sensors

MDPI

Article

Detection of Induced GNSS Spoofing Using S-Curve-Bias

Wenyi Wang [1,*], Na Li [1], Renbiao Wu [1] and Pau Closas [2]

[1] Tianjin Key Lab for Advanced Signal Processing, Civil Aviation University of China, Tianjin 300300, China; nali_nasy@163.com (N.L.); rbwu@vip.163.com (R.W.)

[2] Electrical & Computer Engineering Department, Northeastern University, 360 Huntington Avenue, Boston, MA 02115, USA; closas@northeastern.edu

* Correspondence: wenyi_wang@126.com; Tel.: +86-22-2409-2451

Received: 16 January 2019; Accepted: 18 February 2019; Published: 22 February 2019

Abstract: In Global Navigation Satellite System (GNSS), a spoofing attack consists of forged signals which possibly cause the attacked receivers to deduce a false position, a false clock, or both. In contrast to simplistic spoofing, the induced spoofing captures the victim tracking loops by gradually adjusting it's parameters, e.g., code phase and power. Then the victims smoothly deviates from the correct position or timing. Therefore, it is more difficult to detect the induced spoofing than the simplistic one. In this paper, by utilizing the dynamic nature of such gradual adjustment process, an induced spoofing detection method is proposed based on the S-curve-bias (SCB). Firstly, SCB in the inducing process is theoretically derived. Then, in order to detect the induced spoofing, a detection metric is defined. After that, a series of experiments using the Texas spoofing test battery (TEXBAT) are performed to demonstrate the effectiveness of the proposed algorithm.

Keywords: global navigation satellite system (GNSS); induced spoofing; S-curve-bias (SCB); Texas spoofing test battery (TEXBAT)

1. Introduction

Global navigation satellite system (GNSS) is a general term for various satellite-based navigation systems and their augmentation systems. The application of GNSS is omnipresent, including mobile phone location, the smart grid, emergency rescue, fishing operation, precision guidance and strike of weapons, the transport and management of air, sea and ground and so on [1]. In addition, a great deal of new applications based on GNSS are constantly emerging. Taking into account the significance of GNSS applications, its security becomes a pressing issue [2]. GNSS signals broadcasted by the constellations arrive at the antenna with an extremely low signal power level, e.g., approximately 20 dB lower than the noise. Therefore, it is highly susceptible to various types of interferences. As a special form of interference, spoofing does great harm to GNSS. Recent successful implementations of spoofing tests have further enhanced the awareness of the harm of spoofing attacks [3,4]. Spoofers utilize the open transparency and predictability of GNSS civilian signals to generate spoofing signals which have similar signal structure as authentic ones. Thus they can induce a victim receiver to believe that they are authentic signals and provide incorrect navigation messages or incorrect pseudo-ranges to forge a localition solution at the receiver. It is hard for a conventional GNSS receiver to detect the spoofing attack, which may lead to incorrect position or timing information.

There is a rich literature studying this issue. A representative team comes from the radionavigation laboratory in the University of Texas at Austin [5–8]. According to references [9,10], the type of spoofing is classified as simplistic, intermediate, and sophisticated, depending on their complexity and the level of robustness required to the related anti-spoofing techniques. A simplistic spoofing basically consists of a GNSS signal generator that emits signals which are visually inconsistent (in frequency, phase, code,

and data message) with authentic satellite signals. For the simplistic spoofing, in order to successfully attack the victim receivers, it usually needs to first use jamming to unlock the receiver. Then the victim receivers will lock on the forced signal in the process of recapture. The intermediate and sophisticated spoofing adds synchronization blocks, which makes the counterfeit signals consistent with the real ones and result in spoofing attacks which are more difficult to detect. Furthermore, the sophisticated spoofing attack can be accomplished by using multiple transmitting antennas [11], in which case different forged satellite signals can come from different directions. The design and implementation of a multiple-antenna spoofing device is not simple and may seem laborious.

In this paper, we focus on the induced spoofing, e.g., GPS L1 C/A signals, where the counterfeit signals are consistent with the real ones, but transmitted with a single antenna. Thus the induced spoofing belongs to intermediate spoofing [12]. The induced spoofing captures the victim tracking loops by gradually adjusting it's parameters, e.g., code phase and power. Then the victims smoothly deviate from the correct position or timing [13,14]. Therefore, for the conventional receiver, this kind of spoofing is more subtle and will not lead to an unlock in the tracking loop. Figure 1 shows the correlation peak superposition process of the tracking loop correlator in a victim receiver. Figure 1a is the beginning of adjustment process, the spoofing lags the authentic signal by two chips with a lower power and the same frequency, but a different code rate. From Figures 1a–c, the spoofing gradually approaches the authentic signal in code phase. At the same time, the power is gradually increased but is still lower than that of the authentic signal until it is synchronized with the authentic signal in code phase and carrier frequency. Subsequently, the spoofing slowly increases the power beyond that of the authentic signal, pulls off the authentic signal towards right until the receiver is completely controlled by the spoofing as shown in Figure 1d–f. In Figure 1f, it is about two chips code phase ahead of the authentic signal. In fact, the spoofing only needs a slightly higher power to assure a successful locking of the victim receiver. Since the tracking loop maintains lock in this spoofing process, it would lead to an incorrect position or timing for the victim receiver, while no loss of lock will be detected by a conventional GNSS receiver.

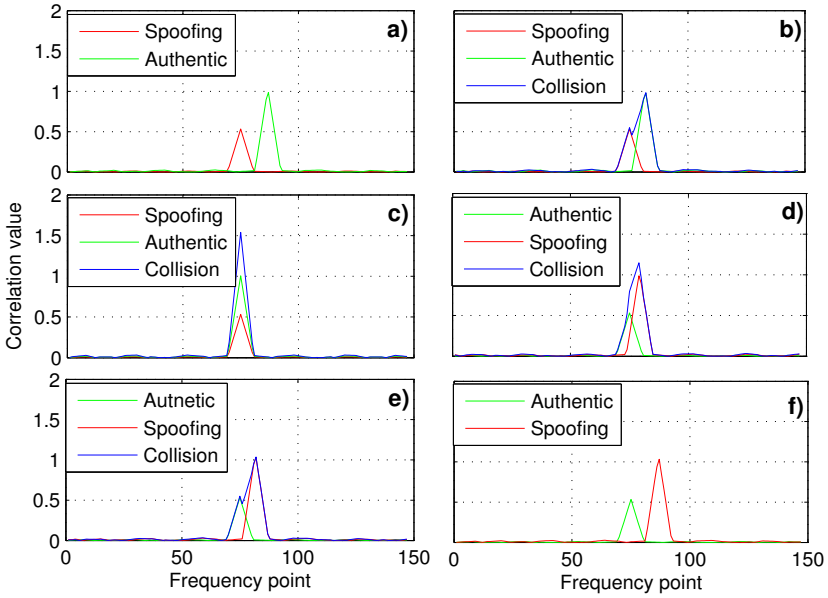

Figure 1. Schematic diagram of the induced spoofing attack process. In (**a**), the spoofing lags the authentic signal with a lower power. From (**a**) to (**c**), the spoofing gradually approaches the authentic signal. Subsequently, the power of spoofing is greater than that of the authentic signal and the receiver is gradually controlled by the spoofing in (**d**–**f**).

The existing anti-spoofing methods can be roughly divided into two categories, namely, detection techniques and suppression techniques. Among them, the detection techniques are designed to identify whether the receiver has been subjected to a spoofing attack, and the purpose of suppression techniques is to help the victim receiver restore its positioning and navigation capability. Here, the existing spoofing detection techniques are briefly reviewed, including spatial-based detection techniques, signal power detection techniques, navigation information detection techniques, integrated navigation detection techniques, encryption authentication techniques, and signal quality monitoring techniques.

Spatially-based detection techniques utilize the characteristics of the spoofer, which transmits multiple satellite signals with the same antenna. On the contrary, the authentic satellite signals come from different directions. Therefore, the spoofing signals are spatially coherent and the spoofing can be identified by determining the correlation degree among satellite signals through a spatial processing technique [15–17]. Such techniques are typically costly to implement, since they require the use of multi-antenna receivers and large observation intervals.

For signal power detection techniques, the receivers continuously monitor the power related parameters and declare a spoofing attack when there is an outlier. The parameters related to power include carrier-to-noise ratio [18,19], absolute power, and distribution checks of correlator outputs [20]. These techniques require the receiver to have a high accuracy in measuring parameters of the received signal, and the hardware complexity of the receiver will also increase correspondingly.

Navigation information detection techniques detect signal code rate and phase rate. For the real satellite signals, the Doppler frequency and code rate are generated by the relative motion between the GNSS satellites and the receiver, thus the two have consistency [21,22]. Simple spoofing can not keep the consistency of Doppler frequency and code rate. When there is inconsistency between them, it is decided to suffer from a spoofing attack. This method is invalid for intermediate and sophisticated spoofing attacks because they overcome such consistency checks.

Integrated navigation detection techniques involve combinations of GNSS signals and other navigation devices, which assist the receiver to identify spoofing effectively [23]. This techniques increase the complexity of GNSS receiver's hardware and software.

Most encryption authentication techniques need to change the structure of GNSS signals and this techniques can not be applied in a short time [24–26]. Signal quality monitoring techniques determine whether there is interference by monitoring the correlation distortion of the tracking loop according to the pseudo-code's auto-correlation property [7,24,26] or even pre-correlation signal quality [27,28]. Several metrics are also proposed in literature [29–31]. These techniques, originally designed for multipath detection [32], were recently found to be useful to identify the deformation on the correlation function due to an intermediate spoofing attack. They generally have simple structures with low complexity, showing good feasibility. As in [33–36], the ratio test metric is used as a measurement compared with predefined thresholds to judge the correlation distortion during the spoofing signals hauling process. However, when the signal's intervals are large, the two signals are not overlapping, and need to wait until distortion occurs. This means that the method is simple but has a large detection time.

In the field of GNSS signal quality evaluation, there are a series of evaluation parameters for judging whether the signal quality is abnormal. Signal correlation domain analysis indexes have a correlation curve, correlation loss, S-curve-bias (SCB), etc. [37]. SCB is an index that can be used to describe the correlation distortion. Specially, SCB is used to describe the deviation between the highest peak and the symmetric point of the correlation curve. The code loop discriminator curve usually locks in the place where the phase is biased, causing SCB. The bias generally results from the influence of the channel transmission distortion and the nonlinear effects of power amplifiers or multipaths. The correlation peak of an induced spoofing attack is similar to such an abnormal signal. Thus SCB has the potential ability to detect spoofing.

In this paper, by utilizing the dynamic feature of gradual adjustment process, an induced spoofing detection method is proposed based on SCB. The main work of this paper is briefly described as

follows. In order to obtain the changing process of SCB, it is derived theoretically for induced spoofing. The theoretical results reflect the whole changing process of induced spoofing. It should be noted that multipath signals can also result in the SCB changing. However, the changing process of multipath is not generally similar with that of induced spoofing. From this point of view, the proposed algorithm is not sensitive to multipath signals in most cases. In addition, front-end filter of receiver may lead to significant SCB variations. However, since only dynamic changes in the SCB are relevant for our method, the the proposed algorithm is also robust to SCB due to the front-end filter. Then a metric is defined to detect induced spoofing. The performance of the proposed algorithm is evaluated with the Texas spoofing test battery (TEXBAT) [38], which has been used to evaluate performance of spoofing detection methods in many papers. In addition, the proposed algorithm is compared with another algorithm based on the ratio test metric, which utilizes the track loop's correlation distortion.

The paper is organized as follows. The signal model is presented in Section 2. The proposed algorithm is derived in Section 3. Section 4 provides experimental results with the TEXBAT data sets. Conclusions are drawn in Section 5.

2. Signal Model

For most GNSS receivers, the received radio frequency (RF) signals will be converted to intermediate frequency (IF) signals. Subsequent processing will be based on the IF signals. When there is an induced spoofing, for a given receiver with single antenna, the received IF signal can be denoted as:

$$x\left(t\right) = x_a\left(t\right) + x_s\left(t\right) + x_n\left(t\right), \tag{1}$$

where $x\left(t\right)$ is the received IF signal, t is time in seconds, $x_a\left(t\right)$ and $x_s\left(t\right)$ are separately authentic satellite signal and spoofing, $x_n\left(t\right)$ denotes the additive white Gaussian noise (AWGN) with zero mean and variance σ^2.

The authentic satellite signal is modeled as:

$$x_a\left(t\right) = \sum_{i=1}^{M} \sqrt{P_i^a} D_i^a\left(t - \tau_i^a\right) C_i\left(t - \tau_i^a\right) \cos\left(2\pi\left(f_0 + f_{d,i}^a\right) t + \phi_i^a\right), \tag{2}$$

where M is the number of authentic satellites included in the received signal, P_i^a is the received power of the i-th satellite, and $D_i^a\left(t\right)$ is the ± 1-valued i-th signal's data bit stream, $C_i\left(t\right)$ is its ± 1-valued spreading code, τ_i^a is the i-th signal's code phase, f_0 is the intermediate frequency, $f_{d,i}^a$ denotes the Doppler shift of the i-th authentic satellite signal in Hertz, and ϕ_i^a is its initial carrier phase.

It is known that induced spoofing has the same signal structure as the authentic satellite signal. Therefore, the spoofing can generally be modeled as:

$$x_s\left(t\right) = \sum_{i=1}^{N} \sqrt{P_i^s} D_i^s\left(t - \tau_i^s\right) C_i\left(t - \tau_i^s\right) \cos\left(2\pi\left(f_0 + f_{d,i}^s\right) t + \phi_i^s\right), \tag{3}$$

where N is the number of satellites included in the spoofing, P_i^s is the received power of i-th satellite, and $D_i^s\left(t\right)$ is the ± 1-valued i-th signal's data bit stream, τ_i^s is the i-th signal's code phase, $f_{d,i}^s$ denotes the Doppler shift of the i-th authentic satellite signal in hertz, and ϕ_i^s is its initial carrier phase. For notational simplicity, the time indication of some parameters, e.g., $f_{d,i}^s$, have been omitted.

For the success of an attack, the spoofing will include most of the satellites in the authentic ones. For the i-th satellite signal, the core of GNSS signal processing is the correlation of the received signal with local replica:

$$\ell_i\left(t, \tau_i\right) = C_i\left(t - \hat{\tau}_i^a\right) \cos\left(2\pi\left(f_0 + \hat{f}_{d,i}^a\right) t + \hat{\phi}_i^a\right) \tag{4}$$

where $\hat{\tau}_i^a$, $\hat{f}_{d,i}^a$ and $\hat{\phi}_i^a$ are separately the estimated τ_i^a, $f_{d,i}^a$, and ϕ_i^a. The goal of a receiver's tracking loops is to accurately drive the estimates $\hat{\tau}_i^a$, $\hat{f}_{d,i}^a$ and $\hat{\phi}_i^a$. It is well known that these parameters are

estimated based on the outputs of correlators in tracking loops. However, when there is an induced spoofing, there will be a distortion on the correlator outputs. Therefore, the tracking loops cannot accurately obtain the estimations.

For the case of a GPS L1 C/A signal, through carrier wipe-off and coherent integration of one millisecond, the cross-correlation function of the local replica and the authentic signal can be written as:

$$R\left(\tau'\right) = \begin{cases} 1 - \left|\tau'\right|, & \left|\tau'\right| \leq 1 \\ 0, & \text{otherwise,} \end{cases} \tag{5}$$

where $\tau' = \hat{\tau}^a - \tau^a$ denotes the code phase lag in chips. It is noted that, for the sake of simplicity, the subscript i has been omitted.

At the beginning of induced spoofing, it is assumed that the spoofing lags behind the authentic signal Δ_c chips. Thus the corresponding cross-correlation of the induced spoofing with the local replica can be expressed as:

$$R\left(\tau' - \left(\Delta_c - \Delta_r t\right)\right) = \begin{cases} 1 - \left|\tau' - \left(\Delta_c - \Delta_r t\right)\right|, & \left|\tau'\right| \leq 1 \\ 0, & \text{otherwise,} \end{cases} \tag{6}$$

where Δ_r is the code rate difference between the induced spoofing and the authentic signal.

Therefore, the correlator output for prompt channel with neglected carrier phase error is shown below:

$$P\left(\tau'\right) = \sqrt{P^a} R\left(\tau'\right) \operatorname{sinc}\left(\Delta f_d^a\right) + \sqrt{P^s} R\left(\tau' - \left(\Delta_c - \Delta_r t\right)\right) \operatorname{sinc}\left(\Delta f_d^s\right) + \tilde{n}, \tag{7}$$

where $\operatorname{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$, $\Delta f_d^a = \hat{f}_d^a - f_d^a$ and $\Delta f_d^s = \hat{f}_d^a - f_d^s$ are the Doppler shift residuals of the authentic signal and the spoofing, respectively. The $\tilde{n}$ comes from AWGN and cross-correlation results between local replica and other satellite signals, which can be expressed as the following:

$$\tilde{n} = \int_0^1 x_n \ell_i\left(t, \tau_i\right) dt + \sum_{j \neq i} \int_0^1 x_{a,j} \ell_i\left(t, \tau_i\right) dt + \sum_{j \neq i} \int_0^1 x_{s,j} \ell_i\left(t, \tau_i\right) dt, \tag{8}$$

where $x_{a,j}$ and $x_{s,j}$ are separately the j-th satellite signal including in the authentic signal and spoofing.

It is assumed that the receiver has stably tracked the authentic signal before the induced spoofing attack. At the same time, for simplicity, it is assumed that the Doppler frequency of the spoofing signal is the same as that of authentic signal, which is called a "frequency lock" in reference [39]. Then the correlation value of the prompt channel is modeled as:

$$P\left(\tau'\right) = \sqrt{P^a} R\left(\tau'\right) + \sqrt{P^s} R\left(\tau' - \left(\Delta_c - \Delta_r t\right)\right) + \tilde{n}. \tag{9}$$

3. Detection of Induced Spoofing

3.1. The Proposed Method

In the correlation domain analysis of navigation signal quality, SCB is a common index to measure the navigation ranging error [37]. S-curve refers to the code-discriminatior curve of the early–late correlation value in the receiver code tracking loop, which varies with the different code-discriminator algorithms. The theoretical zero-crossing point of S-curve was located at the zero point of code tracking error. In fact, due to the influence of channel transmission distortion and nonlinear effect of the power amplifier, the discriminatior curve of code loop was usually locked in the place where a code phase deviation existed, resulting in SCB.

Assume that correlator spacing is d, the non-coherent power discriminator's S-curve can be defined by the following formula [37]:

$$S_c\left(\varepsilon\left(t\right),d\right)=\left|P\left(\varepsilon\left(t\right)-\frac{d}{2}\right)\right|^2-\left|P\left(\varepsilon\left(t\right)+\frac{d}{2}\right)\right|^2 \tag{10}$$

where $P\left(\cdot\right)$ is the correlation value between the received signal and local replica, the code phase difference between local replica and prompt channel is the argument of the correlation operator, and $\varepsilon\left(t\right)$, i.e., SCB, satisfied with the following formula:

$$\varepsilon\left(t\right)=\arg\left\{S_c\left(\varepsilon\left(t\right),d\right)=0\right\}. \tag{11}$$

It should be noted that $\varepsilon\left(t\right)$ changes with time when there is induced spoofing.

According to Equations (8) and (9), we can get:

$$\begin{aligned}S_c\left(\varepsilon\left(t\right),d\right)=&\left|\sqrt{P^a}R\left(\varepsilon\left(t\right)-\frac{d}{2}\right)+\sqrt{P^s}R\left(\varepsilon\left(t\right)-\frac{d}{2}-\left(\Delta_c-\Delta_rt\right)\right)\right|^2\\&-\left|\sqrt{P^a}R\left(\varepsilon\left(t\right)+\frac{d}{2}\right)+\sqrt{P^s}R\left(\varepsilon\left(t\right)+\frac{d}{2}-\left(\Delta_c-\Delta_rt\right)\right)\right|^2,\end{aligned} \tag{12}$$

where the noise $\tilde{n}$ has been omitted.

Next, substituting Equations (5) and (6) into (12),

$$\begin{aligned}S_c\left(\varepsilon\left(t\right),d\right)=&\left|\sqrt{P^a}\left(1-\left|\varepsilon\left(t\right)-\frac{d}{2}\right|\right)+\sqrt{P^s}\left(1-\left|\varepsilon\left(t\right)-\frac{d}{2}-\left(\Delta_c-\Delta_rt\right)\right|\right)\right|^2\\&-\left|\sqrt{P^a}\left(1-\left|\varepsilon\left(t\right)+\frac{d}{2}\right|\right)+\sqrt{P^s}\left(1-\left|\varepsilon\left(t\right)+\frac{d}{2}-\left(\Delta_c-\Delta_rt\right)\right|\right)\right|^2.\end{aligned} \tag{13}$$

Combined with Equations (11) and (13), SCB can be obtained by solving the following equation:

$$\begin{aligned}&\left|\sqrt{P^a}\left(1-\left|\varepsilon\left(t\right)-\frac{d}{2}\right|\right)+\sqrt{P^s}\left(1-\left|\varepsilon\left(t\right)-\frac{d}{2}-\left(\Delta_c-\Delta_rt\right)\right|\right)\right|^2\\&=\left|\sqrt{P^a}\left(1-\left|\varepsilon\left(t\right)+\frac{d}{2}\right|\right)+\sqrt{P^s}\left(1-\left|\varepsilon\left(t\right)+\frac{d}{2}-\left(\Delta_c-\Delta_rt\right)\right|\right)\right|^2.\end{aligned} \tag{14}$$

For convenience, we denote $A=\sqrt{P^a}$, $B=\sqrt{P^s}$, $d=1$. In addition, it is noted that Δ_c is the code phase difference in chips between authentic signal and spoofing at the beginning of the attack. As an example, letting $\Delta_c=-2$ will be consistent with the experiments in reference [39].

Then, since $R\left(\tau'\right)$ is a piecewise function, the solution of Equation (14) needs a piecewise analysis. Therefore, the theoretical formula of SCB can be obtained as:

$$\varepsilon\left(t\right)=\begin{cases}0, & 0<\Delta_rt\le 0.5\\ \frac{B\left(\Delta_rt-0.5\right)}{2A-B-1}, & 0.5<\Delta_rt\le\frac{A}{2B}\\ \frac{4B\left(2-\Delta_rt\right)-3A}{2\left(B-A\right)}, & \frac{A}{2B}<\Delta_rt\le 1.5-\frac{A}{4B}\\ \frac{2B\left(2-\Delta_rt\right)}{A+B}, & 1.5-\frac{A}{4B}<\Delta_rt\le 2.5+\frac{A}{4B}\\ \frac{8B\left(2-\Delta_rt\right)+3A}{2\left(4B-A\right)}, & 2.5+\frac{A}{4B}<\Delta_rt\le 3.5\\ 2-\Delta_rt, & \Delta_rt>3.5.\end{cases} \tag{15}$$

On the other hand, when there is no induced spoofing, the theoretical formula of SCB can be obtained by solving the following equation:

$$|A\,(1-|\varepsilon\,(t)-0.5|)| = |A\,(1-|\varepsilon\,(t)+0.5|)|\,. \tag{16}$$

Resulting in the SCB being:

$$\varepsilon\,(t) = 0. \tag{17}$$

In order to gain an understanding about the theoretical SCB, Figure 2 shows the theoretical SCB with and without induced spoofing. As Equation (17) stated, SCB is always 0 when there is no spoofing. However, when there is an induced spoofing signal, SCB is changing over time which results in the gradual adjustment process. Specially, in Figure 2, SCB is reduced from 110 s to about 140 s. After that, SCB was increased from about 140 s. More importantly, the slope was almost unchanged from 110 s to about 140 s and from about 140 s to about 200 s. Thus there was slope mutation at about 140 s. Based on the above observation, the first-order derivative or the second-order derivative of SCB could be used to detect induced spoofing.

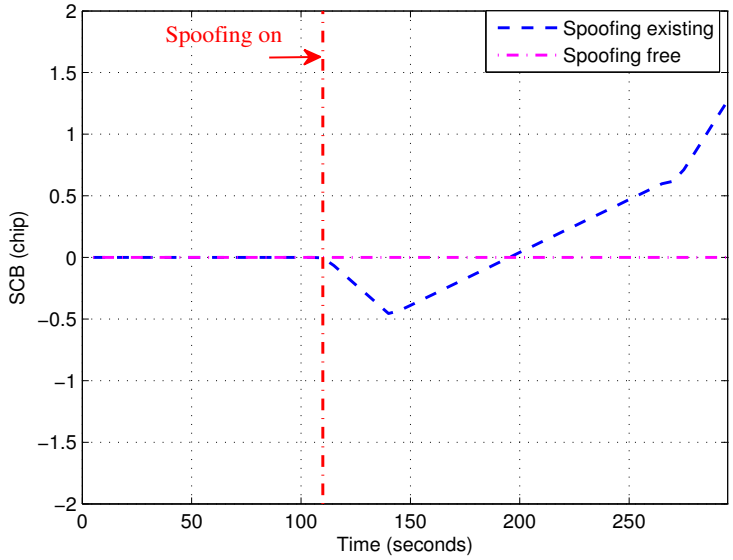

Figure 2. Theoretical S-curve-bias (SCB) curve with and without induced spoofing.

In this paper, a detection metric based on the derivative of SCB is proposed. In GNSS receivers, the first-order derivative of SCB can be computed using the finite differences method as:

$$\delta_t = \frac{\varepsilon\,(t+\Delta t)-\varepsilon\,(t)}{\Delta t}, \tag{18}$$

where $\varepsilon\,(t)$ is the SCB value at time t, Δt is the time difference between two adjacent timings. For a given threshold γ, if $|\delta_t| > \gamma$, it means that the first-order derivative exceeds the given threshold. Then the proposed algorithm declared an induced spoofing. Therefore, the proposed algorithm detected induced spoofing by utilizing the dynamic nature of gradual adjustment process. In experiments, SCB was calculated based on the method in reference [37]. In the code tracking loop of the software receiver, we can get the correlation values of the early code and the late code. After that, the S-type correlation curve can be obtained. Then SCB can be calculated based on the definition. More details can be found in the reference [37].

It is well known that there will be changes in the SCB when there is multipath. However, it is very unlikely that the changing process of multipath SCB is generally similar to that of induced spoofing

due to the inherent randomness of multipath [40,41]. From this point of view, the proposed algorithm is not sensitive to multipath signals.

3.2. Probability Analysis

The detection of induced spoofing can be regarded as a binary detection problem, that is, to determine whether spoofing exists or not. Two hypotheses are defined as $\mathcal{H}_0$ if an induced spoofing does not exist and $\mathcal{H}_1$ if an induced spoofing does exist. Thus, given that (17) is the decision test, the hypothesis test can be expressed as:

$$\begin{cases} \mathcal{H}_0: & |\delta_t| \leq \gamma, \quad \text{without spoofing} \\ \mathcal{H}_1: & |\delta_t| > \gamma, \quad \text{with spoofing.} \end{cases} \tag{19}$$

The probability of false alarm P_{fa} is the probability that the hypothesis of the presence of an induced spoofing attack is accepted, but in fact, it is not present. The detection probability P_d is the probability that the hypothesis of the presence of a spoofing attack is accepted, and it is present. For the calculation of P_{fa} and P_d, we should obtain the distribution of SCB under the spoofing-present situation. However, according to the analysis above, for the induced spoofing, the inducing process has time-varying characteristics. In addition, the distribution of SCB depends on the tracking loop configuration of the victim receiver and the specific form of spoofing, i.e., changing speeds of code phase and power. But it is unknown to the receiver how code phase and power (carrier-to-noise ratio, $\frac{C}{N_0}$) of the spoofing will vary. Thus it is difficult for the victim receiver to predict the behavior of induced spoofing. It is also difficult to determine the specific distribution of SCB [37] when there is an induced spoofing. Under this circumstance, it is difficult to derive the analytical expression of the probability density function to compute P_{fa} and P_d.

If the pattern of induced spoofing is given, P_{fa} is also a function of the threshold value γ. Thus the probability of false alarm P_{fa} can be calculated as the following:

$$P_{fa} = \int_{\gamma}^{+\infty} p\left(\mathcal{T}; H_0\right) d\mathcal{T}, \tag{20}$$

where $\mathcal{T} = |\delta_t|$, $p\left(\mathcal{T}; H_0\right)$ denotes the probability density function of $\mathcal{T}$ when there is no induced spoofing.

Similarly, the detection probability P_d can be calculated as the following:

$$P_d = \int_{\gamma}^{+\infty} p\left(\mathcal{T}; H_1\right) d\mathcal{T}, \tag{21}$$

where $p\left(\mathcal{T}; H_1\right)$ is the probability density function of $\mathcal{T}$ when there is an induced spoofing.

In experiments, as that in [3,34], the probability of false alarm P_{fa} will be obtained when there is no induced spoofing as the following:

$$P_{fa} = \frac{\#\left\{\mathcal{T} > \gamma\right\}}{M}, \tag{22}$$

where $\#\{\cdot\}$ is the total number of satisfied argument conditions. P_{fa} is explained as a relative frequency, that is a ratio between the number of times the test statistic exceeds the given threshold out of the total number of experiment realizations M.

When there is an induced spoofing, the detection probability P_d will be obtained as the following:

$$P_d = \frac{\#\left\{\mathcal{T} > \gamma\right\}}{M} \tag{23}$$

P_d is similarly explained as a relative frequency, that is a ratio between the number of times the test statistic exceeds the given threshold out of the total number of experiment realizations M.

For a given P_{fa}, the threshold is first calculated based on Equaiton (22). In addition, a similar hypothesis testing can be performed for the ratio method. In this paper, we calculated the detection probability every 10 s where the number 10 is selected as an experience value. That is to say, spoofing detection was performed within each small detection window. The performance of the proposed algorithm will be evaluated and compared with the ratio method.

4. Experiments

In this section, experiments are carried out to evaluate the performance of the proposed method. Based on the theoretical analysis of the previous section, the proposed induced spoofing detection method will be embedded into a conventional software GPS receiver which is developed in Civil Aviation University of China. The TEXBAT data sets [39] are used in all experiments.

4.1. Introduction of TEXBAT Data Sets

The radionavigation laboratory in the University of Texas at Austin produced the first public database (ds1–ds6) of signals affected by several types of spoofing attacks concerning GPS satellites in 2012. Two additional data sets, ds7 and ds8 were added to TEXBAT in August 2015. Therefore, there were eight different GPS L1 C/A spoofing data sets in TEXBAT [39,42], namely ds1–ds8, which represent different spoofing attack scenarios. They were based on two "clean data sets" replayed through the vector signal generator, and 25 Msps sampling rate data grabber attached in one case to a static antenna building on the campus of the University of Texas and in the other case to an antenna mounted on a vehicle, which travelled across the city [39].

In this paper, ds7 was chosen to evaluate the performance of the proposed method. In this scenario, it represented the so-called seamless takeover attack. There were no offsets in samples and time, and spoofing was already perfectly aligned since it was digitally added to the clean data sets. No obvious disruption can be observed in the tracking loop. The ds8 represents a zero-delay security code estimation and replay (SCER) attack, which was identical to the ds7, except for the spoofer guesses, and generated the navigation data bits in real time [42]. Since the proposed method did not employ security codes to detect spoofing attacks, its anti-spoofing performance in ds7 and ds8 will be the same. Therefore, ds8 was not be considered in the paper.

For ds7, spoofing is free from 0 to 110 s, data is identical to "clean static date sets" during this time. The spoofing signals are injected for each GPS L1 C/A signals at the 110-th second and the amplitude of spoofing varied nonlinearly. After that, the code phases of the spoofing relative to the counterpart authentic ones increased at a rate of 1.2 m per second, that is, 409.2×10^{-5} Hz. Finally, a 1.27 μs clock offset is induced in the victim receiver which is described in the reference [42].

4.2. Ratio Test Detection Method

As a comparison, the intermediate spoofing detection algorithm based on the ratio test metric (called the ratio method) [33] is also used in this paper. As in [33], the detection metric of the ratio method is defined by the following formula:

$$R_d = \frac{E_i^{\frac{d}{2}} + L_i^{\frac{d}{2}}}{\beta P_i} \tag{24}$$

where $E_i^{\frac{d}{2}}$, $L_i^{\frac{d}{2}}$ and P_i represent the early, late and prompt correlator output over the in-phase branch, the superscript $\frac{d}{2}$ denotes the correlator spacing between the early/late correlator and prompt correlator, β is the correlation main peak slope. For more details, refer to [33]. According to the theory presented

in [33], the threshold, e.g., γ', can be derived with a given false detection probability. Therefore, if $|R_d| > \gamma'$, it is decided that the receiver has been attacked by a spoofing.

It is worth pointing out that the ratio method detects spoofing by finding the distortion of correlator output at a given timing. In other words, it detects spoofing based on the static distortions of the correlator output. In contrast, the proposed algorithm declares an induced spoofing attack by detecting the dynamic changes of the SCB.

4.3. Results of the Proposed Method

Figure 3 shows the comparisons between the experimental and theoretical SCBs. The time length was 294 s and the induced spoofing attack occurred at 110 s (vertical point-line). Each satellite actually had a theoretical SCB curve, but these theoretical curves coincided with each other and only one theoretical SCB curve is shown in Figure 3. For the experimental SCBs, five curves according to five tracked satellites are shown. From 0 to 110 s, there were almost no fluctuations, except for PRN23 which caused the other curves to be masked by the curve of PRN23. For PRN23, the fluctuation may have been due to poor signal quality or high noise conditions. It is noted that the experimental SCB curves take the fluctuations on both sides of the theoretical value. The main reason is that the theoretical SCB was derived by ommiting the noise $\tilde{n}$ in Equation (8). However, in fact, noise was unavoidable, which lead to fluctuations. On the other hand, the overall trend was consistent with the theoretical curve. In order to reduce the impact of fluctuations, the curves were filtered with a Butterworth digital filter. The coefficient vectors of the filter system function's molecular polynomial and denominator polynomial are $\mathbf{b} = [9.9419 \times 10^{-4}, 2.0 \times 10^{-4}, 9.9419 \times 10^{-4}]$ and $\mathbf{a} = [1, -1.908, 0.9218]$.

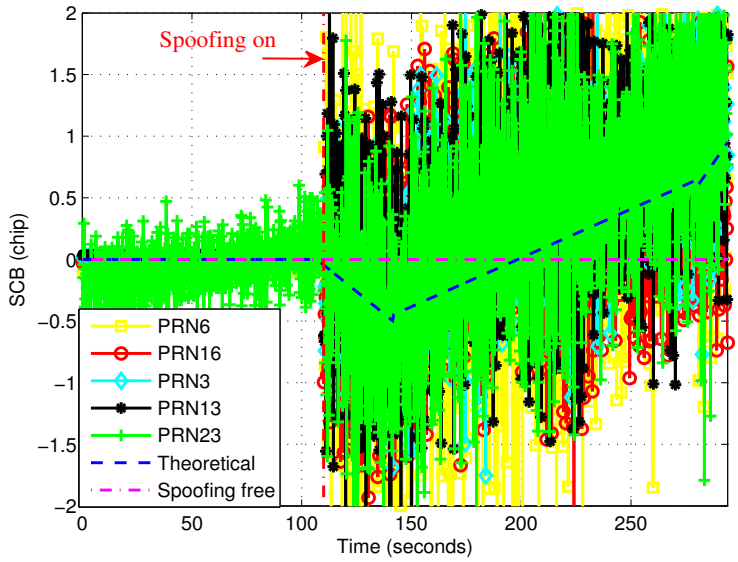

Figure 3. Comparisons between experimental SCB curve and theoretical SCB curve.

Figure 4 shows the filtered experimental SCB curves. It is more clear to show that the experimental curves were almost consistent with the theoretical curve. It is noted that experimental SCB values had a very small fluctuation around 0 when there was no spoofing in the first 110 s. From 110 s, the curve gradually deviated from zero. It indicates that there was an induced spoofing and it's code phase lagged behind that of the authentic satellite signal. When the maximum negative value was reached, the value of SCB slowly increased to zero. At this time the spoofing was already very close (about within 0.5 chips) to the authentic signal. After arriving at zero point, the receiver tracking loop was controlled by induced spoofing. The tracking loop of the victim receiver locked on the induced spoofing and was slowly pulled out of the authentic signal. Then the value of SCB increases gradually.

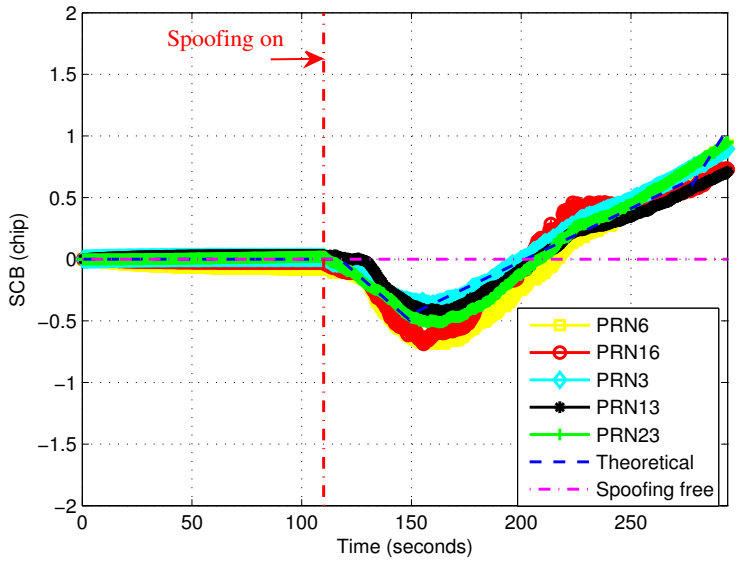

Figure 4. Comparisons between filtered experimental and theoretical SCB curves.

In order to obtain more details, as an example, the SCB curve of PRN23 is shown in Figure 5. The experimental SCB curve had a good fit with the theoretical curve. As stated before, when the spoofing began to induce the victim receiver, the SCB curve changed gradually.

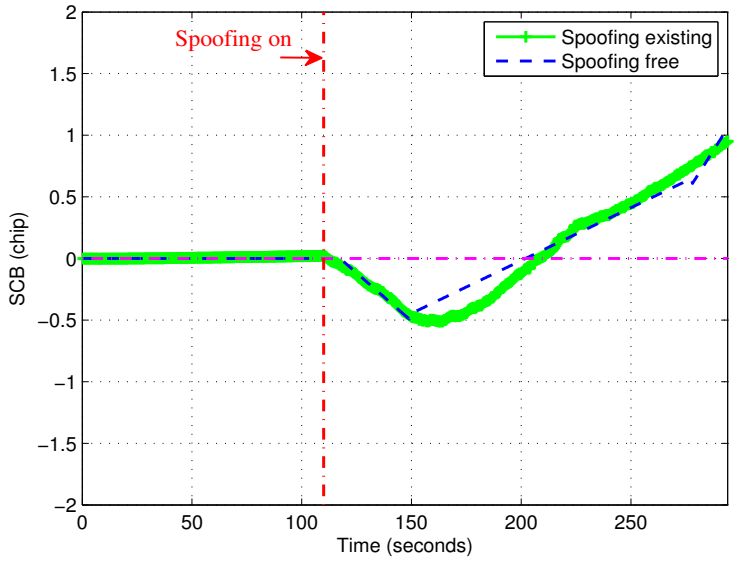

Figure 5. Experimental and the theoretical SCB curves for PRN 23.

For PRN23, the first derivative of SCB is shown in Figure 6. It is clear that the theoretical value with spoofing was significantly greater than that without spoofing. When there was spoofing, the experimental values fluctuated around the theoretical ones. The experimental values were close to zero before 110 s where there was no spoofing. More importantly, it was far less than the value with spoofing. Therefore, it was easy to find a reasonable detection threshold γ.

Table 1 summarizes the detection threshold γ corresponding to the false alarm probability P_{fa} for the proposed algorithm. It is reminded that the thresholds are selected based on Equation (22).

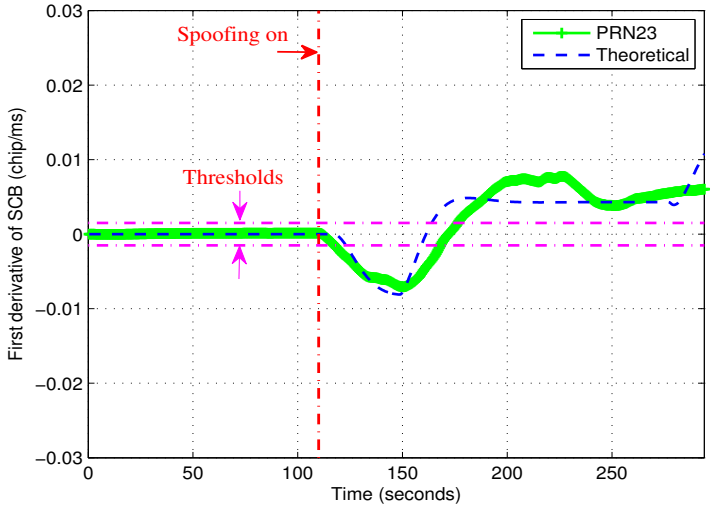

Figure 6. The first derivatives of experimental and the theoretical SCB curves for PRN 23.

Table 1. The relationship between false alarm probability and detection threshold for the proposed algorithm.

	False Alarm Probability (%)	Detection Threshold
1	10	1.421×10^{-4}
2	1	1.476×10^{-4}
3	0.1	1.480×10^{-4}
4	0.01	1.485×10^{-4}
5	0	1.495×10^{-4}

4.4. Results of Ratio Method

For the ratio method, Figure 7 shows the curve during an induced spoofing attack. The time length was also 294 s. The induced spoofing was also added at the 110-th s. We can see that the changing of different satellites were almost the same. Before 200 s, the changing amplitude of the ratio method was not obvious. Thus it was difficult to detect an induced spoofing attack before 200 s. After that, the ratio method was slowly changing.

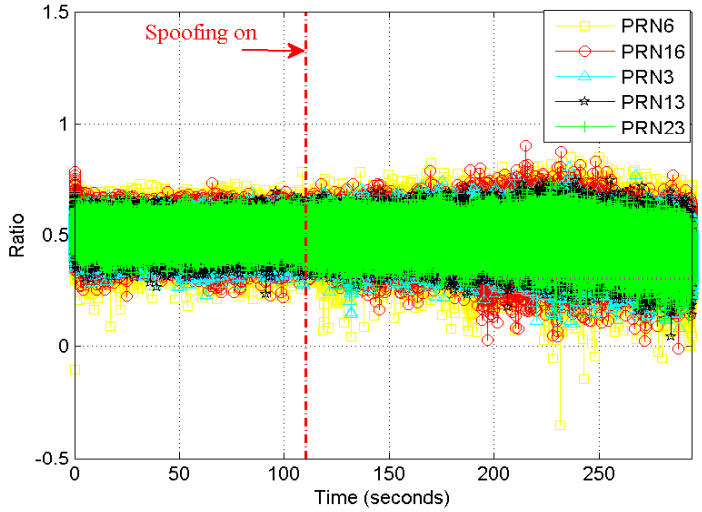

Figure 7. Ratio method curves during an induced spoofing attack.

Figure 8 shows the ratio method curve of PRN 23. In Figure 8, the sold curve is the ratio test metric for PRN23. The different dashed curves are detection thresholds γ' according to different false alarm probabilities. The thresholds were increased with increasing of the false alarm probability. The values of detection threshold corresponding to different false alarm probability are summarized in Table 2.

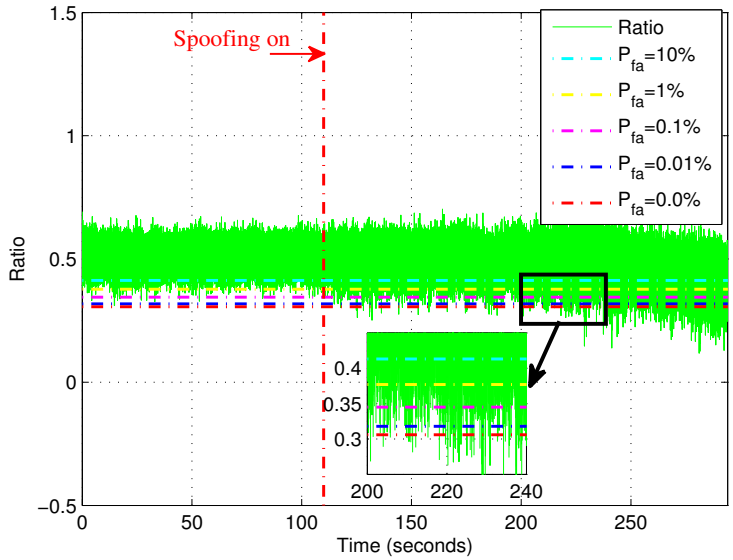

Figure 8. The ratio method curve for PRN 23. The solid curve is the ratio method metric. The dashed curves are detection thresholds according to different false alarm probabilities.

Table 2. The relationship between false alarm probability and detection threshold for the ratio method.

	False Alarm Probability (%)	Detection Threshold
1	10	0.455
2	1	0.413
3	0.1	0.379
4	0.01	0.342
5	0	0.315

4.5. Comparison of Two Methods

When the false alarm probability is set as 0.1, the thresholds of two algorithms are selected as those in Tables 1 and 2. It is reminded that the detection probability is calculated every 10 s. Figure 9 shows detection probabilities with time for the proposed method and the ratio method, respectively. The red solid and blue dashed curves are separately corresponding to the proposed algorithm and the ratio method. It is noted that the solid and dashed curves are separately corresponding to the proposed algorithm and the ratio method. At about the 110-th s, the proposed method can detect spoofing and the detection probability is almost unity. However, until about the 294-th s, the ratio method reaches the maximal detection probability which is about 0.7. But it is still slightly lower than the proposed method. Therefore, compared with the ratio method, the proposed algorithm can detect induced spoofing at a much earlier stage, which is because the proposed method utilizes the dynamic feature of induced spoofing.

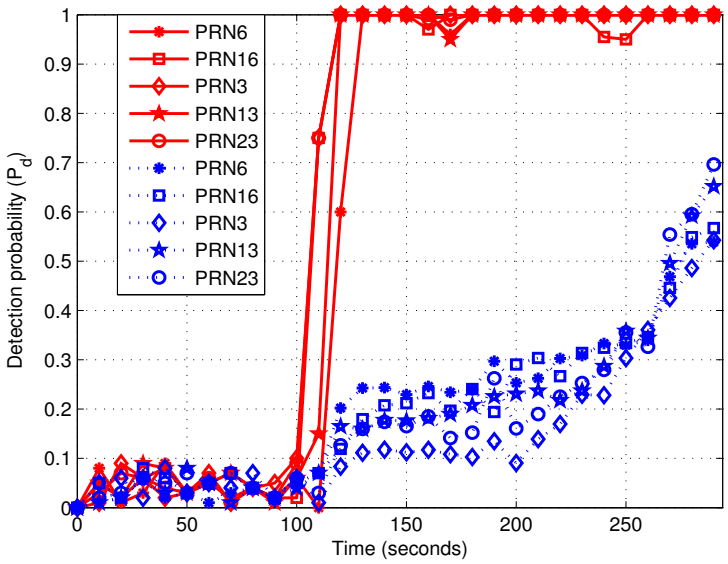

Figure 9. The relationship between detection probability and time length. The red solid and blue dashed curves are separately corresponding to the proposed algorithm and the ratio method. The false alarm probability was set to 0.1.

In order to obtain more details, the detection probabilities of the two algorithms are compared for different lengths of the received signal. When the length of the data are separately 200 s and 294 s, Figures 10 and 11 show the relationship between detection probability and false alarm probability.

Figure 10 shows the detection probabilities for the first 200 s data. As expected, P_d tends to 1 for increasing P_{fa} values. However, the curves corresponding to the proposed algorithm attain $P_d \to 1$ faster than the ratio method. Therefore, when the data length is 200 s, the proposed algorithm outperforms the ratio method.

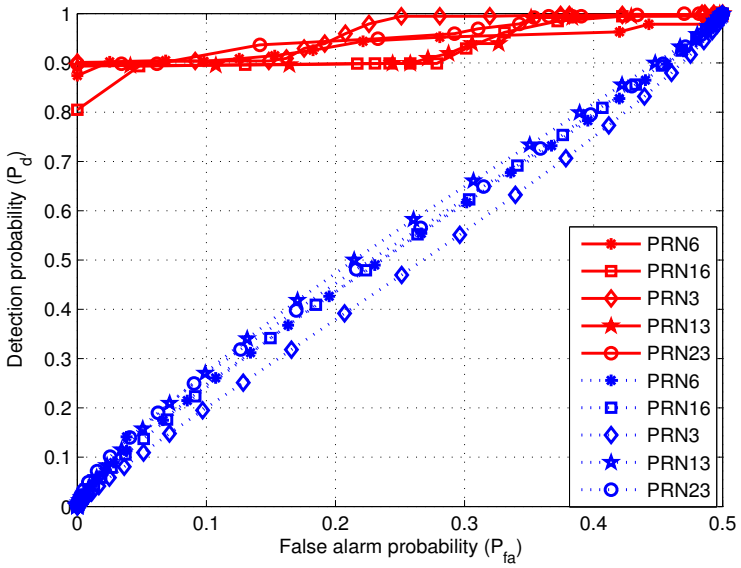

Figure 10. The relationship between detection probability and false alarm probability for the first 200 s data. The red solid and blue dashed curves are separately corresponding to the proposed algorithm and the ratio method.

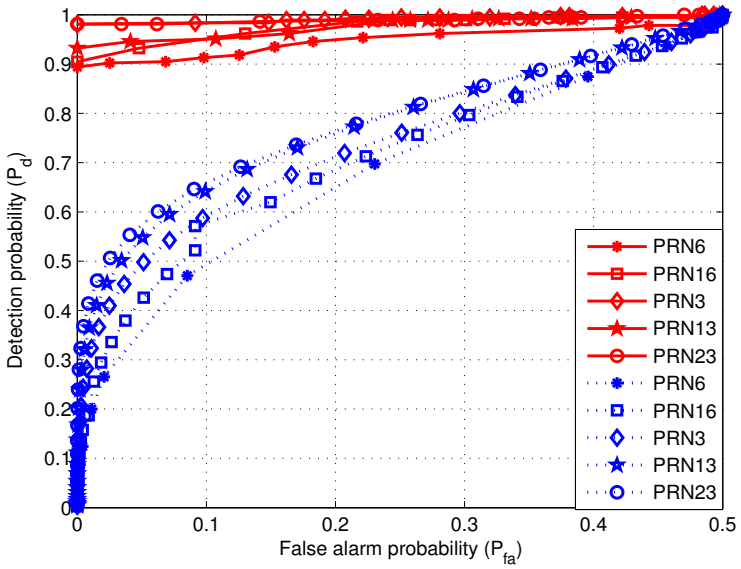

Figure 11. The relationship between detection probability and false alarm probability for the first 294 s data. The red solid and blue dashed curves are separately corresponding to the proposed algorithm and the ratio method.

When the data length is 294 s, the relationship between the detection probability and false alarm probability is shown in Figure 11. With much longer data length, the performance of the ratio method is significantly improved. It means that, for a given satisfied detection performance, the ratio method needs longer data. At the same time, the performance of the proposed algorithm is also improved. Moreover, the proposed algorithm performs still better than the ratio method.

5. Conclusions

In this paper, an induced spoofing detection algorithm is proposed. By gradually adjusting its parameters, the induced spoofing can capture victim tracking loops without creating loss of locks. However, it will lead to a significant change in the SCB. The proposed algorithm is based on the change of SCB to detect induced spoofing. In other words, the proposed algorithm utilized the dynamic feature of gradual adjustment process. More specifically, a detection metric based on the first derivative of SCB is defined in this paper. When the detection metric exceeds a given threshold, an induced spoofing will be declared. A series of experiments with the Texas Spoofing Test Battery (TEXBAT) are performed to verify the effectiveness of the proposed algorithm. The experimental results demonstrate that the proposed algorithm can detect induced spoofing in a earlier stage.

Future work includes deducing the theoretical threshold value for a given P_{fa} or P_d. On the other hand, it is noted that the proposed algorithm detects induced spoofing based on the dynamic nature of gradual adjustment process. Then there is overlapping between the two correlation peaks corresponding to authentic signal and spoofing, respectively. When the induction process is finished, the correlation peak of spoofing will not be overlapped with that of authentic signal and the proposed algorithm may fail. Then the proposed algorithm could be combined with other techniques such as power level monitoring to detect spoofing. Therefore, another possible future direction could be combining the proposed algorithm with other detection methods.

Author Contributions: W.W. and R.W. raised the idea and drafted the paper; N.L. performed the experiments and analyzed the results; P.C. analyzed results and revised the paper. All authors reviewed the paper.

Funding: This work was supported by the National Natural Science Foundation of China (U1833112) and by the National Science Foundation (Awards 1815349 and 1845833).

Acknowledgments: Comments from the anonymous referees and the editor are also gratefully appreciated.

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

References

1. European GNSS Agency. *GNSS Market Report*; Technical Report; GSA: Prague, Czech Republic, 2017.
2. Amin, M.G.; Closas, P.; Broumandan, A.; Volakis, J.L. Vulnerabilities, threats, and authentication in satellite-based navigation systems [scanning the issue]. *Proc. IEEE* **2016**, *104*, 1169–1173. [CrossRef]
3. Ali, K.; Manfredini, E.G.; Dovis, F. Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics. In Proceedings of the IEEE/ION PLANS, Monterey, CA, USA, 5–8 May 2014; pp. 1240–1247.
4. Bhatti, J.; Humphreys, T.E. Hostile control of ships via false GPS signals: Demonstration and detection. *Navigation* **2017**, *64*, 51–66. [CrossRef]
5. Shepard, D.P.; Humphreys, T.E.; Fansler, A.A. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In Proceedings of the ION GNSS Meeting, Nashville, TN, USA, 19–22 September 2012; pp. 19–21.
6. Psiaki, M.L.; Humphreys, T.E.; Stauffer, B. Attackers can spoof navigation signals without our knowledge. Heres how to fight back GPS lies. *IEEE Spectr.* **2016**, *53*, 26–53. [CrossRef]
7. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In Proceedings of the ION GNSS Meeting, Savannah, GA, USA, 16–19 September 2008; pp. 16–19.
8. Humphreys, T.E.; Shepard, D.P.; Bhatti, J.A.; Wesson, K.D. A testbed for developing and evaluating GNSS signal authentication techniques. In Proceedings of the CERGAL, Dresden, Germany, 8–9 July 2014.
9. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *Int. J. Navig. Obs.* **2012**, *2012*, 1–16. [CrossRef]
10. Montgomery, P.Y.; Humphreys, T.E.; Ledvina, B.M. A multiantenna defense: Receiver-autonomous GPS spoofing detection. *Inside GNSS* **2009**, *4*, 40–46.
11. McDowell, C.E. GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling. U.S. Patent 7,250,903 B1, 31 July 2007.
12. Wang, J.; Zhou, M.; Li, H.; Cui, X.; Lu, M. On the requirements of GNSS intermediate spoofing. In *Proceedings of China Satellite Navigation Conference (CSNC)*; Lecture Notes in Electrical Engineering; Springer: Berlin/Heidelberg, Germany, 2014; Volume 303, pp. 543–552.
13. Ioannides, R.; Pany, T.; Gibbons, G. Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. *Proc. IEEE* **2016**, *104*, 1174–1194. [CrossRef]
14. Psiaki, M.L.; Humphreys, T.E. GNSS spoofing and detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
15. Montgomery, P.Y.; Humphreys, T.E.; Ledvina, B.M. Receiver autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In Proceedings of the ION GNSS Meeting, Anaheim, CA, USA, 26–28 January 2009; pp. 124–130.
16. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N_0 observables. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 181–191. [CrossRef]
17. Borio, D.; Gioia, C. A sum-of-squares approach to GNSS spoofing detection. *IEEE Trans. Aerosp. Electr. Syst.* **2016**, *52*, 1756–1768. [CrossRef]
18. Moshavi, S. Multi-user detection for DS-CDMA communications. *IEEE Commun. Mag.* **1996**, *34*, 124–136. [CrossRef]
19. Dehghanian, V.; Nielsen, J.; Lachapelle, G. GNSS spoofing detection based on receiver C/N_0 estimates. In Proceedings of the ION GNSS Meeting, Nashville, TN, USA, 17–21 September 2012; pp. 2878–2884.
20. Gamba, M.T.; Truong, M.D.; Motella, B.; Falletti, E.; Ta, T.H. Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets. *GPS Solut.* **2017**, *21*, 577–589. [CrossRef]
21. Jafarnia-Jahromi, A.; Lin, T.; Broumandan, A.; Nielsen, J.; Lachapelle, G. Detection and mitigation of spoofing attack on a vector based tracking GPS receiver. In Proceedings of the ION GNSS Meeting, Portland, OR, USA, 19–23 September 2011; pp. 790–800.
22. Yuan, D.; Li, H.; Wang, F.; Lu, M. A GNSS acquisition method with the capability of spoofing detection and mitigation. *Chin. J. Electron.* **2018**, *27*, 213–222. [CrossRef]

23. Lo, S.C.; Enge, P.K. Authenticating aviation augmentation system broadcasts. In Proceedings of the IEEE/ION PLANS, Indian Wells, CA, USA, 4–6 May 2010; pp. 708–717.
24. Fantino, M.; Molino, A.; Mulassano, P.; Nicola, M.; Rao, M. Signal quality monitoring: correlation mask based on ratio test metrics for multipath detection. In Proceedings of the IGNSS, Surfers Paradise, QLD, Australia, 1–3 December 2009.
25. Wesson, K.D.; Rothlisberger, M.; Humphreys, T.E. Practical cryptographic civil GPS signal authentication. *Navigation* **2012**, *59*, 177–193. [CrossRef]
26. Broumandan, A.; Jafarnia-Jahromi, A.; Lachapelle, G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solut.* **2014**, *19*, 1–13. [CrossRef]
27. Closas, P.; Arribas, J.; Fernández-Prades, C. Spoofing detection by a reduced acquisition process. In Proceedings of Precise Time and Time Interval Systems and Applications Meeting (ION PTTI 2016), Monterey, CA, USA, 25–28 January 2016.
28. Wang, F.; Li, H.; Lu, M. GNSS spoofing detection and mitigation based on maximum likelihood estimation. *Sensors* **2017**, *17*, 1532. [CrossRef] [PubMed]
29. Pini, M.; Fantino, M.; Cavaleri, A.; Ugazio, S.; Lo Presti, L. Signal quality monitoring applied to spoofing detection. In Proceedings of the ION GNSS Meeting, Portland, OR, USA, 20–23 September 2001; pp. 1888–1896.
30. Phelts, P.; Akos, D.; Enge, P. Robust signal quality monitoring and detection of evil waverforms. In Proceedings of the ION GNSS+ Meeting, Salt Lake City, UT, USA, 19–22 September 2000; pp. 1180–1190.
31. Mitelman, A.M. Signal Quality Monitoring for GPS Augmentation System. Ph.D. Thesis, Stanford University, Stanford, CA, USA, January 2005.
32. Phelts, R.E. Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality. Ph.D. Thesis, Stanford University, Stanford, CA, USA, October 2001.
33. Cavaleri, A.; Motella, B.; Pini, M.; Fantino, M. Detection of spoofed GPS signals at code and carrier tracking level. In Proceedings of the NAVITEC'10, ESA/ESTEC, Noordwijk, The Netherlands, 8–10 December 2010; pp. 2875–2884.
34. Manfredini, E.G.; Dovis, F.; Motella, B. Validation of a signal quality monitoring technique over a set of spoofed scenarios. In Proceedings of the NAVITEC'14, ESA/ESTEC, Noordwijk, The Netherlands, 3–5 December 2014; pp. 1–7.
35. Jafarnia-Jahromi, A.; Broumandan, A.; Daneshmand, S.; Lachapelle, G.; Ioannides, R.T. Galileo signal authenticity verification using signal quality monitoring methods. In Proceedings of ICL-GNSS, Barcelona, Spain, 28–30 June 2016; pp. 1–8.
36. Yang, Y.; Li, H.; Lu, M. Performance assessment of signal quality monitoring based GNSS spoofing detection techniques. In Proceedings of the CSNC 2015, Xi'an, China, 13–15 May 2015; pp 783–793.
37. Soellner, M.; Kurzhals, C.; Hechenblaikner, G.; Rapisarda, M.; Burger, T.; Erker, S.; Furthner, J.; Grunert, U.; Meurer, M.; Tholert, S. GNSS offline signal quality assessment. In Proceedings of the ION GNSS+ Meeting, Fairfax, VA, USA, 16–19 September 2007; pp. 164–182.
38. Humphreys, T.E.; Bhatti, J.A.; Shepard, D.P.; Wesson, K.D. The Texas spoofing test battery: Toward a standard for evaluating GNSS signal authentication techniques. In Proceedings of the ION GNSS+ Meeting, Nashville, TN, USA, 17–21 September 2012; pp. 3569–3583.
39. Laboratory, T.R. Texas Spoofing Test Battery (TEXBAT). Available online: http://radionavlab.ae.utexas.edu/texbat (accessed on 22 February 2019).
40. Closas, P.; Fernández-Prades, C. A statistical multipath detector for antenna array based GNSS receivers. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 916–929. [CrossRef]
41. Jia, Q.; Wu, R.; Wang, W.; Lu, D.; Wang, L.; Li, J. Multipath interference mitigation in GNSS via WRELAX. *GPS Solut.* **2017**, *21*, 487–498. [CrossRef]
42. Humphreys, T.E. Texbat Data Sets 7 and 8. 2015. Available online: http://radionavlab.ae.utexas.edu/datastore/texbat/texbat_ds7_and_ds8.pdf (accessed on 22 February 2019).