sensors

MDPI

Article

Spoofing Detection and Mitigation in a Multi-correlator GPS Receiver Based on the Maximum Likelihood Principle

Yanbing Guo, Lingjuan Miao and Xi Zhang *

School of Automation, Beijing Institute of Technology (BIT), Beijing 100081, China; 20080089@bit.edu.cn (Y.G.); miaolingjuan@bit.edu.cn (L.M.)

* Correspondence: 3120120355@bit.edu.cn; Tel.: +86-134-8868-7572

Received: 27 October 2018; Accepted: 19 December 2018; Published: 22 December 2018

Abstract: As a structural interference, spoofing is difficult to detect by the target receiver while the advent of a repeater makes the implementation of spoofing much easier. Most existing anti-spoofing methods are merely capable of detecting the spoofing, i.e., they cannot effectively remove counterfeit signals. Therefore, based on the similarities between multipath and spoofing, the feasibility of applying multipath mitigation methods to anti-spoofing is first analyzed in this paper. We then propose a novel algorithm based on maximum likelihood (ML) estimation to resolve this problem. The tracking channels with multi-correlators are constructed and a set of corresponding steps of detecting and removing the counterfeit signals is designed to ensure that the receiver locks the authentic signals in the presence of spoofing. Finally, the spoofing is successfully executed with a software receiver and the saved intermediate frequency (IF) signals, on this basis, the effectiveness of the proposed algorithm is verified by experiments.

Keywords: repeater; anti-spoofing; ML estimation; multi-correlators; detecting and removing the counterfeit signals

1. Introduction

GPS is susceptible to a variety of interferences due to the low signal power. For GPS receivers, there are two major types of interferences at present: jamming and spoofing. Strong interferences are used in jamming, usually resulting in loss of lock and positioning failure of the target receiver. Hence the concealment of this interference is poor. On the other hand, spoofing is a structural interference, the counterfeit signals rebroadcasted by spoofers are very similar to the authentic signals from satellites and can gradually induce the positioning results of the target receiver to a false location [1–4]. Compared with jamming, spoofing is less likely to be found by the target receiver and hence is more sinister.

The early spoofing is simplistic. Specifically, one simply attaches a power amplifier and a transmitting antenna to a satellite signal simulator and broadcasts the counterfeit signals toward the target receiver. However, the simplistic spoofing usually needs the cooperation of jamming to bring the target receiver into the reacquisition first. In 2008, Humphreys et al. successfully developed a repeater based on a software receiver, which can directly deceive the target receiver at the tracking stage. It reminds people of the threat of spoofing once again [1]. Correspondingly, research on anti-spoofing began to develop rapidly. In 2012, Jafarnia-Jahromi et al. made a comprehensive study of spoofing threats and briefly introduced different techniques for two main categories, namely spoofing detection and spoofing mitigation [5]. According to the description of related papers, common spoofing countermeasures can be categorized to four groups: signal power anomaly detection [2,3], time-of-arrival anomaly detection [6–8], space processing [9–12], and correlation peak distortion detection [13–17]. Daneshmand [12] proposed adaptive antenna array beamforming null steering method, which can directly shield the counterfeit signals from a single interference source. However, it is difficult in deploying multiple antennas. In view of the diversity of spoofing, Broumandan used multiple anti-spoofing methods simultaneously on the receiver and achieved the mitigation of simplistic spoofing [18]. However, on the whole, most of the current anti-spoofing techniques are merely able to detect the spoofing. This means that the target receiver can ensure that the positioning results are not affected by closing the corresponding channels after detecting the spoofing only when the number of the authentic signals spoofed with the counterfeit signals is small.

Based on the discussions above, the spoofing mitigation needs to be further researched in anti-spoofing. Multipath and spoofing share the similarity that they distort the correlation peaks of the composite signals. In particular, if the carrier frequency of the counterfeit signal deviates from that of its corresponding authentic signal, the distortion of the correlation peak of the composite signal will be serious. Instead, if the carrier frequency of the counterfeit signal is consistent with that of its corresponding authentic signal, the correlation peak of the composite signal of spoofing will be similar to that of multipath, which is the most difficult situation to detect and handle. Hence, the carrier frequencies of the counterfeit signal and its corresponding authentic signal are set to be the same (frequency lock mode) [19]. As a result, multipath mitigation approaches can be applied to anti-spoofing [20]. However, the counterfeit signals rebroadcasted by spoofers and the multipath signals are significantly different. The major differences are as follows [21]:

(1) Except for the special case that the direct signal is blocked, multipath signals from a satellite are typically weaker than its direct signal, while the counterfeit signals for spoofing are usually slightly higher in power than the authentic signals.

(2) The correlation peaks of multipath signals lag behind the correlation peak of the corresponding direct signal. The distance between these two kinds of peaks is commonly considered to be quite close. The effective overlapping of these two kinds of peaks indicates a quite close distance. By contrast, the counterfeit signals for spoofing can be aligned with the authentic signals, even ahead of the authentic signals. The distance between the correlation peaks of these two kinds of signals may be either far or close.

It means that not all multipath mitigation methods can be generalized to anti-spoofing. For example, the code phase discriminators of the multipath mitigation methods represented by early/late slope technique are specifically designed for the characteristics of multipath effects and cannot be applied to anti-spoofing. Multipath estimation is another type of important multipath mitigation methods. The composite signals are corrected to restore the direct signals on the basis of estimating the specific parameters of multipath signals. Such methods are usually based on least squares estimation, ML estimation, or Bayesian estimation and require fewer assumptions on multipath signals. Hence, such methods are promising in anti-spoofing.

The rest of this paper is organized as follows. Section 2 briefly introduces the characteristics of a repeater and the spoofing rebroadcasted by it. Section 3 starts from the concepts of ML estimation and constructs the tracking channels with multi-correlators. Section 4 designs a set of corresponding steps of detecting and removing the counterfeit signals. Section 5 simulates the spoofing and verifies the effectiveness of the proposed algorithm. Finally, the work in this paper is summarized in Section 6.

2. A Repeater and the Spoofing Rebroadcasted by It

In most cases, the counterfeit signals generated by a satellite signal simulator are not overlapped effectively with the authentic signals present in the space in which the receiver is located. If the counterfeit signal and the authentic signal correspond to the same satellite, and the code phase difference between them is less than $1 + d$ chips, then the overlapping of the two signals is considered to be effective in this paper, where d is the spacing between early and prompt correlators (or the spacing between prompt and late correlators) of the code loop. The autocorrelation and cross-correlation properties of C/A codes mean that the counterfeit signal is equivalent to the noise for the receiver channel which locks the authentic signal, i.e., it is difficult for the simplistic spoofing to affect the positioning results of the tracking receiver. By contrast, the spoofing executed by the repeater can affect the positioning results of the target receiver without reacquisition. As shown in Figure 1, the repeater consists of two modules, namely the receiver module and the spoofer module. The receiver module is the same with an ordinary GPS receiver. The spoofer module properly delays and amplifies the received authentic signals and rebroadcasts the resulting counterfeit signals toward the target receiver. In order to ensure that counterfeit signals are effectively overlapped with the authentic signals, the repeater needs to know the approximate location of the target receiver to determine the appropriate time delay. Since the size of the repeater is usually small, it can be inconspicuously deployed near the target receiver, which facilitates the execution of spoofing [1]. Since it is easy for the simplistic spoofing to be handled, the spoofing mentioned subsequently in this paper is always executed by the repeater and has the form shown in Figure 2. The correlation peaks of the counterfeit signal and the authentic signal have successively gone through three stages: approaching, effective overlapping, and moving away. The amplitude of the counterfeit signal is higher than that of the authentic signal throughout the process. In fact, as long as λ is greater than 1.1, the target receiver will gradually lose its lock on the authentic signal [16]. λ is the power ratio of the counterfeit signal to the authentic signal.

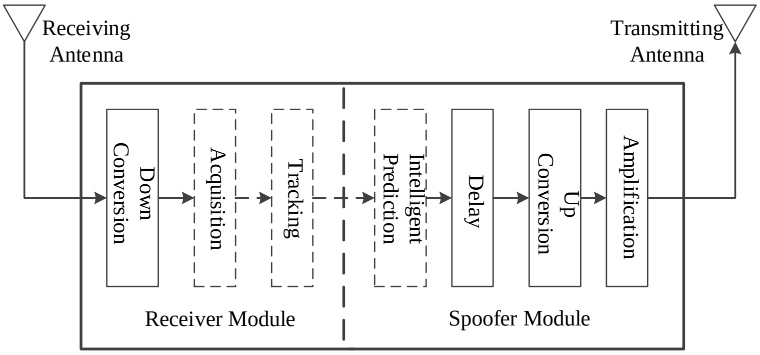


Figure 1. The structure of a repeater.

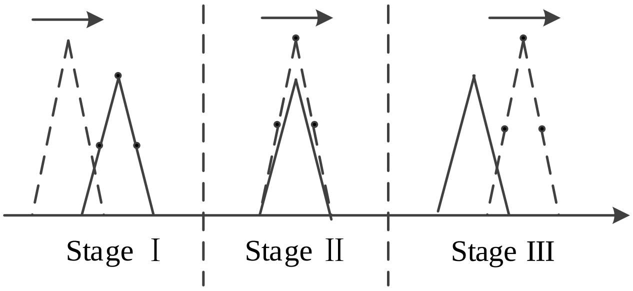


Figure 2. Spoofing rebroadcasted by a repeater.

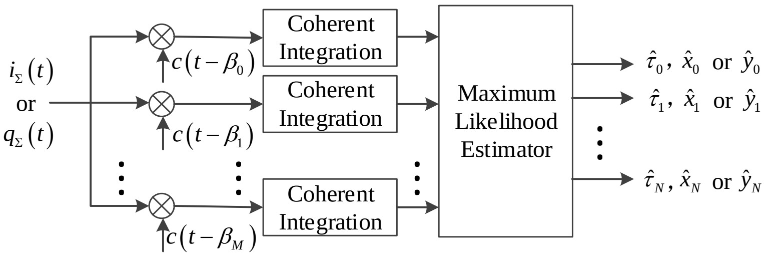
3. Construction of Multi-Correlators and Maximum Likelihood Rstimation of Dignal Parameters

In order to achieve the mitigation of spoofing, we employ the idea of multipath estimation. Firstly, in the presence of spoofing, the composite signals for the in-phase (I) and quadrature (Q) branches of any channel of the target receiver can be modeled as

$$i_\Sigma(t) = \sum_{n=0}^{N} a_n(t) A_0 D[t - \tau_n(t)] c[t - \tau_n(t)] \cos[\phi_n(t)] + v_\mathrm{i}(t), \tag{1}$$

$$q_\Sigma(t) = \sum_{n=0}^{N} a_n(t) A_0 D[t - \tau_n(t)] c[t - \tau_n(t)] \sin[\phi_n(t)] + v_\mathrm{q}(t), \tag{2}$$

respectively, where A_0 is the known amplitude of the authentic signal, $D(\cdot)$ is the navigation data bit, $c(\cdot)$ is the CA code, N is the number of counterfeit signals in the current channel, $n = 0, 1, 2, \cdots, N$, $v_{\mathrm{i}}(t)$ and $v_{\mathrm{q}}(t)$ denote the noises in the I and Q branches, respectively. $a_n(t)$, $\tau_n(t)$, $\phi_n(t)$ are the amplification coefficient of the amplitude, code delay (time delay) and carrier phase corresponding to the n-th signal, respectively. If $n = 0$, they correspond to the authentic signal and $a_0(t) = 1$, $\tau_0(t) = 0$, $\phi_0(t) = 0$. Otherwise, they correspond to the counterfeit signals and $a_n(t) \geq \sqrt{1.1}$. In reality, the repeater delays and amplifies the authentic signal, and then rebroadcasts it. This principle determines that there is usually only one counterfeit signal corresponding to each satellite, namely, $N = 1$. Although the counterfeit signals for spoofing can be ahead of the authentic signal, we assume $\tau_n(t) \geq 0$ by symmetry in order to facilitate the discussion.



$i_\Sigma(t)$
or
$q_\Sigma(t)$
$c(t-\beta_0)$
$c(t-\beta_1)$
$c(t-\beta_M)$
Coherent Integration
Coherent Integration
Coherent Integration
Maximum Likelihood Estimator
$\hat{\tau}_0$, $\hat{x}_0$ or $\hat{y}_0$
$\hat{\tau}_1$, $\hat{x}_1$ or $\hat{y}_1$
$\hat{\tau}_N$, $\hat{x}_N$ or $\hat{y}_N$

Figure 3. Multi-correlator and maximum likelihood estimator.

As shown in Figure 3, a series of correlators whose time delays are $\beta_0, \beta_1, \beta_2, \cdots, \beta_M$ is deployed in the channel. Take the I branch for example, the composite signal is correlated with these correlators. It is assumed that the variations of $a_n(t)$, $\tau_n(t)$ and $\phi_n(t)$ are negligible and $D(\cdot)$ does not flip in the coherent integration time of T_{coh}. Then the result of this coherent integration can be expressed as

$$\begin{aligned} I_{m,k} &= \sum_{n=0}^{N} \frac{x_n}{T_{coh}} \int_{t_k}^{t_k+T_{coh}} c(t-\tau_n)c(t-\beta_m)\mathrm{d}t + I_{m,k}^{\mathrm{v}} \\ &= \sum_{n=0}^{N} x_n R_{\mathrm{C}}(\beta_m - \tau_n) + I_{m,k}^{\mathrm{v}}, \end{aligned} \tag{3}$$

where k is the index of the discretized sampling time t_k, $R_{\mathrm{C}}(\cdot)$ is the autocorrelation function of the CA code, $m = 0, 1, 2, \cdots, M$, and

$$x_n = a_n A_0 \cos(\phi_n), \tag{4}$$

$$I_{m,k}^{\mathrm{v}} = \frac{1}{T_{\mathrm{coh}}} \int_{t_k}^{t_k+T_{coh}} v_{\mathrm{i}}(t)c(t-\beta_m)\mathrm{d}t. \tag{5}$$

Similarly, the expressions for the quadrature branch are written as

$$Q_{m,k} = \sum_{n=0}^{N} y_n R_{\mathrm{C}}(\beta_m - \tau_n) + Q_{m,k}^{\mathrm{v}}, \tag{6}$$

$$y_n = a_n A_0 \sin(\phi_n), \tag{7}$$

$$Q_{m,k}^{\mathrm{v}} = \frac{1}{T_{\mathrm{coh}}} \int_{t_k}^{t_k+T_{coh}} v_{\mathrm{q}}(t)c(t-\beta_m)\mathrm{d}t. \tag{8}$$

Assume that $v_{\mathrm{i}}(t)$ and $v_{\mathrm{q}}(t)$ are white Gaussian noises with zero mean and variance σ_{v}^2, then $I_{m,k}^{\mathrm{v}}$ and $Q_{m,k}^{\mathrm{v}}$ are white Gaussian noises with

$$\begin{cases} \mathrm{E}\left(I_{m,k}^{\mathrm{v}}\right) = \mathrm{E}\left(Q_{m,k}^{\mathrm{v}}\right) = 0 \\ E\left[I_{m_1,k}^{\mathrm{v}} I_{m_2,k}^{\mathrm{v}}\right] = E\left[Q_{m_1,k}^{\mathrm{v}} Q_{m_2,k}^{\mathrm{v}}\right] = \frac{\sigma_{\mathrm{v}}^2}{N_{\mathrm{coh}}} R_{\mathrm{C}}(\beta_{m_1} - \beta_{m_2}), \end{cases} \tag{9}$$

where $m_1 = 0, 1, 2, \cdots, M$, $m_2 = 0, 1, 2, \cdots, M$.

Take the I branch for instance and ignore k. Equation (3) can be extended to a matrix form as

$$\boldsymbol{I}_\Sigma = \boldsymbol{G}_\Sigma \boldsymbol{X}_\Sigma + \boldsymbol{I}_\Sigma^{\mathrm{v}}, \tag{10}$$

where

$$\boldsymbol{I}_\Sigma = [I_0\ I_1\ I_2\ \cdots\ I_M]^T, \tag{11}$$

$$\boldsymbol{X}_\Sigma = [x_0\ x_1\ x_2\ \cdots\ x_N]^T, \tag{12}$$

$$\boldsymbol{I}_\Sigma^{\mathrm{v}} = [I_0^{\mathrm{v}}\ I_1^{\mathrm{v}}\ I_2^{\mathrm{v}}\ \cdots\ I_M^{\mathrm{v}}]^T, \tag{13}$$

$$\boldsymbol{G}_\Sigma = \begin{bmatrix} R_{\mathrm{C}}(\beta_0 - \tau_0) & R_{\mathrm{C}}(\beta_0 - \tau_1) & \cdots & R_{\mathrm{C}}(\beta_0 - \tau_N) \\ R_{\mathrm{C}}(\beta_1 - \tau_0) & R_{\mathrm{C}}(\beta_1 - \tau_1) & \cdots & R_{\mathrm{C}}(\beta_1 - \tau_N) \\ \vdots & \vdots & \ddots & \vdots \\ R_{\mathrm{C}}(\beta_M - \tau_0) & R_{\mathrm{C}}(\beta_M - \tau_1) & \cdots & R_{\mathrm{C}}(\beta_M - \tau_N) \end{bmatrix}, \tag{14}$$

and the covariance matrix of $\boldsymbol{I}_\Sigma^{\mathrm{v}}$ is $\boldsymbol{P}_\Sigma = \frac{\sigma_{\mathrm{v}}^2}{N_{\mathrm{coh}}} \boldsymbol{C}_\Sigma$, where

$$\boldsymbol{C}_\Sigma = \begin{bmatrix} 1 & R_{\mathrm{C}}(\beta_0 - \beta_1) & \cdots & R_{\mathrm{C}}(\beta_0 - \beta_M) \\ R_{\mathrm{C}}(\beta_1 - \beta_0) & 1 & \cdots & R_{\mathrm{C}}(\beta_1 - \beta_M) \\ \vdots & \vdots & \ddots & \vdots \\ R_{\mathrm{C}}(\beta_M - \beta_0) & R_{\mathrm{C}}(\beta_M - \beta_1) & \cdots & 1 \end{bmatrix}. \tag{15}$$

It is handy that the observation vector $\boldsymbol{I}_\Sigma$ follows a Gauss distribution, namely $\boldsymbol{I}_\Sigma \sim \mathrm{N}(\boldsymbol{G}_\Sigma \boldsymbol{X}_\Sigma, \boldsymbol{P}_\Sigma)$.

It can be assumed that τ_n is known to facilitate the estimation of signal parameters. In this case, only linear problems need to be solved. Actually, τ_n can hardly be consistent with our assumption. In this case, some additional strategies are needed to estimate τ_n. See Step 3 in Section 4 for more details. The probability distribution function (PDF) of $\boldsymbol{I}_\Sigma$ given $\boldsymbol{X}_\Sigma$ can be expressed as

$$f(\boldsymbol{I}_\Sigma | \boldsymbol{X}_\Sigma) = \frac{1}{\left(\sqrt{2\pi}\right)^{M+1} \det(\boldsymbol{P}_\Sigma)^{1/2}} \exp\left\{ -\frac{1}{2} [\boldsymbol{I}_\Sigma - \boldsymbol{G}_\Sigma \boldsymbol{X}_\Sigma]^T \boldsymbol{P}_\Sigma^{-1} [\boldsymbol{I}_\Sigma - \boldsymbol{G}_\Sigma \boldsymbol{X}_\Sigma] \right\}. \tag{16}$$

Furthermore, we select the following ML function

$$\mathrm{L}(\boldsymbol{I}_\Sigma, \boldsymbol{X}_\Sigma) = \ln f(\boldsymbol{I}_\Sigma | \boldsymbol{X}_\Sigma). \tag{17}$$

Then, the ML estimate of $\boldsymbol{X}_\Sigma$ [22] is

$$\hat{\boldsymbol{X}}_\Sigma = \left(\boldsymbol{G}_\Sigma^T \boldsymbol{C}_\Sigma^{-1} \boldsymbol{G}_\Sigma \right)^{-1} \boldsymbol{G}_\Sigma^T \boldsymbol{C}_\Sigma^{-1} \boldsymbol{I}_\Sigma. \tag{18}$$

Similarly, the ML estimate of $\boldsymbol{Y}_\Sigma = [y_0\ y_1\ y_2\ \cdots\ y_N]^T$ for the quadrature branch can be obtained as

$$\hat{\boldsymbol{Y}}_\Sigma = \left(\boldsymbol{G}_\Sigma^T \boldsymbol{C}_\Sigma^{-1} \boldsymbol{G}_\Sigma \right)^{-1} \boldsymbol{G}_\Sigma^T \boldsymbol{C}_\Sigma^{-1} \boldsymbol{Q}_\Sigma, \tag{19}$$

where $\boldsymbol{Q}_\Sigma = [Q_0\ Q_1\ Q_2\ \cdots\ Q_M]^T$.

It can be drawn from the above derivations that M must be no less than N. In particular, it is possible that $M = N$ and $\beta_0, \beta_1, \beta_2, \cdots, \beta_M$ are equal to $\tau_0, \tau_1, \tau_2, \cdots, \tau_N$, respectively. In this setting, Equations (18) and (19) can be simplified as

$$\hat{\boldsymbol{X}}_\Sigma = \boldsymbol{C}_\Sigma^{-1} \boldsymbol{I}_\Sigma, \tag{20}$$

$$\hat{\boldsymbol{Y}}_\Sigma = \boldsymbol{C}_\Sigma^{-1} \boldsymbol{Q}_\Sigma. \tag{21}$$

When the time delay of a counterfeit signal equals β_n, only the sum of squares of $\hat{x}_n$ and $\hat{y}_n$ is not obviously close to 0 regardless of the authentic signal. Other cases and the specific deployment of multiple-correlators will be explained in detail in the next section.

4. Detection and Removal of Counterfeit Signals

Since a wide correlator with 0.5 chips spacing between early and prompt correlators (or the spacing between prompt and late correlators) of the code loop is vulnerable to multipath effects or similar spoofing, the spacing d is typically set to 0.5 chips to validate the effectiveness of the proposed anti-spoofing method. It is assumed that the target receiver has locked authentic signals before spoofing is applied. It is well-known that the carrier frequency difference between the counterfeit signal and its corresponding authentic signal makes spoofing very easy to be detected. Since the repeater and the target receiver are usually very close, the repeater obtains the carrier frequency of the authentic signal before delaying and amplifying the authentic signal. As a result, the carrier frequency of the counterfeit signal rebroadcasted by the repeater is close to that of the authentic signal received by the target receiver. Hence, the carrier frequencies of the counterfeit signal and its corresponding authentic signal are set to be the same [19]. The counterfeit signal is effectively overlapped with the authentic signal only when the distance between the correlation peaks of the two signals is less than 1.5 chips. If the distance between the correlation peaks of the counterfeit signal and the authentic signal is greater than 1.5 chips, then the counterfeit signal is considered to have a long delay. This kind of counterfeit signal cannot directly affect the result of the code phase discriminator, but the partial energy of its correlation peak may stimulate a number of correlators with long time delays in the multi-correlator structure. Accordingly, this will adversely affect the estimation of signal parameters and lead to erroneous restoring of the authentic signal. Therefore, the multi-correlator structure should have self-checking capabilities, i.e., it should be able to detect whether the counterfeit signal has a long delay to help the receiver to take reasonable countermeasures in the face of spoofing at different stages (see Figure 2). For these reasons, we let $N = 8$ and note that $\beta_0, \beta_1, \beta_2, \cdots, \beta_M$ are equal to $\tau_0, \tau_1, \tau_2, \cdots, \tau_N$, respectively. β_n are set to $0.2n$ chips, respectively, where $n = 0, 1, 2, \cdots, N$.

The time delays of the counterfeit signals for spoofing are usually not equal to those of the deployed multi-correlator. Detection and removal of counterfeit signals should be carried out according to the following steps.

Step 1: Determine whether the signal amplitude of the n-th correlator is valid.

According to Equations (20) and (21), the estimated x_n and y_n are obtained as $\hat{x}_n$ and $\hat{y}_n$ and $\hat{A}_n = \sqrt{\hat{x}_n^2 + \hat{y}_n^2}$ denotes the estimate of $A_n = a_n A_0$. In order to facilitate the discussion, $\hat{A}_n$ is termed as the signal amplitude of the n-th correlator. We choose the value of threshold A based on the carrier-to-noise ratio C/N_0 of the authentic signal. That is, the value of A is set according to A_0, which can be obtained from the stimulation of the authentic signal to the first correlator based on the assumption that the target receiver locks authentic signals in advance. If $\hat{A}_n > A$, $\hat{A}_n$ is valid. Otherwise, $\hat{A}_n$ is invalid.

Step 2: Determine whether the counterfeit signal has a long delay.

If the counterfeit signal has a long delay, the correlation peak of the counterfeit signal is closest to that of the correlator with a time delay of 1.6 chips. The stimulating effect on this correlator is also the most significant. Hence, if $\hat{A}_8 > \hat{A}_7 + A$, the counterfeit signal is considered to have a long delay and not to be overlapped effectively with the authentic signal. Then go to Step 6. Otherwise, countinue to Step 3. More details on determining whether the counterfeit signal has a long delay will be further explained in the following experiments.

Step 3: Determine the time delay and amplitude of the counterfeit signal.

In practice, there is usually only one counterfeit signal in any channel. In this case, besides $\hat{A}_0$, the signal amplitude(s) of one single correlator or two adjacent correlators will be valid. Based on this assumption, if $\hat{A}_0$, $\hat{A}_n$ and $\hat{A}_{n+1}$ are valid, where $n = 1, 2, \cdots, 7$, then

$$\hat{\tau}_x = \tau_n + \frac{\hat{x}_{n+1}}{\hat{x}_n + \hat{x}_{n+1}}(\tau_{n+1} - \tau_n) := \tau_n + \lambda_x(\tau_{n+1} - \tau_n), \tag{22}$$

$$\hat{\tau}_y = \tau_n + \frac{\hat{y}_{n+1}}{\hat{y}_n + \hat{y}_{n+1}}(\tau_{n+1} - \tau_n) := \tau_n + \lambda_y(\tau_{n+1} - \tau_n). \tag{23}$$

Generally, $\hat{\tau}_x \neq \hat{\tau}_y$, so we have

$$\hat{\tau} = \tau_n + \frac{\lambda_x \hat{x} + \lambda_y \hat{y}}{\hat{x} + \hat{y}}(\tau_{n+1} - \tau_n), \tag{24}$$

$$\hat{A} = \sqrt{\hat{x}^2 + \hat{y}^2}, \tag{25}$$

where $\hat{x}$ and $\hat{y}$ are the estimated amplitudes of the I branch and the Q branch of the counterfeit signal, respectively and

$$\hat{x} = \hat{x}_n + \hat{x}_{n+1}, \tag{26}$$

$$\hat{y} = \hat{y}_n + \hat{y}_{n+1}. \tag{27}$$

If only $\hat{A}_0$ and $\hat{A}_n$ are valid, then the estimated time delay $\hat{\tau}$ of the counterfeit signal is equal to $0.2n$ chips and the estimated amplitude $\hat{A}$ is equal to $\hat{A}_n$, where $n = 2, 3, \cdots, 7$. If only $\hat{A}_0$ and $\hat{A}_1$ are valid, then $\hat{\tau} \leq 0.2$ chips. Eliminating the effect of the authentic signal on the estimated amplitude of the first correlator in the I branch, we have from Equation (26)

$$\hat{x} = \hat{x}_0' + \hat{x}_1, \tag{28}$$

where $\hat{x}_0' = \hat{x}_0 - A_0$. Afterwards, $\hat{\tau}$ and $\hat{A}$ can still be obtained using Equations (24) and (25).

If the above assumptions are not valid, it is indicated that the effect of noise is significant or there is more than one counterfeit signal in the current channel. In this scenario, we can either deploy additional correlators near the correlators whose signal amplitudes are valid to calculate $\hat{\tau}$ and $\hat{A}$, or just skip the calculation of $\hat{\tau}$ and $\hat{A}$ such that the authentic signal is directly restored with the valid signal amplitudes. Since this situation is rare, it will not be detailed here.

Step 4: Determine the carrier phase of the counterfeit signal.

In the process of determining the time delay and amplitude of the counterfeit signal, the calculations of $\hat{x}$ and $\hat{y}$ are involved in different cases. It should be pointed out that the C/N_0 of the authentic signals used in the experiments are relatively high. Correspondingly, the counterfeit signals whose power is slightly higher than that of their corresponding authentic signals also have relatively high C/N_0. Therefore, based on $\tan(\hat{\varphi}) = \hat{y}/\hat{x}$, the estimated carrier phase of the counterfeit signal can be obtained in three cases. If $\hat{x} > 0$, $\hat{\varphi} = \arctan(\hat{y}/\hat{x})$. If $\hat{x} < 0$, $\hat{\varphi} = \pi + \arctan(\hat{y}/\hat{x})$. If $\hat{x} = 0$, $\hat{\varphi} = \mathrm{sgn}(\hat{y})\pi/2$.

Step 5: Remove the counterfeit signal.

After detecting the time delay, amplitude and carrier phase of the counterfeit signal, the counterfeit signal is confirmed to have a short delay. The opposite counterfeit signal is added to the composite signal to restore the authentic signal. It is worth noting that the assumption of locking the authentic signal in advance can prevent us from mistakenly removing the authentic signal.

Step 6: Discriminate the phase of the authentic signal.

Discriminate the phase of the authentic signal with the normalized early minus late envelope function and go to the next loop.

The corresponding flow chart is shown in Figure 4.

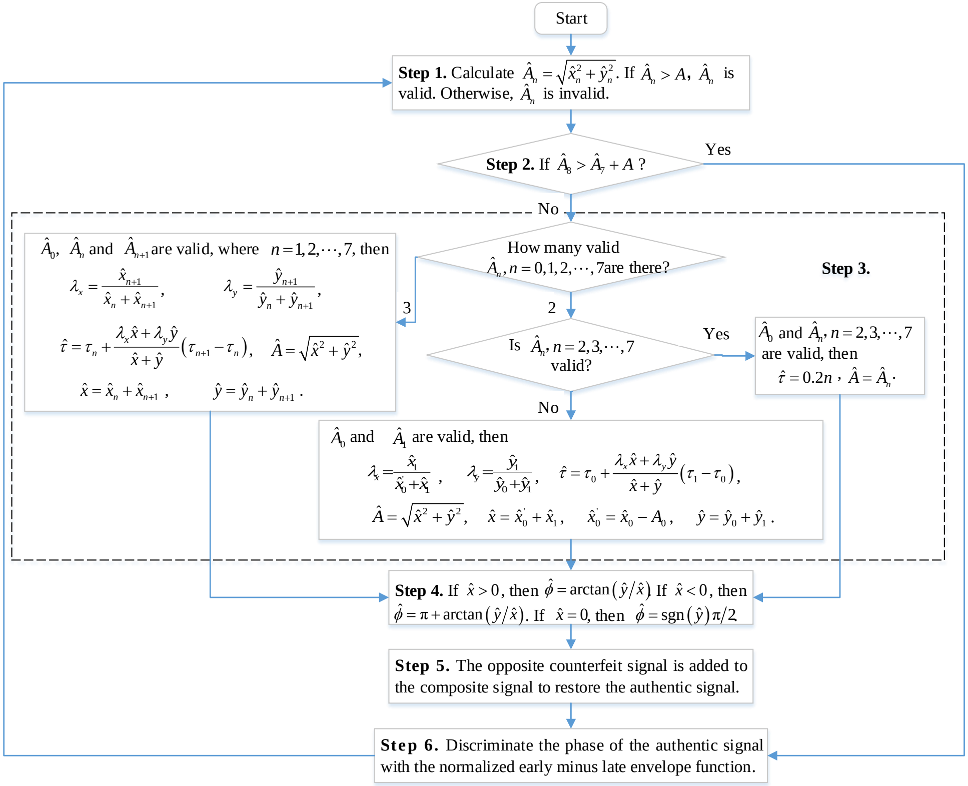

Start
Step 1. Calculate $\hat{A}_n = \sqrt{\hat{x}_n^2 + \hat{y}_n^2}$. If $\hat{A}_n > A$, $\hat{A}_n$ is valid. Otherwise, $\hat{A}_n$ is invalid.
Step 2. If $\hat{A}_8 > \hat{A}_7 + A$?
Yes
No
How many valid $\hat{A}_n, n = 0,1,2,\cdots,7$are there?
Step 3.
3
2
$\hat{A}_0$, $\hat{A}_n$ and $\hat{A}_{n+1}$are valid, where $n = 1,2,\cdots,7$, then
$\lambda_x = \frac{\hat{x}_{n+1}}{\hat{x}_n + \hat{x}_{n+1}}$, $\lambda_y = \frac{\hat{y}_{n+1}}{\hat{y}_n + \hat{y}_{n+1}}$,
$\hat{\tau} = \tau_n + \frac{\lambda_x \hat{x} + \lambda_y \hat{y}}{\hat{x} + \hat{y}}(\tau_{n+1} - \tau_n)$, $\hat{A} = \sqrt{\hat{x}^2 + \hat{y}^2}$,
$\hat{x} = \hat{x}_n + \hat{x}_{n+1}$, $\hat{y} = \hat{y}_n + \hat{y}_{n+1}$.
Is $\hat{A}_n, n = 2,3,\cdots,7$ valid?
Yes
$\hat{A}_0$ and $\hat{A}_n, n = 2,3,\cdots,7$ are valid, then $\hat{\tau} = 0.2n$, $\hat{A} = \hat{A}_n$.
No
$\hat{A}_0$ and $\hat{A}_1$ are valid, then
$\lambda_x = \frac{\hat{x}_1}{\hat{x}_0' + \hat{x}_1}$, $\lambda_y = \frac{\hat{y}_1}{\hat{y}_0 + \hat{y}_1}$, $\hat{\tau} = \tau_0 + \frac{\lambda_x \hat{x} + \lambda_y \hat{y}}{\hat{x} + \hat{y}}(\tau_1 - \tau_0)$,
$\hat{A} = \sqrt{\hat{x}^2 + \hat{y}^2}$, $\hat{x} = \hat{x}_0' + \hat{x}_1$, $\hat{x}_0' = \hat{x}_0 - A_0$, $\hat{y} = \hat{y}_0 + \hat{y}_1$.
Step 4. If $\hat{x} > 0$, then $\hat{\phi} = \arctan(\hat{y}/\hat{x})$ If $\hat{x} < 0$, then $\hat{\phi} = \pi + \arctan(\hat{y}/\hat{x})$. If $\hat{x} = 0$, then $\hat{\phi} = \mathrm{sgn}(\hat{y})\pi/2$
Step 5. The opposite counterfeit signal is added to the composite signal to restore the authentic signal.
Step 6. Discriminate the phase of the authentic signal with the normalized early minus late envelope function.

Figure 4. Flow chart for detecting and removing the counterfeit signal.

The whole process of detecting and removing the counterfeit signal is elaborated above. Due to the complexity and variability of deliberate interferences, it is very difficult for one single anti-spoofing method to properly handle all kinds of spoofing. For example, the anti-spoofing method based on the multi-correlator structure can help the tracking receiver to keep the authentic signal locked. However, if spoofing during acquisitionalready exists, this method will be incapable of distinguishing between the authentic and counterfeit signals of the receiver. Therefore, multiple anti-spoofing methods should be adopted in the receiver simultaneously [18]. For instance, if the counterfeit signal corresponding to each satellite comes from a single interference source, the antenna can be moved along any small trajectory. In this case, the relative motion between the receiver and the repeater makes the variation of the carrier frequency of each counterfeit signal exactly the same. If the multi-correlator structure can detect the spoofing at the initial tracking stage, this method can be introduced to help the receiver determine whether the locked signal is the authentic signal. If spoofing with unlocked carrier frequency succeeds in spoofing the target receiver, significant abnormalities in the outputs of phase discriminators will be inevitable [19]. In this case, this method can also be introduced to help the receiver determine whether it is necessary to enter the reacquisition stage. If the carrier frequency difference between the counterfeit signal and its corresponding authentic signal increases to a relatively large value, two distinct correlation peaks will appear at the reacquisition stage. That is, the spoofing degenerates into the simplistic form. In addition, other common anti-spoofing methods can also be used on the receiver to detect the simplistic spoofing earlier or more conveniently and ensure the correctness of the positioning results.

5. Experimental Results and Analysis

5.1. Spoofing

Since it is prohibited to broadcast spoofing signals in real world, the following method is devised to simulate an intentional attack, as shown in Figure 5. Firstly, a previously stored interval of authentic

IF GPS signals with a sampling rate of 38.192 MHz is read. Secondly, these loaded signals are acquired and tracked by a software receiver, and the authentic signal from each satellite is amplified by 1.2 times such that the output is denoted as the counterfeit signal. Thirdly, time delay is applied to the counterfeit signal from each satellite. Lastly, we simulate the composite signals received by the target receiver by adding all original authentic signals and certain time-delayed counterfeit signals.

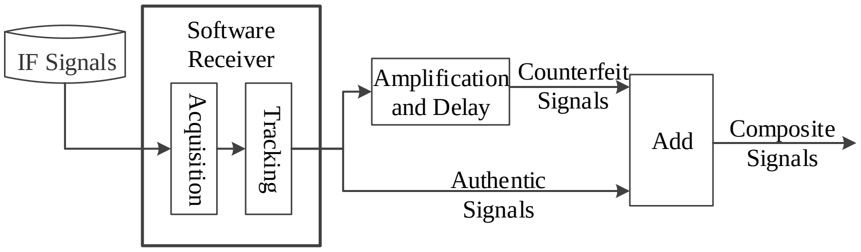


Figure 5. Simulation of spoofing.

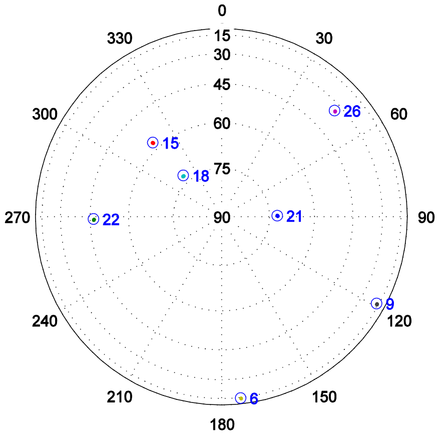


Figure 6. Satellites sky plot.

The visible satellites corresponding to the used IF signals are shown in Figure 6. Fixed delay spoofing and variable delay spoofing are applied to PRN22 and PRN21, respectively. The fixed delay spoofing is executed at 300 ms and the delay is 0.6 chips. The variable delay spoofing is also executed at 300 ms and the delay changes gradually from 0 chips to 2 chips. It should be noted that all time domains where there are spoofing signals are highlighted in the following figures.

Figure 7 shows the outputs of the prompt correlators of PRN22 I and Q branches within 1000 ms. The receiver starts tracking at 0 ms. Since the initial tracking value obtained by the conventional acquisition method is not accurate enough, the carrier phase of the local signal gradually aligns with that of the authentic signal until about 180 ms. The output of the I prompt correlator is stabilized at around 1. After the spoofing is executed, the output of the quadrature prompt correlator suddenly changes, which indicates that the carrier phases of the counterfeit signal and the authentic signal are not the same. However, the counterfeit signal lags behind the authentic signal by only 0.6 chips. Their carrier frequencies are close, and the carrier phase difference between them is almost fixed. Therefore, the carrier phases of the local signal and the composite signal align rapidly, and the output of the quadrature prompt correlator is restored to near zero. At the same time, due to the large amplitude of the composite signal, the output of the I prompt correlator becomes larger. In addition, the noises of the prompt correlators of I and Q branches also become larger after the spoofing is executed, which indicates that spoofing signals might increase the noise level and deteriorate the precision of the estimated coordinates (similar to solar radio emission) [23]. As shown in Figure 8, at the beginning of spoofing, there is a significant jump in the output of the code phase discriminator of PRN22, which is confirmed by the results in Figure 7 and vice versa. The effective overlapping of the counterfeit signal and the authentic signal is equivalent to indirectly magnifying C/N_0. Consequently, after the receiver locks the composite signal, the accuracy of the code phase discriminator is slightly improved.

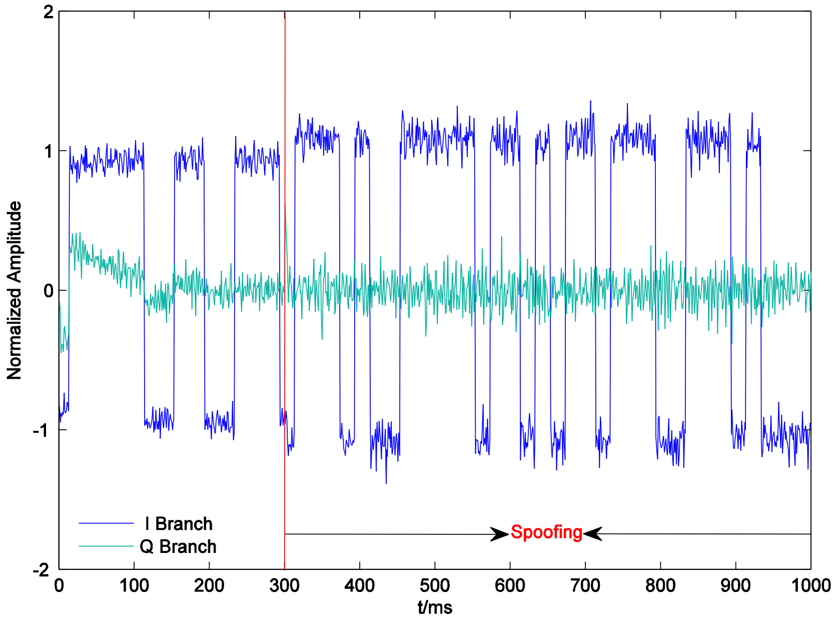


Figure 7. Outputs of the prompt correlators of PRN22 I and Q branches.

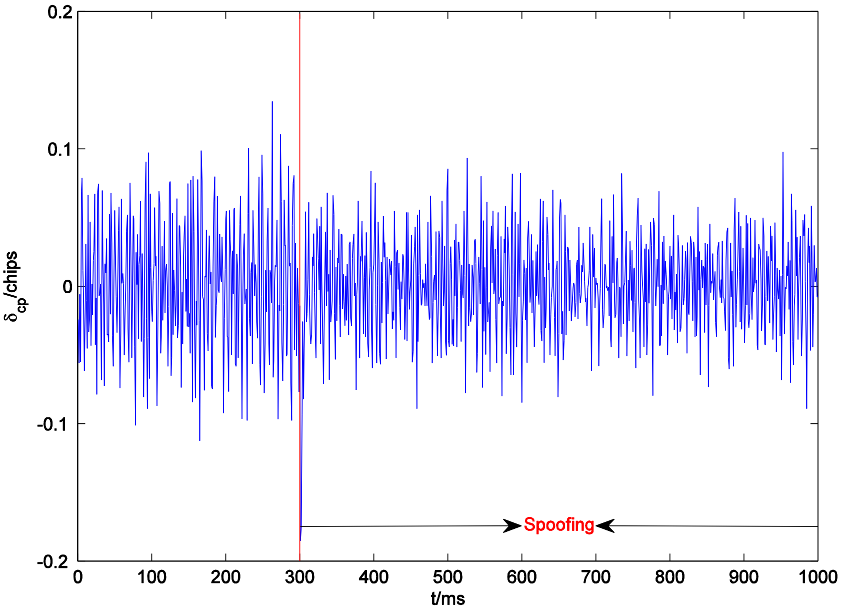


Figure 8. Code phase tracking error δ_{cp} of the code phase discriminator of PRN22.

Figure 9 shows the outputs of the prompt correlators of PRN21 I and Q branches within 1000 ms. On one hand, since the counterfeit signal corresponding to the PRN 21 has the same carrier phase as the authentic signal, the output of the quadrature prompt correlator remains near 0 throughout spoofing. On the other hand, at the beginning of spoofing, the output of the I prompt correlator has jumped to about 2.2, which is the sum of the amplitudes of the counterfeit signal and the authentic signal. It decreases and finally arrives at the steady state of around 1.2 as the counterfeit signal correlation peak gradually moves away from the authentic signal correlation peak. This indicates that the receiver has turned to lock the counterfeit signal. As shown in Figure 10, the accuracy of the code phase discriminator is improved during the effective overlapping of the counterfeit signal and the authentic signal. Since the signal and noise are both amplified at the same time when generating the counterfeit signal, after the two correlation peaks move away from each other, the accuracy of the code phase discriminator is restored to the level at which the spoofing was not executed.

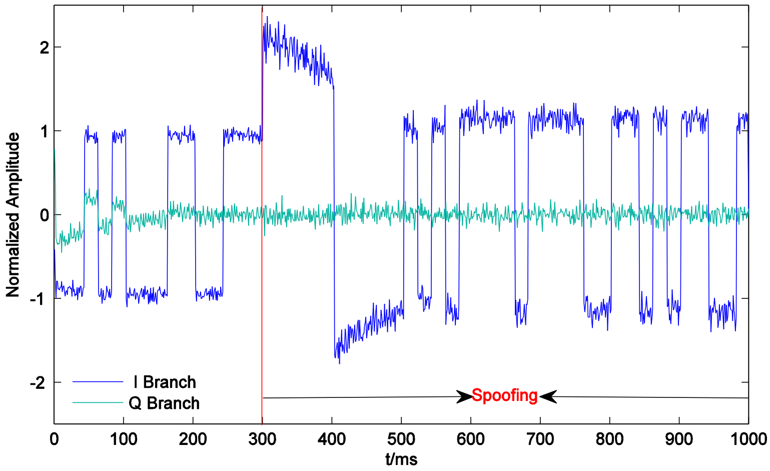


Figure 9. Outputs of the prompt correlators of PRN21 I and Q branches.

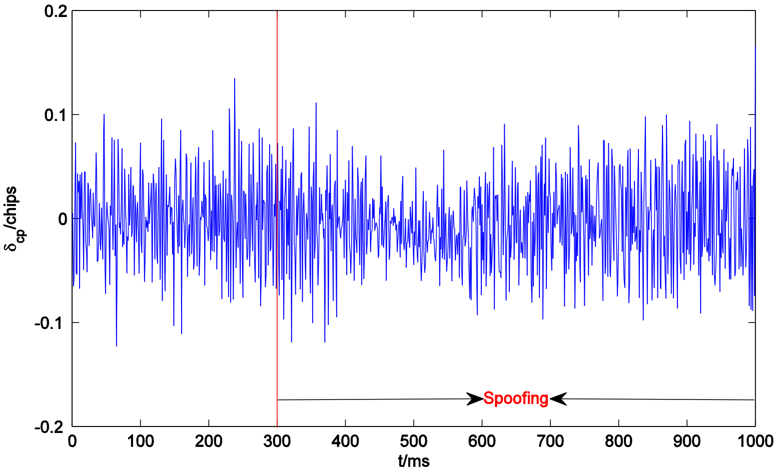


Figure 10. The δ_{cp} of the code phase discriminator of PRN21.

5.2. Anti-Spoofing Effect of the Multi-Correlator Structure

In order to facilitate the discussion, in addition to the above spoofing, spoofing with fixed short delays is applied to PRN18, PRN15, and PRN26, and spoofing with fixed long delays is applied to PRN9 and PRN6. The setups of time delays are shown in Table 1. The counterfeit signal and its corresponding authentic signal from each satellite are set to have the same carrier phase. Figure 11 shows the estimation result of PRN22's carrier phase when the carrier phases of the counterfeit signal and its corresponding authentic signal are different. Hence, the carrier phases of the counterfeit signal and its corresponding authentic signal from each satellite are set to be the same in order to focus on the estimation of time delay and amplitude. In addition, we let $A = 0.2A_0$ empirically.

Table 1. Time delays of counterfeit signals.

Counterfeit Signal	Fixed Delay
PRN18	0.11 chips
PRN15	1.05 chips
PRN26	1.5 chips
PRN9	1.69 chips
PRN6	2.49 chips

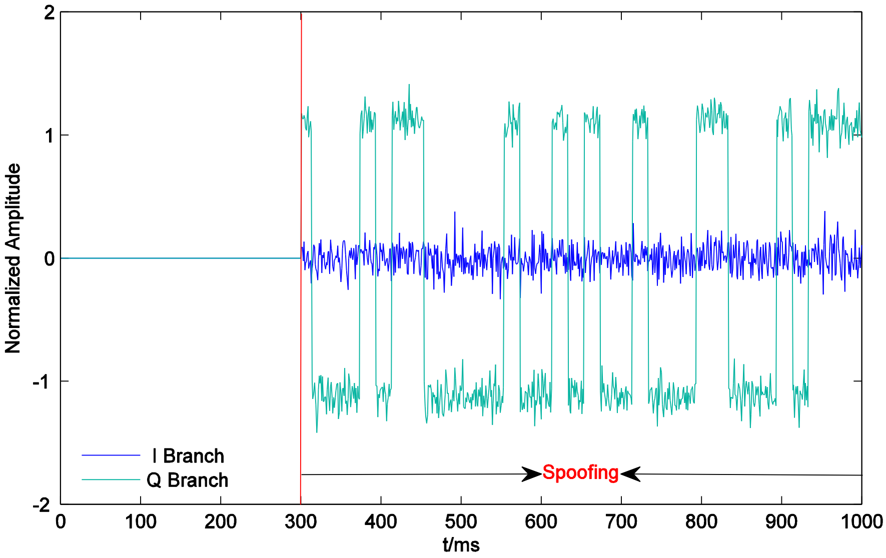
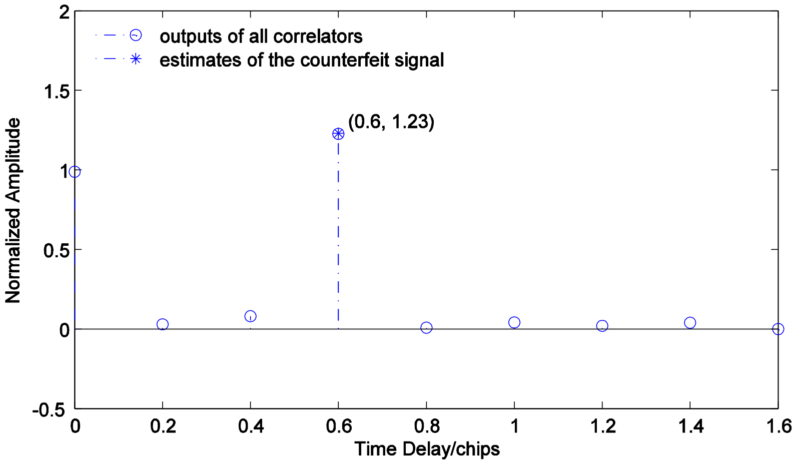


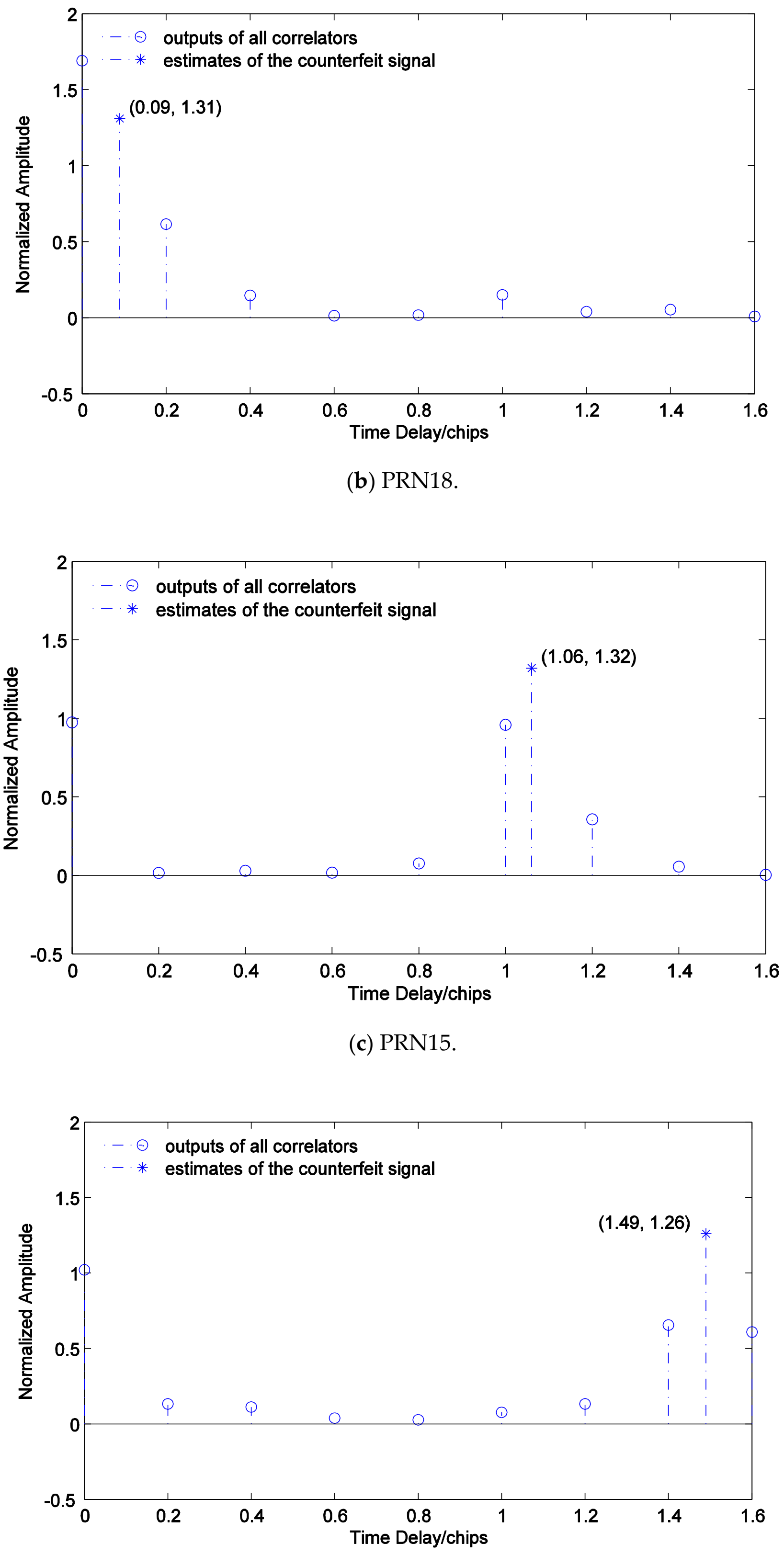
Figure 11. $\hat{x}$ and $\hat{y}$ of the counterfeit signal of PRN22.

Figure 11 shows $\hat{x}$ and $\hat{y}$ of the counterfeit signal of PRN22. It can be seen that the carrier phase of the counterfeit signal is different from that of the authentic signal, which is consistent with the results in Figures 7 and 8. If the effect of the data bit flipping is disregarded, the carrier phase of the counterfeit signal is approximately $-\pi/2$. Since the results of ML estimation at different instants are independent, and its effects at different instants are similar, the estimation results at a certain instant are visualized in order to demonstrate the effect of the multi-correlator structure and to verify the estimation method described conveniently in Section 4. Figure 12 shows all correlators' outputs of I branches of PRN22, PRN18, PRN15, and PRN26, and corresponding estimated time delays and amplitudes of the counterfeit signals. It is observed that the estimates are consistent with the true values, which means the proposed multi-correlator structure is accurate in estimating the time delays and amplitudes of the counterfeit signals.



(**a**) PRN22.

Figure 12. *Cont.*



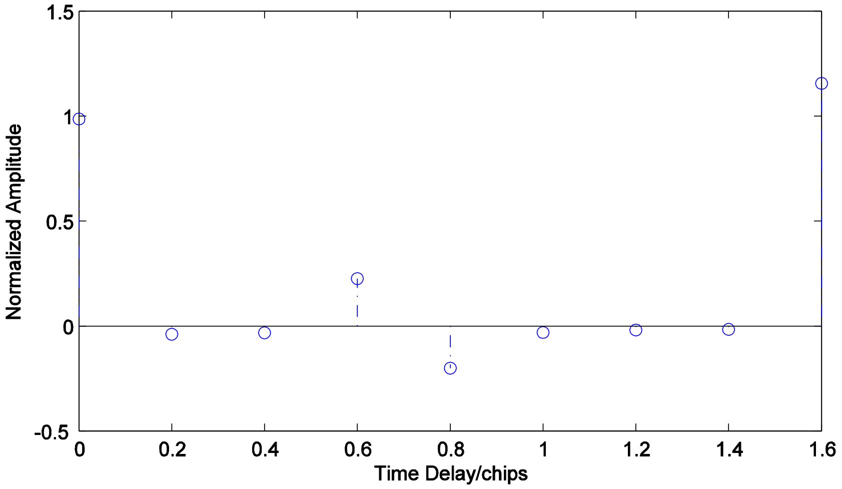
(**b**) PRN18.

(**c**) PRN15.

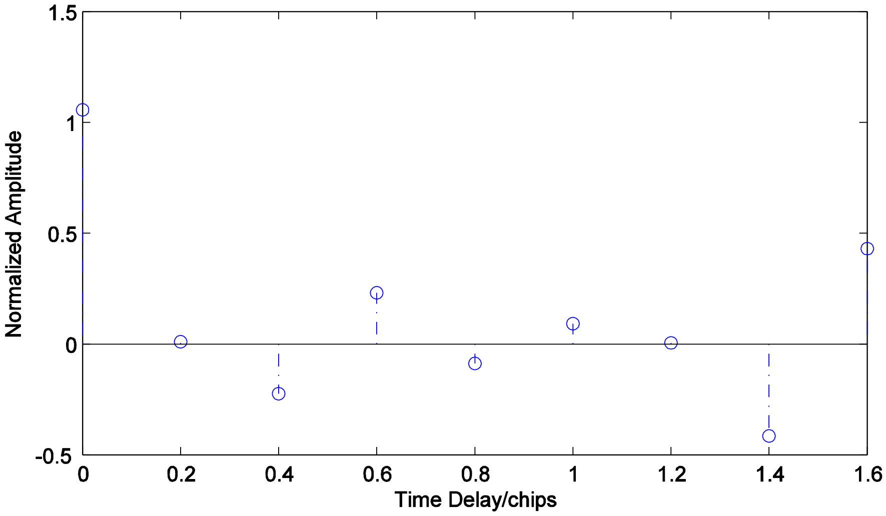
(**d**) PRN26.

Figure 12. Estimated time delays and amplitudes of the counterfeit signals with short delays

Figure 13 shows all correlators' outputs of I branches of PRN9 and PRN6. Since the time delay of the counterfeit signal of PRN9 is close to 1.6 chips, the stimulating effect on the last correlator in subfigure (a) is significant. The receiver can easily determine that the counterfeit signal has a long delay and directly starts discriminating the phase of the authentic signal. Note that the sizes of $\hat{x}_7$ and $\hat{x}_8$ in subfigure (b) are close. However, if the time delay of the counterfeit signal is within the effective estimation interval of the multi-correlator structure from 0 to 1.6 chips, it is impossible that $\hat{x}_n$ and $\hat{x}_{n+1}$ of two adjacent correlators are close in size but are opposite in direction. Therefore, this can help the receiver to recognize the counterfeit signal with a long delay, and then perform phase discrimination directly on the authentic signal.



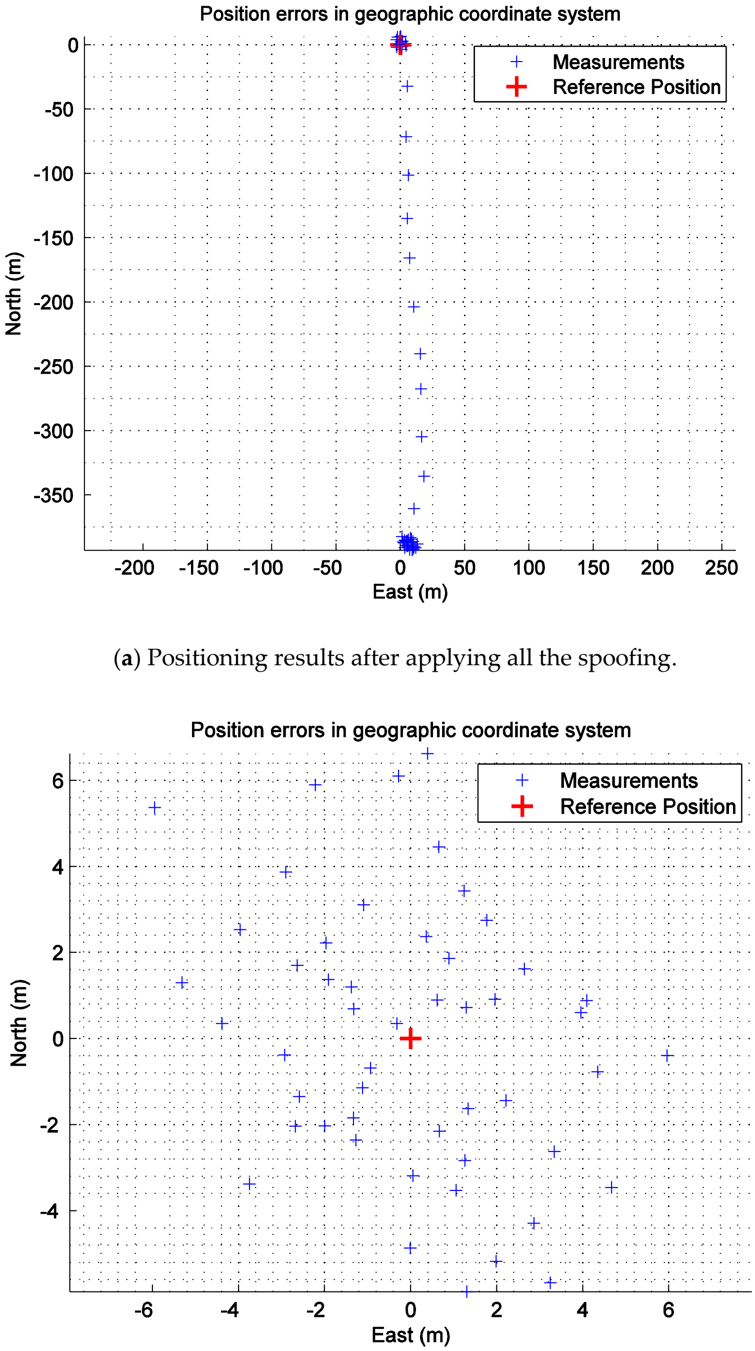
(**a**) PRN9.



(**b**) PRN6.

Figure 13. All correlators' outputs of I branches of the counterfeit signals with long delays.

Figure 14 shows the positioning results after applying all the spoofing and the positioning results after employing the proposed anti-spoofing method in an east–north–up geographic coordinate system. The period of data update is 20 ms. In subfigure (a), the positioning of the target receiver is normal at 0-300 ms. Then, all the spoofing is executed at 300 ms. As a result, the positioning results of the target receiver gradually deviate from the real position and finally arrive at the steady state. In subfigure (b), the positioning of the target receiver remains stable and is not obviously affected by the spoofing, which consolidates the effectiveness of the proposed anti-spoofing method.



(**a**) Positioning results after applying all the spoofing.

(**b**) Positioning results after employing the proposed anti-spoofing method.

Figure 14. The positioning results after applying all the spoofing and the positioning results after employing the proposed anti-spoofing method.

6. Conclusions

In this paper, several anti-spoofing methods are introduced, and their characteristics are briefly summarized. On this basis, the similarities and differences between spoofing and multipath are analyzed. Improvements of the multipath estimation method are proposed to detect and mitigate spoofing accordingly. Based on ML estimation, the tracking channels with multi-correlators are constructed. At the same time, a set of corresponding steps of detecting and removing the counterfeit signals is designed. The experimental results show that the proposed anti-spoofing method can accurately estimate the time delay, amplitude, and carrier phase of the counterfeit signal with a short delay and can then eliminate it by adding the opposite counterfeit signal. Besides, this method is able to perform self-checking such that it can directly discriminate the phase of the authentic signal when the counterfeit signal has a long delay. In conclusion, the proposed method can ensure that the receiver keeps the authentic signal locked when the correlation peak of the counterfeit signal is overlapped with or moves away from that of the authentic signal and can further guarantee that the receiver is positioned correctly in the presence of spoofing.

Author Contributions: Y.G. and X.Z. provided original ideas, completed mathematical modeling, and designed the experiments. Y.G. improved the novel method and some details, and wrote the paper. L.M. critically reviewed and edited the paper. All authors read, revised, and approved the final manuscript.

Funding: This research was financially supported by the National Natural Science Foundation of China, grant number 61473039.

Acknowledgments: The authors wish to acknowledge Yao Chen, who provided some valuable suggestions and modified the language for the responses to the reviewers' comments.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M., Jr. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008), Savannah, GA, USA, 16–19 September 2008; pp. 1198–1209.
2. Wen, H.; Huang, P.Y.; Dyer, J.; Archinal, A.; Fagan, J. Countermeasures for GPS Signal Spoofing. In Proceedings of the 18th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2005), Long Beach, CA, USA, 13–16 September 2005; pp. 1285–1290.
3. Jahromi, A.J.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS Spoofer Countermeasure Effectiveness Based on Signal Strength, Noise Power and C/N$_0$ measurements. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 181–191. [CrossRef]
4. Zhang, Z.; Zhan, X. GNSS Spoofing Network Monitoring Based on Differential Pseudorange. *Sensors* **2016**, *16*, 1771. [CrossRef] [PubMed]
5. 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]
6. Zhang, L. Research on Key Techniques of Anti-interference Satellite Navigation Receiver. Ph.D. Thesis, Harbin Institute of Technology, Harbin, China, 2007.
7. Lo, S.C.; Enge, P.K. Authenticating Aviation Augmentation System Broadcasts. In Proceedings of the 2010 IEEE/ION Position, Location, and Navigation Symposium (IEEE/ION PLANS 2010), Indian Wells, CA, USA, 3–6 May 2010; pp. 708–717.
8. Lo, S.C.; Lorenzo, D.D.; Enge, P.K.; Akos, D.; Bradley, P. Signal Authentication: A Secure Civil GNSS for Today. *Inside GNSS* **2009**, *4*, 30–39.
9. 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 2009 International Technical Meeting of the Institute of Navigation (ITM 2009), Anaheim, CA, USA, 26–28 January 2009; pp. 124–130.
10. Nielsen, J.; Broumandan, A.; Lachapelle, G. Spoofing Detection and Mitigation with a Moving Handheld Receiver. *GPS World* **2010**, *21*, 27–33.
11. Nielsen, J.; Broumandan, A.; Lachapelle, G. GNSS Spoofing Detection for Single Antenna Handheld Receivers. *J. Inst. Navig.* **2011**, *58*, 335–344. [CrossRef]
12. Daneshmand, S.; Jahromi, A.J.; Broumandan, A.; Lachapelle, G. A Low-complexity GPS Anti-spoofing Method Using a Multi-antenna Array. In Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012; pp. 1233–1243.

13. Cavaleri, A.; Motella, B.; Pini, M.; Fantino, M. Detection of Spoofed GPS Signals at Code and Carrier Tracking Level. In Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC 2010), Noordwijk, The Netherlands, 8–10 December 2010; pp. 1–6.
14. 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 (ITM 2010), San Diego, CA, USA, 25–27 January 2010; pp. 698–712.
15. Pini, M.; Fantino, M.; Cavaleri, A.; Ugazio, S.; Lo Presti, L. Signal Quality Monitoring Applied to Spoofing Detection. In Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA, 19–23 September 2011; pp. 1888–1896.
16. Shepard, D.P.; Humphreys, T.E. Characterization of Receiver Response to a Spoofing Attack. In Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA, 19–23 September 2011; pp. 2608–2618.
17. 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 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA, 19–23 September 2011; pp. 2646–2656.
18. Broumandan, A.; Jahromi, A.J.; Lachapelle, G. Spoofing Detection, Classification and Cancelation (SDCC) Receiver Architecture for a Moving GNSS Receiver. *GPS Solut.* **2015**, *19*, 475–487. [CrossRef]
19. Humphreys, T.E.; Bhatti, J.A.; Shepard, D.P.; Wesson, K.D. The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques. In Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012; pp. 3569–3583.
20. Wang, F.; Li, H.; Lu, M. GNSS Spoofing Detection and Mitigation Based on Maximum Likelihood Estimation. *Sensors* **2017**, *17*, 1532. [CrossRef] [PubMed]
21. Gamba, G.; Fantinato, S.; Pozzobon, O.; Anghileri, M.; Ioannides, R.; Rodríguez, J.A. The Spoofing Estimating Delay Lock Loop. In Proceedings of the 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC 2014), Noordwijk, The Netherlands, 3–5 December 2014.
22. Gadallah, E.A. Global Positioning System (GPS) Receiver Design for Multipath Mitigation. Ph.D. Thesis, Air Force Institute of Technology, Dayton, OH, USA, 1998.
23. Demyanov, V.V.; Yasyukevich, Y.V.; Jin, S. References. In *Geodetic Sciences: Observations, Modeling and Applications*; Jin, S., Ed.; Effects of Solar Radio Emission and Ionospheric Irregularities on GPS/GLONASS Performance; InTech Publisher: Rijeka, Croatia, 2013; pp. 177–222, ISBN 978-953-51-1144-3.