, leading to a high false alarm probability.

Figure 4. The improper R results in poor monitoring performance.

5.2. The Lower Bound (LB) on the Detection Probability

Based on the hypothesis test, the detection probability (P_d) is defined as the probability that at least 4 spoofing DPFs are within the predefined range R.

$$P_d = \Pr\{N(R) \geq 4\} \tag{18}$$

wherein Pr{x} denotes the probability of the event x. Actually, the P_d increases in the number of the received spoofing signals, m. This is because more spoofing signals results in more spoofing DPFs. Given more spoofing DPFs, more of them will be within R, leading to the higher P_d. Considering that the m cannot be controlled at the monitoring side, this section focuses on the P_d in the worst case, where the m achieves the minimum possible value, 4. The P_d in such worst case is denoted as the lower bound (LB) detection probability, $\widetilde{P}_d$

$$P_d \geq \widetilde{P}_d = \Pr\{N(R) \geq 4 | m = 4\} = \Pr\{N(R) = 4 | m = 4\} \tag{19}$$

The second equality sign is considering the $N(R)$ cannot be larger than 4 because the N(R) always equals or is less than the overall number of DPFs, m. Further, given that the 4 spoofing DPFs will be within R if and only if the range of the 4 DPFs is smaller than R, the $\widetilde{P}_d$ is further written as:

$$\widetilde{P}_d = \Pr\{\text{maximum DPF Element} - \text{ minimum DPF Element } \leq R\} = \Pr\{r(4) \leq R\} \tag{20}$$

wherein $r(x)$ denotes the range of the x spoofing DPFs, which is the difference between the maximum and the minimum DPF element. The cumulative distribution function (cdf) of the $r(4)$, $F_{r(4)}$, is derived in Appendix C and the result is:

$$F_{r(4)}(R) = \Pr\{r(4) \leq R\} = 4\int_{-\infty}^{\infty} g'(x)\left[G'(x + R/\sigma_\delta) - G'(x)\right]^3 dx \tag{21}$$

wherein the g' and G' are respectively the probability density function and the cdf of the zero mean Gaussian with unit variance. Based on Equations (20) and (21), the $\widetilde{P}_d$ can be finally modeled as:

$$\widetilde{P}_d = F_{r(4)}(R) \tag{22}$$

Based on Equation (22), the minimum R can be also determined based on a required detection probability:

$$R = F_{r(4)}^{-1}\left(\widetilde{P}_d\right) \tag{23}$$

Figure 5 gives the $\widetilde{P}_d$ versus the predefined range R and Table 1 gives the minimum R required to achieve the typical desired detection probabilities.

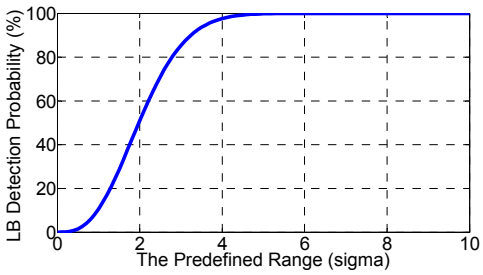


Figure 5. LB detection probability versus the predefined range.

Table 1. The minimum R required to achieve the typical detection probabilities.

LB Detection Probability	99.00%	99.90%	99.99%
Minimum R	$4.4\sigma_\delta$	$5.3\sigma_\delta$	$6\sigma_\delta$

5.3. Algorithm

The algorithm to deal with the hypothesis test follows the 6 steps:

- Define the range R based on Equation (23).
- Sort the calculated DPFs from minimum to maximum: $[k_1 \leq k_2 \leq \ldots \leq k_n]$.
- Generate a counter *cnt* and initialize it as 1.
- Define a search range $[k_{cnt}, k_{cnt} + R]$ and calculate the number of elements within the range.
- If the number equals or is over 4, the presence of spoofing is determined. Otherwise, goes to step 6.
- Update *cnt* as: $cnt = cnt + 1$, and goes to step 4 to test the next range.

Figure 6 gives an example to illustrate the algorithm. As the counter *cnt* is 1, only one element (k_1) is in the search range $[k_1, k_1 + R]$, which means the spoofing has not been found. After the *cnt* is updated as 2, 2 elements (k_2 and k_3) are within the search range $[k_2, k_2 + R]$ and therefore the spoofing has not been found. But after the counter is updated as 3, the number of elements within the search range $[k_3, k_3 + R]$ equals to 4. Hence, the alternate hypothesis H_1 is accepted and the presence of spoofing is identified.

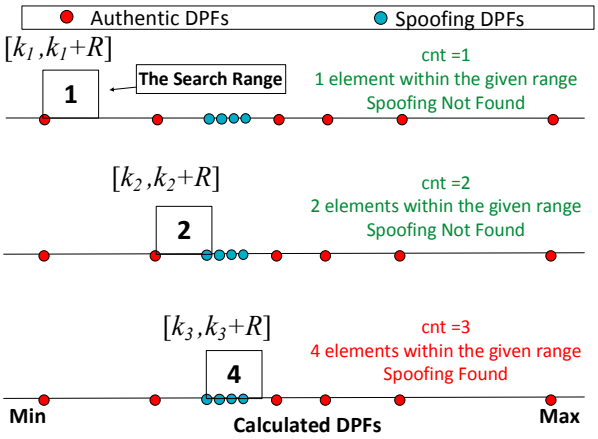


Figure 6. An example to illustrate the spoofing monitoring algorithm.

6. Performance Analysis

The performance of the SNM can be characterized by the lower bound detection probability ($\widetilde{P}_d$) and the false alarm probability (P_{fa}). The $\widetilde{P}_d$ can be determined by the predefined range R, (see Equation (22)). However, the P_{fa} has not yet been tested. Hence, Monte Carlo simulations are conducted in this section to test the P_{fa}. The P_{fa} is defined as the probability that at least 4 authentic DPFs that are within the predefined range R.

6.1. Simulation Setup

The simulation setup is given by Figure 7. The two inputs are respectively the distance between two receivers (d_{12}) and the number of authentic DPFs (l_a). Each DPF is generated based on the model given by Equation (12), wherein the multipath difference is sampled from a $\mathbf{N}[0, 0.3/c]$; the clock difference is sampled from a uniform distribution over the range of [−500 ms, 500 ms]; and the DPF estimation noise is sampled from $\mathbf{N}[0, \sigma_\delta]$. The σ_δ is given by Equation (15), where the pseudorange

noise σ is set as typically 0.2 m according to the GPS UERE (user equivalent range error) budget [27]. The TDOA $\Delta\tau^{a,i}$ is generated as:

$$\Delta\tau^{a,i} = \mathbf{H_i}\Delta\mathbf{x}/c \tag{24}$$

where, $\mathbf{H_i} = [-\cos\theta_i\sin\alpha_i, -\cos\theta_i\cos\alpha_i, -\sin\alpha_i]$, wherein the elevation and azimuth of a GNSS satellite, θ_i and a_i, are randomly sampled over the range of respectively [0,π/2] and [0,2π]. The orientation vector between two receivers $\mathbf{\Delta x}$ is sampled from a uniform distribution on the unit sphere.

Figure 7. Simulation Setup.

6.2. Result

Figure 8 shows the predefined range R versus P_{fa} for various d_{12} and number of authentic signals l_a. As shown, for a given predefined range R, the farther the two receivers are placed, the lower the P_{fa} would be. This is because the TDOAs of authentic signals will be more dispersed with a longer d_{12}, resulting in the decrease of the P_{fa}. On the other hand, a larger number of authentic signals leads to a higher P_{fa}. This is because more authentic signals give more DPFs, and given more DPFs, it will be more likely that at least 4 of them are within the R, resulting in a higher P_{fa}. Also, it is found in Section 5.2 that the predefined range of $6\sigma_\delta$ could give a $\widetilde{P}_d$ of 99.99%. Fortunately, the P_{fa} is also satisfactory for such a range. As is illustrated in Table 2, with the R of $6\sigma_\delta$ (or equivalently, the $\widetilde{P}_d$ of 99.99%), the P_{fa} is no more than 2.5×10^{-3} (for d_{12} = 100 m) or 1.0×10^{-4} (for d_{12} = 300 m).

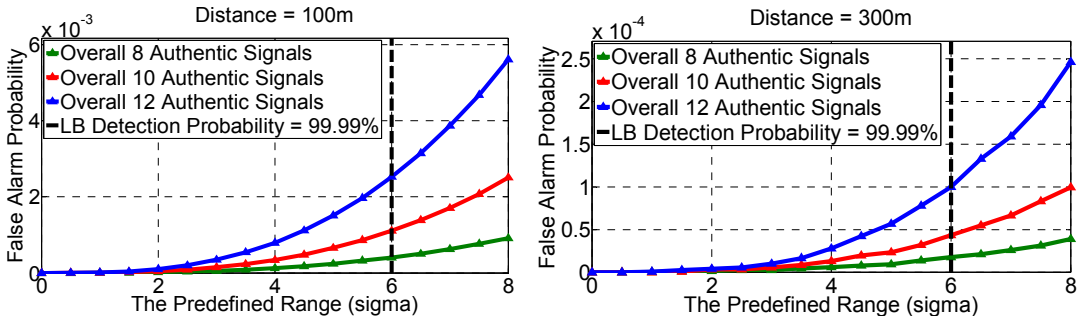


Figure 8. The predefined range versus false alarm probability.

Table 2. Numerical P_{fa} for $R = 6\sigma_\delta$ ($\widetilde{P}_d$ = 99.99%).

	Number of Authentic Signals = 8	**10**	**12**
Distance = 100 m	4.0×10^{-4}	1.1×10^{-3}	2.5×10^{-3}
Distance = 300 m	1.8×10^{-5}	4.3×10^{-5}	1.0×10^{-4}

Figure 9 gives the receiver operating characterization (ROC). It shows that the performance is satisfactory especially for the case that the d_{12} is set as 300 m. It is noted that the false alarm probability shown by the x-axis ranges from 0 to 2×10^{-3} instead of 0 to 1.

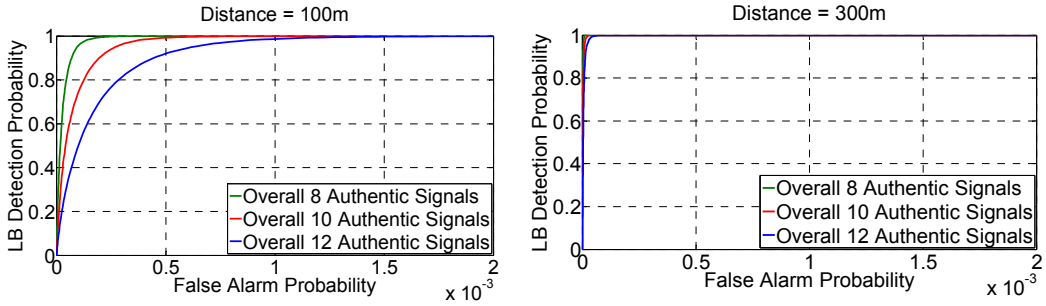


Figure 9. The Receiver Operating Characterization (ROC).

7. Experiments and Results

7.1. Setup

7.1.1. Signal Collection

In this experiment, a Labsat GNSS record & replay is adopted as the spoofer. Two GN3SV2 front ends (FE), FE A and B, are used to collect the Intermediate Frequency (IF) GNSS signals. Each FE is connected to a laptop to collect the signals and the local computer time is used as the receiver time. The ideal setup for the data collection is to put the spoofer and the two front ends outside under a clear view of sky, so that both the spoofing and authentic signals can be collected simultaneously. However, it is challenging to conduct such an experiment as it is illegal to transmit spoofing signals outdoors. Hence, the authentic and spoofing signals are collected separately in this experiment. As is shown in Figure 10, the spoofing signals are collected indoors while the authentic signals are collected under a clear view of the sky, and the distance between the two antennas is 100 m. The PRN set of the collected spoofing and authentic signals are given by Table 3. It shows there are three common elements (14, 25 and 32) between the two sets.

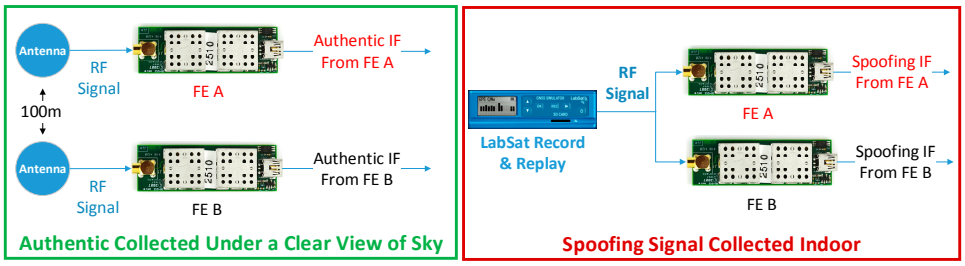


Figure 10. Signal collection: authetic and spoofing signals are collected seperately.

Table 3. The spoofing and authentic PRN sets.

Spoofing:	14,16,25,27,29,30,31,32
Authentic:	06,12,14,17,22,24,25,32

7.1.2. Signal Process

Figure 11 illustrates the workflow of the signal process. As shown, the authentic and spoofing IF signals are respectively fed into a Matlab based software defined radio receiver (SDR) and the outputs are the pseudorange and Doppler measurements. After that, the raw measurements of authentic and spoofing signals from the same FE are combined and are then fed into a spoofing monitoring block.

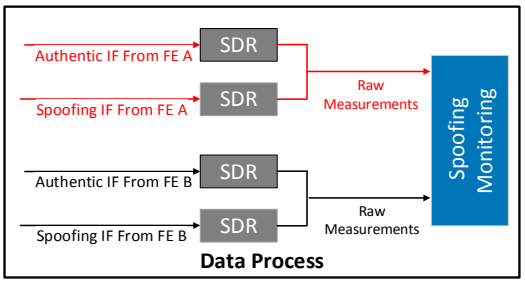


Figure 11. Signal process for spoofing monitoring.

7.1.3. The Limitations of the Adopted Experiment

The 'ideal' experiment discussed before can be expressed by Figure 12, where the spoofer is placed outside under a clear view of sky. By this, the spoofing and authentic signals can be collected and processed by the SDR simultaneously. However, considering conducting such experiment is challenging, the spoofing and authentic IF signals are actually collected and processed separately. The limitation of the adopted experiment is that the modified acquisition process introduced in Section 2 cannot be verified, which is designed to acquire all the signals (spoofing and authentic) simultaneously. Fortunately, such an acquisition process has already been introduced and verified in [10–12]. Besides this limitation, the adopted and the ideal experiment setups are similar. As shown, in both cases, the measurements fed into the spoofing monitoring block include both spoofing and authentic. Hence, the verification of the spoofing monitoring technique will not be influenced.

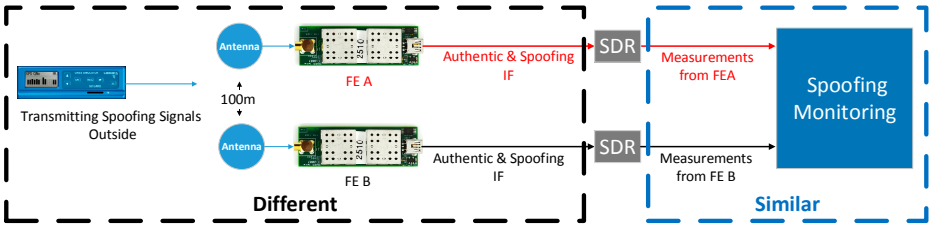
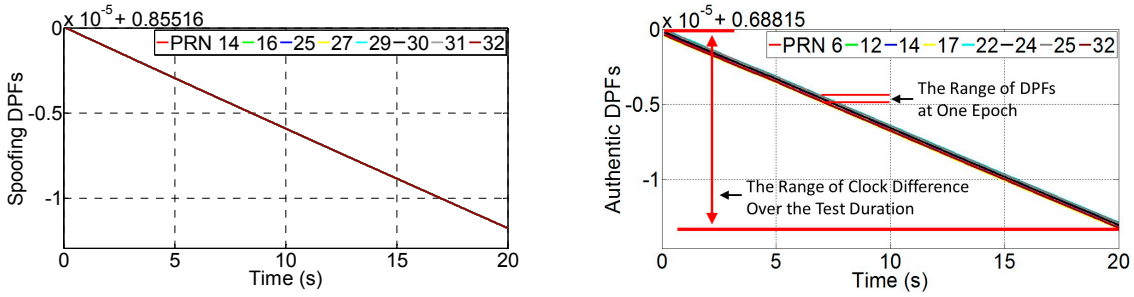


Figure 12. The ideal experimental setup.

7.2. Result

7.2.1. DPF

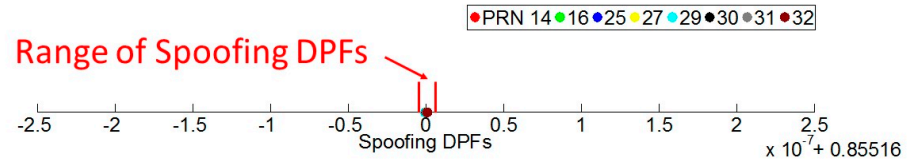
The spoofing monitoring block firstly calculates the DPFs based on the raw measurements. At each epoch, the calculated DPFs include authentic, spoofing and AS DPFs. The spoofing and authentic DPFs are given by Figure 13. It shows all the DPFs decrease over time. This is because each DPF includes clock difference Δt, and it decreases over time due to the clock drift difference. It also shows the spoofing DPFs overlay each other. Note that although the authentic DPFs are actually much more dispersed, it is not obviously illustrated in the figure. This is because the range of the clock difference over the test duration is too large (around 1.5×10^{-5} s) compared with the range of the authentic DPFs (from $-d/c$ to d/c, where d is the distance between two antennas and c is the speed of light). Hence, the authentic DPFs seem to be slightly overlapped even though they are not.



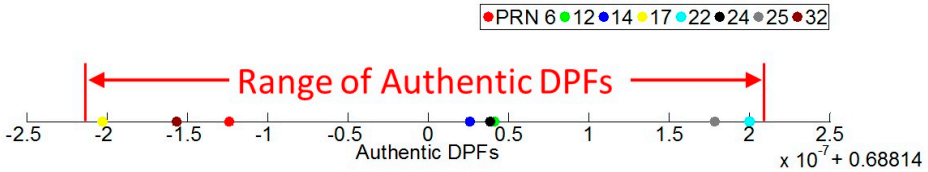
(**a**) Spoofing DPFs (**b**) Authentic DPFs

Figure 13. The DPFs over the test duration.

In order to illustrate the authentic and spoofing DPF range clearly, Figure 14 gives the DPFs at one epoch (corresponding to the 10th second). As seen, the spoofing DPFs given by Figure 14a are overlapped while authentic DPFs given by Figure 14b are much more dispersed. Further, considering the large range of Δt prevents the range of DPFs from being clearly illustrated, the spoofing and authentic DPFs at each epoch are respectively subtracted by their mean values. By this, the clock difference can be removed and the DPF range over the test duration can be clearly illustrated. Note that this subtraction process only aims to show the range clearly. This process does not affect the range of the DPFs because the DPFs at each epoch are subtracted by a common mean value and therefore their range will remain the same. The results are shown in Figure 15. It shows the authentic DPFs are dispersed over a range of approximately 4×10^{-7} while the spoofing DPFs are almost overlapped and are within a range of 3×10^{-9}.

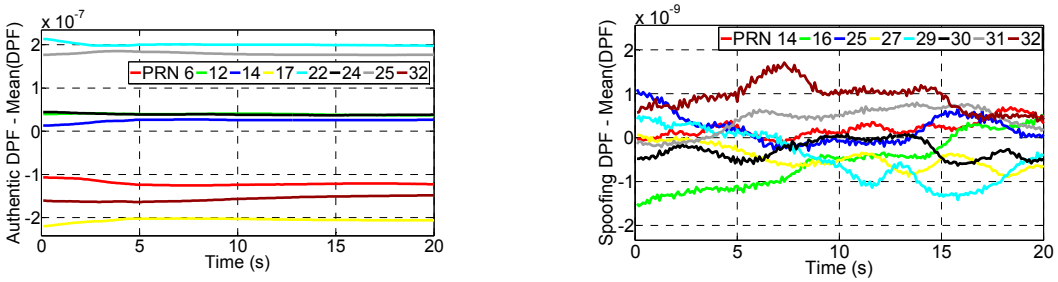


(**a**) Spoofing DPFs



(**b**) Authentic DPFs

Figure 14. The DPFs for one epoch.

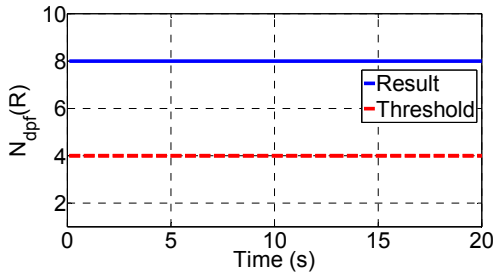


(**a**) Authentic (**b**) Spoofing

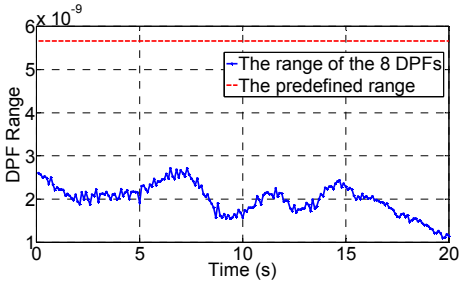
Figure 15. The DPFs are subtracted by their mean value in order to show the DPF range clearly.

7.2.2. Spoofing Monitoring

After the DPFs are calculated, the algorithm introduced in Section 5.3 is performed to test whether there are at least 4 DPFs being within the predefined range that is set as $6\sigma_\delta$. The σ_δ is calculated based on Equation (15), where the pseudorange noise is set as typically 0.2 m according to the UERE budget [27]. The results are given by Figure 16. As shown in Figure 16a, the number of DPFs that are within the predefined range at every epoch, 8, is larger than the threshold of 4. Hence, the existence of spoofing is determined. Figure 16b further gives the range of the 8 DPFs. It shows the range of the 8 DPFs is much smaller than the predefined range.



(**a**) 8 DPFs are found within the predefined range



(**b**) The range of the 8 DPFs

Figure 16. The monitoring result: spoofing is detected because more than 4 DPFs are found within the predefined range.

Additionally, the monitoring methodology has also been tested in the non-spoofing case, where the spoofing measurements are removed and only the authentic measurements are fed into the spoofing monitoring block. The result shows that only 2 DPFs are found within the predefined range, which correspond to the authentic signals with PRN 12 and 24.

8. Discussions and Future Work

The SNM mechanism proposed in the paper are mainly based on two assumptions: (1) multiple spoofing signals are transmitted from a common spoofer/antenna; and (2) there are 4 or more spoofing signals present in the spoofing case. As is validated, the SNM can be effective under the two assumptions. However, the practicalities of the two assumptions are not clearly given in the previous discussions. Hence, this section firstly discusses the rationality of the two assumptions, based on which our future work is recommended.

8.1. The Rationality of the Two Assumptions

8.1.1. Assumption 1: Multiple Fake Signals are Transmitted from a Common Antenna

The proposed SNM mechanism is effective in defending against a single spoofing attack in which multiple spoofing signals are transmitted from a common antenna. Compared with single spoofing, a more advanced spoofing mode is multiple spoofing, which consists of multiple spatially distributed spoofing devices, with each device transmitting a single spoofing signal. In the case of multiple spoofing, however, the TDOA of spoofing signals from various directions will not be overlapped and therefore distinguishing spoofing from authentic signals based on their different TDOA properties becomes impractical, leading to the failure of the proposed SNM mechanism.

Although multiple spoofing could defeat the SNM, such a mode of spoofing is deemed impractical because performing this attack is very challenging [11,13]. In order to defeat the RAIM technique that is currently equipped in most commercial-off-the-shelf (COTS) receivers, the fake pseudoranges (or equivalently the code phases) at the target receiver (s) have to be self-consistent to guarantee small pseudorange residuals. To achieve this, the following three strict requirements need to be satisfied:

(1) the clocks of the spatially distributed spoofers need to be synchronized; (2) the processing delay within each spoofing device should be precisely estimated to achieve nano-second level; (3) the spoofing devices should have sub-meter-level knowledge of the three-dimensional position of the target's antenna phase center. This is almost impossible in the case of moving victim targets. In addition to these three requirements, there are also limitations regarding the placement of the multiple spoofing devices, the cost of the spoofing infrastructure, and the expertise of developing and performing such a spoofing attack.

8.1.2. Assumption 2: There are 4 or More Spoofing Signals Present in the Spoofing Case

The proposed SNM mechanism assumes that there are 4 or more spoofing signals present in the spoofing case, and the presence of spoofing is determined when 4 or more DPFs are found within a predefined small range (or equivalently, overlapped). However, in the case that only a few (less than 4) spoofing signals are present, there will be less than 4 DPFs being overlapped and therefore the SNM mechanism will be failed.

Fortunately, the assumption that there are 4 or more spoofing signals is practical considering the following: if only a few spoofing signals are present (e.g., less than 4), the victim receivers tend to use a combination of spoofing and authentic signals to report PVT solutions. This will lead to the inconsistency among the observed pseudoranges, which can be easily detected by the RAIM [28]. Furthermore, it is not clear how sophisticated the spoofer should be to spoof only a few signals without being detected by RAIM [28]. Although the spoofing might be successful in an extreme scenario, where the signals in view are too few (no more than 4) so that the RAIM is not available (e.g., there are only 4 authentic signals in view and a subset of these signals are spoofed), this scenario is rare and cannot be controlled at the spoofer side. The scenario is highly unlikely for static victims. This is because for static applications such as smart grids, high precision surveys, etc., the receivers are usually placed under a clear view of sky where there are normally sufficient signals (e.g., >10) in view. In terms of moving victims, this scenario is possible, but it is rare and hard to control. For instance, if the targets are moving targets in urban canyons, there might be sometimes no more than 4 visible signals. However, the number of visible signals for moving targets in urban canyon tends to change rapidly. At a certain epoch there are 4 signals in view, but at the next epoch there might be more. Once more than 4 signals are visible, the RAIM becomes available and the spoofing can be detected. And what's worse, the number of visible signals cannot be controlled at spoofing side.

Hence, in order to defeat the RAIM that is equipped in most current COTS receivers, most spoofers tend to transmit 4 or more spoofing signals and induce the target receivers to use only the spoofing signals for PVT calculation.

8.2. Future Work

Although multiple spoofing is deemed impractical at present [11,13], it might become a threat in the future. In order to be more robust against a spoofing attack, further improvement of the SNM should be focused on defending against multiple spoofing attacks.

9. Conclusions

The proposed SNM is based on the differential pseudorange to carrier frequency ratio (DPF), which is mathematically formulated and analyzed in this paper. As shown, the spoofing DPFs are almost overlapped while authentic DPFs are dispersed. Considering both the overlapped spoofing and dispersed authentic DPFs will be present in the spoofing case, the SNM is designed to search for the DPFs that are within the predefined small range. The predefined range could be determined based on the desired detection probability. This shows that a detection probability of 99.99% can be achieved with the predefined range of $6\sigma_\delta$ (σ_δ is the DPF estimation noise). Also, false alarm probabilities are tested based on Monte Carlo simulations. As shown, both the predefined range and the distance between two receivers have great impact on false alarm probabilities. With the predefined range of

$6\sigma_\delta$ and the distance of 300 m, a false alarm rate of 0.01% can be achieved. The effectiveness of the spoofing monitoring technique is validated by real data experiments. It shows that the spoofing DPFs are within a much smaller range than the authentic ones, and overall 8 DPFs are found within the predefined range. This implies the existence of spoofing.

Acknowledgments: This work described in this paper was conducted under The National High Technology Research and Development Program of China (863 Project) (No. 2014AA123103).

Author Contributions: Xingqun Zhan conceived and designed the experiments; Zhenjun Zhang performed the experiments; Zhenjun Zhang analyzed the data; Xingqun Zhan contributed analysis tools; and Zhenjun Zhang wrote the paper.

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

Appendix A

A.1. Spoofing Pseudorange

As shown in the spoofing scenario given by Figure 1, the spoofing pseudorange measurement at rcv_x at receiver time t', $\widetilde{\rho}_x^{s,i}$, can be modelled as:

$$\widetilde{\rho}_x^{s,i}\left(t'\right) = r_x^s + A_x^s + M_x^s + \rho_x^{s,i} + c\Delta t_x + \xi_x^{s,i} \tag{A1}$$

wherein the superscript i denotes the PRN index and c is the speed of light. The pseudorange measurement consists of 6 parts: (1) distance between spoofer and rcv_x: r_x^s; (2) atmosphere delay: A_x^s; (3) multipath delay: M_x^s; (4) the faked pseudorange at rcv_x: $\rho_x^{s,i}$; (5) clock Bias: $c\Delta t_x$; (6) measurement noise: $\xi_x^{s,i}$. The first three parts are altogether considered to be the transmission delay between spoofer and rcv_x, $c\tau_x^s$.

$$c\tau_x^s = r_x^s + A_x^s + M_x^s \tag{A2}$$

Considering that the $\rho_x^{s,i}$ at rcv_x at t' is actually that generated at $t' - \Delta t_x - \tau_x^s$, it can be further modeled as:

$$\begin{aligned} &\rho_x^{s,i}\left(t'\right) = \rho^{s,i}\left(t' - \Delta t_x - \tau_x^s\right) = \rho^{s,i}\left(t'\right) + \left(\Delta t_x + \tau_x^s\right)\dot{\rho}^{s,i} \\ &= \rho^{s,i}\left(t'\right) + \left(\Delta t_x + \tau_x^s\right)\Delta f^{s,i}\lambda \end{aligned} \tag{A3}$$

in which $\dot{\rho}^{s,i}$ is the pseudorange rate, which is a product of the faked Doppler $\Delta f^{s,i}$ and GNSS carrier wavelength λ. By substituting Equations (A2) and (A3) into Equation (A1), the spoofing pseudorange estimation model becomes:

$$\begin{aligned} \widetilde{\rho}_x^{s,i}\left(t'\right) &= \left(c + \Delta f^{s,i}\lambda\right)\left(\tau_x^s + \Delta t_x\right) + \rho^{s,i}\left(t'\right) + \xi_x^{s,i} \\ &= \tfrac{1}{c}\left(c + \Delta f^{s,i}\lambda\right)\left[r_x^s + A_x^s + M_x^s + c\Delta t_x\right] + \rho^{s,i}\left(t'\right) + \xi_x^{s,i} \end{aligned} \tag{A4}$$

Further, the c can be modelled as a product of λ and the GNSS carrier frequency f (e.g., 1.57542 GHz for GPS L1 signal): $c = \lambda f$. Hence, the Equation (A4) can be modified as:

$$\widetilde{\rho}_x^{s,i}\left(t'\right) = \frac{1}{c}\lambda f^{s,i}\left(r_x^s + A_x^s + M_x^s + c\Delta t_x\right) + \rho^{s,i}\left(t'\right) + \xi_x^{s,i} \tag{A5}$$

where

$$f^{s,i} = f + \Delta f^{s,i} \tag{A6}$$

A.2. Authentic Pseudorange

The authentic pseudorange measurement at rcv_x at receiver time t', $\widetilde{\rho}_x^{a,i}$ can be modelled as:

$$\widetilde{\rho}_x^{a,i}\left(t'\right) = r_x^{a,i} + A_x^{a,i} + M_x^{a,i} + c\Delta t_x + \xi_x^{a,i} \tag{A7}$$

The $\widetilde{\rho}_x^{a,i}$ consists of 5 parts: (1) distance between satellite and rcv_x: $r_x^{a,i}$; (2) atmosphere delay, $A_x^{a,i}$; (3) multipath delay: $M_x^{a,i}$; (4) clock bias: $c\Delta t_x$; (5) measurement noise: $\xi_x^{a,i}$. The first three parts are altogether considered as the transmission delay between satellite i and rcv_x, $c\tau_x^{a,i}$:

$$c\tau_x^{a,i} = r_x^{a,i} + A_x^{a,i} + M_x^{a,i} \tag{A8}$$

Considering the authentic signal received at receiver time t', is actually that generated at the time of $t' - \Delta t_x - \tau_x^{a,i}$, the $r_x^{a,i}$ is actually the distance between satellite and rcv_x at time $t' - \Delta t_x - \tau_x^{a,i}$:

$$\begin{aligned} r_x^{a,i} &= r_x^{a,i}\left(t' - \Delta t_x - \tau_x^{a,i}\right) = r_x^{a,i}\left(t'\right) + \left(\Delta t_x + \tau_x^{a,i}\right) v^{a,i} \\ &= r_x^{a,i}\left(t'\right) + \left(\Delta t_x + \tau_x^{a,i}\right) \Delta f^{a,i} \lambda \end{aligned} \tag{A9}$$

in which the $v^{a,i}$ is the relative velocity between the satellite and rcv_x, which is a product of carrier Doppler $\Delta f^{a,i}$ and λ. By combining Equations (A8) and (A9), $c\tau_x^{a,i}$ is further deducted as:

$$c\tau_x^{a,i} = \frac{c}{\left(c - \lambda\Delta f^{a,i}\right)}\left[r_x^{a,i}\left(t'\right) + \Delta t_x \Delta f^{a,i}\lambda + A_x^{a,i} + M_x^{a,i}\right] \tag{A10}$$

By combining Equations (A7), (A8) and (A10), $\widetilde{\rho}_x^{a,i}$ becomes:

$$\begin{aligned} \widetilde{\rho}_x^{a,i}\left(t'\right) &= \tfrac{c}{\left(c-\lambda\Delta f^{a,i}\right)}\left[r_x^{a,i}\left(t'\right) + \Delta t_x \Delta f^{a,i}\lambda + A_x^{a,i} + M_x^{a,i}\right] + c\Delta t_x + \xi_x^{a,i} \\ &= \tfrac{c}{\left(c-\lambda\Delta f^{a,i}\right)}\left[r_x^{a,i}\left(t'\right) + A_x^{a,i} + M_x^{a,i} + c\Delta t_x\right] + \xi_x^{a,i} \\ &= \tfrac{1}{\left(c-\left(\lambda\Delta f^{a,i}\right)^2/c\right)}\left(c + \lambda\Delta f^{a,i}\right)\left[r_x^{a,i}\left(t'\right) + A_x^{a,i} + M_x^{a,i} + c\Delta t_x\right] + \xi_x^{a,i} \\ &\approx \tfrac{1}{c}\left(c + \lambda\Delta f^{a,i}\right)\left[r_x^{a,i}\left(t'\right) + A_x^{a,i} + M_x^{a,i} + c\Delta t_x\right] + \xi_x^{a,i} \end{aligned} \tag{A11}$$

wherein considering the maximum received Doppler for a static receiver is 7 kHz, the $\left(\lambda\Delta f^{a,i}\right)^2/c$ in the denominator is neglected as it is way smaller than c. Also, considering $c = \lambda f$, the Equation (A11) is rewritten as:

$$\widetilde{\rho}_x^{a,i}\left(t'\right) = \frac{1}{c}\lambda f^{a,i}\left[r_x^{a,i}\left(t'\right) + A_x^{a,i} + M_x^{a,i} + c\Delta t_x\right] + \xi_x^{a,i} \tag{A12}$$

where,

$$f^{a,i} = f + \Delta f^{a,i} \tag{A13}$$

Appendix B

By substituting Equation (A6) into Equation (13), $\delta^{s,i}$ becomes:

$$\delta^{s,i} = \frac{\Delta\xi^{s,i}}{\lambda\left(f + \Delta f^{s,i}\right)} = \frac{\Delta\xi^{s,i}}{\lambda f}\left[\frac{1}{1 + \Delta f^{s,i}/f}\right] \tag{B1}$$

Considering that the $\Delta f^{s,i}$ (typically −7 k–7 kHz) is much smaller than the f (1.57542 GHz), the $\delta^{s,i}$ is further given as:

$$\delta^{s,i} = \Delta\xi^{s,i}/\left(\lambda f\right) = \Delta\xi^{s,i}/c \tag{B2}$$

wherein the second equals sign is considering the product of the GNSS frequency and wavelength equals to the speed of light: $c = \lambda f$. Further, based on the zero mean Gaussian distributed $\Delta\xi^{s,i}$ given by Equation (9), the spoofing DPF noise $\delta^{s,i}$ is modelled as a zero-mean Gaussian distribution. Likewise, the $\delta^{a,i}$ can be modelled as the same way and the results are:

$$\delta^{s,i} \sim \mathbf{N}\left[0, \sigma_\delta\right], \delta^{a,i} \sim \mathbf{N}\left[0, \sigma_\delta\right] \tag{B3}$$

where $\sigma_\delta = \sqrt{2}\sigma/c$

Appendix C

The range of n random variables, X_1, X_2, ..., X_n , is defined as the difference between the maximum and the minimum of these variables [29]: $r_x = max(X_i) - min(X_i)$. For n identically and independently distributed variables, the cumulative distribution function (cdf) of the range is given by [29]:

$$F_{r_X(n)}(t) = \Pr\{r_X \leq t\} = n\int_{-\infty}^{\infty} l(x)\left[L(x+t) - L(x)\right]^{n-1} dx \tag{C1}$$

wherein the $l(x)$ and $L(x)$ are respectively the probability density function (pdf) and the cdf of the distribution of X_i. Since it is analyzed in Section 4 that the spoofing DPFs are identically and independently Gaussian distributed, the cdf of the range of the m spoofing DPFs, $F_{r(m)}$, can be modelled based on Equation (C1):

$$F_{r(m)}(R) = \Pr\{r(m) \leq R\} = m\int_{-\infty}^{\infty} g(x)\left[G(x+R) - G(x)\right]^{m-1} dx \tag{C2}$$

wherein $r(m)$ denotes the range of the m spoofing DPFs, the g and G are the pdf and cdf of the spoofing DPF distribution, which is the Gaussian distribution with the standard deviation of σ_δ (see Equation (15)). The $F_{r(m)}$ can be further derived as:

$$F_{r(m)}(R) = m\int_{-\infty}^{\infty} g\prime(x)\left[G\prime(x + R/\sigma_\delta) - G\prime(x)\right]^{m-1} dx \tag{C3}$$

wherein the g' and G' are respectively the pdf and cdf of the zero mean Gaussian distribution with unit variance. Based on this model, the cdf of the range for a case in which the number of spoofing DPFs is m = 4 can be modelled as:

$$F_{r(4)}(R) = 4\int_{-\infty}^{\infty} g\prime(x)\left[G\prime(x + R/\sigma_\delta) - G\prime(x)\right]^{3} dx \tag{C4}$$

References

1. John, A. *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*; Volpe National Transportation Systems Center: Cambridge, MA, USA, 2001.
2. Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle. *GPS World* **2012**, *23*, 30–33.
3. Proctor, A.G.; Curry, C.W.T.; Tong, J.; Watson, R.; Greaves, M.; Cruddace, P. Protecting the UK infrastructure: A system to detect GNSS jamming and interference. *Inside GNSS* **2011**, *September/October*, 49–57.
4. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.; Kintner, P.M., Jr. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In Proceedings of the ION GNSS International Technical Meeting of the Satellite Division, Savannah, GA, USA, 16–19 September 2008.
5. Psiaki, M.L.; Humphreys, T.E. GNSS spoofing and detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
6. Lo, S.; De Lorenzo, D.; Enge, P.; Akos, D.; Bradley, P. Signal authentication: A secure civil GNSS for today. *Inside GNSS* **2009**, *4*, 30–39.
7. Wesson, K.; Rothlisberger, M.; Humphreys, T.E. Practical cryptographic civil GPS signal authentication. *Navig. J. Inst. Navig.* **2012**, *59*, 177–193. [CrossRef]
8. Humphreys, T.E. Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Trans. Aerosp. Electron. Syst.* **2013**, *49*, 1073–1090. [CrossRef]
9. Nielsen, J.; Broumandan, A.; Lachapelle, G. Method and System for Detecting GNSS Spoofing Signals. U.S. Patent 7,952,519 B1, 31 May 2011.

10. Nielsen, J.; Broumandan, A.; Lachapelle, G. GNSS spoofing detection for single antenna handheld receivers. *Navig. J. Inst. Navig.* **2011**, *58*, 335–344. [CrossRef]
11. Broumandan, A.; Jafarnia, A.; Dehghanian, V.; Nielsen, J.; Lachapelle, G. GNSS spoofing detection in handheld receivers based on signal spatial correlation. In Proceedings of the 2012 IEEE/ION Position Location and Navigation Symposium (PLANS), Myrtle Beach, SC, USA, 23–26 April 2012; pp. 479–487.
12. 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]
13. Ledvina, B.M.; Bencze, W.J.; Galusha, B.; Miller, I. An in-line anti-spoofing device for legacy civil GPS receivers. In Proceedings of the 2010 International Technical Meeting of The Institute of Navigation, San Diego, CA, USA, 25–27 January 2010; pp. 698–712.
14. Wesson, K.D.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In Proceedings of the 2011 ION GNSS, Portland, OR, USA, 20–23 September 2011; pp. 2646–2656.
15. Akos, D.M. Who's Afraid of the Spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *Navigation* **2012**, *59*, 281–290.
16. Jafarnia, J.A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. Pre-despreading authenticity verification for GPS L1 C/A signals. *Navigation* **2014**, *61*, 1–11. [CrossRef]
17. Psiaki, M.L.; O'Hanlon, B.W.; Powell, S.P.; Bhatti, J.A.; Wesson, K.D.; Humphreys, T.E.; Schofield, A. GNSS spoofing detection using two-antenna differential carrier phase. In Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014), Tampa, FL, USA, 8–12 September 2014.
18. Swaszek, P.F.; Hartne, R.J. Spoof detection using multiple COTS receivers in safety critical applications. In Proceedings of the 2013 ION GNSS+, Nashville, TN, USA, 16–20 September 2013.
19. Swaszek, P.F.; Richard, J.H. A multiple COTS receiver GNSS spoof detector—Extensions. In Proceedings of the 2014 International Technical Meeting of the Institute of Navigation, San Diego, CA, USA, 27–29 January 2014.
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.
21. Tippenhauer, N.O.; Pöpper, C.; Rasmussen, K.B.; Capkun, S. On the requirements for successful GPS spoofing attacks. In Proceedings of the ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 75–86.
22. Radin, S.D.; Swaszek, P.F.; Seals, K.C.; Hartnett, R.J. GNSS spoof detection based on pseudoranges from multiple receivers. In Proceedings of the 2015 International Technical Meeting of The Institute of Navigation, Dana Point, CA, USA, 26–28 January 2015; pp. 657–671.
23. Montgomery, P.Y.; Humphreys, T.E.; Ledvina, B.M. A multi-antenna defense receiver autonomous GPS spoofing detection. *Inside GNSS* **2009**, *4*, 40–46.
24. Kaplan, E.D. *Understanding GPS: Principles and Applications*; Artech House: Norwood, MA, USA, 1996.
25. Neagoe, T.; Cristea, V.; Banica, L. NTP versus PTP in computer networks clock synchronization. In Proceedings of IEEE International Symposium on Industrial Electronics, Montreal, QC, Canada, 9–13 July 2006; pp. 317–362.
26. Parkinson, B.W.; Spilker, J.J.; Axelrad, P.; Enge, P. *Global Positioning System: Theory and Applications*; American Institute of Aeronautics and Astronautics Inc.: New York, NY, USA, 1996.
27. Enge, P.K. The global positioning system: Signals, measurements, and performance. *Int. J. Wirel. Inf. Netw.* **1994**, *1*, 83–105. [CrossRef]
28. Psiaki, M.L.; Powell, S.P.; O'Hanlon, B.W. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 16–20 September 2013; pp. 2949–2991.
29. Tsimashenka, I.; Knottenbelt, W.; Harrison, P. Controlling variability in split-merge systems. In Proceedings of the International Conference on Analytical and Stochastic Modeling Techniques and Applications, Grenoble, France, 4–6 June 2012.