IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 28, 2016, accepted June 14, 2016, date of publication September 21, 2016, date of current version January 27, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2587322

Performance Evaluation of Multimodal Detection Method for GNSS Intermediate Spoofing

JING LI[1,2], JIANTONG ZHANG[2], SHOUFENG CHANG[3], AND MENG ZHOU[4]

[1]University of Electronic Science and Technology of China
[2]China Transportation Telecommunications and Information Center, Beijing 100011, China
[3]Beijing Satellites Navigation Center, China
[4]Tsinghua University, Beijing, China

Corresponding author: J. Zhang (zhangjiantong@cttic.cn)

This work was supported by the National Engineering Laboratory on Transportation Safety and Emergency Informatics, China.

ABSTRACT With the appearance of Global Navigation Satellite Systems spoofers, anti-spoofing has become a pressing issue. Intermediate spoofing is performed at a power only slightly higher than that of an authentic signal; therefore, it is quite difficult to detect counterfeit signals in real time via current detection methods. Multimodal detection is a well-known method for detecting counterfeit signals. However, it is often used in the acquisition stage, and thus, its effective time is very short. In this paper, we define the searching process as when the acquisition module does not need to find new signals. In addition, we utilize multimodal detection to detect intermediate spoofing in the acquisition module when performing the searching process, which is almost real time and can address the condition of arbitrary signal intervals. The acquisition module is used to monitor the signals that are being tracked; if we find at least two peaks above a threshold, we declare that counterfeit signals are detected. Then, we define an evaluation standard and provide a theoretical performance calculation method. An empirical formula is proposed to calculate the method's performance. By analyzing the effect of five influencing factors, we better understand the empirical formula and obtain the conclusion that, by decreasing the code phase's search step, we can obtain better detection results. The results are desirable for designing anti-spoofing receivers.

INDEX TERMS Intermediate spoofing, acquisition module, multimodal detection, counterfeit signals, empirical formula.

I. INTRODUCTION

As a special form of interference, spoofing does great harm to GNSS. A spoofer generates counterfeit signals that are of the same signal structure as authentic signals, and they can induce a receiver to believe that they are authentic signals. Counterfeit signals have a certain purpose: to provide incorrect information to the target receiver, for example, incorrect navigation messages and incorrect pseudo-ranges. This can make the receiver output incorrect position or timing information. Moreover, a spoofer can manipulate the receiver to output information expected by the spoofer. Thus, spoofers represent an important threat to navigation applications, especially in fields related to people's livelihoods such as the military, electricity generation, and finance. In 2008, Texas University developed a low-cost spoofer and tested a commercial receiver's vulnerability in a lab environment [1].

Intermediate spoofing represents a certain type of spoofing [1]. This type of spoofing is able to spoof a GNSS receiver without interrupting the receiver's tracking loop. The counterfeit signal sent by the spoofer is of only slightly higher power than the authentic signal sent by GNSS satellites [1]–[4]. The spoofing process is presented in Fig. 1 [1]. Here, the Global Position System (GPS) civil signal (C/A code) is considered because it is the most widely used signal in GNSS. The process is as follows. First, the counterfeit signal enters the tracking loop with a low power and the same carrier frequency but a different code rate. Then, it moves toward the authentic signal in the code phase. Because of the periodicity of the GPS C/A code, the two signals will eventually align in the code phase. In this case, the authentic and counterfeit signals are completely synchronous in code phase and carrier frequency. Subsequently, the counterfeit signal increases its amplitude until it is locked by the tracking loop of the receiver. Indeed, only a slightly higher power can guarantee a successful locking. Then, the counterfeit signal continues moving its code phase until there is at least one code phase difference between the counterfeit signal and the authentic signal. Now, the receiver locks the

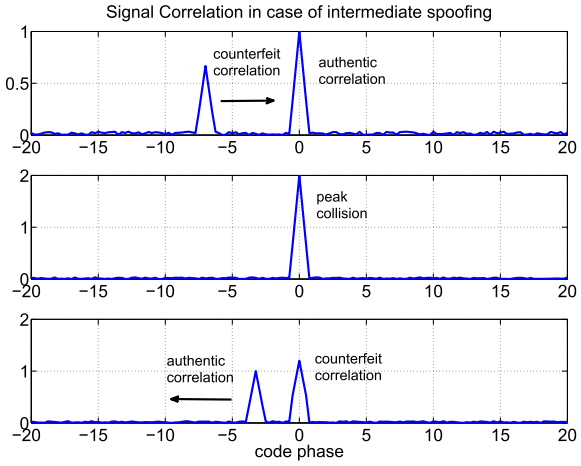

FIGURE 1. Schematic of intermediate spoofing.

counterfeit signal. Because pseudo-ranges are obtained from locked signals [5], an incorrect pseudo-range would be derived and would cause the receiver to output incorrect position information. Because the spoofing process would not cause a significant change in signal parameters [1], it is a secret and difficult to detect. This type of spoofer has been manufactured and demonstrated in an experiment [3]. In the experiment, an intermediate spoofer successfully spoofed a GPS receiver of an Unmanned Aerial Vehicle (UAV) and caused the UAV to deviate from its true position by 0.62 km.

Currently, the methods of detecting intermediate spoofing can be categorized into three types: antenna techniques, measurement domain techniques and baseband signal processing techniques. Antenna techniques detect and suppress spoofing by extracting and judging airspace information of the received signals [6], [7]. Such techniques are effective but expensive. Measurement domain techniques detect the reasonableness of measurements and the consistency of redundant information to detect spoofing [8]–[10] for GNSS receivers or to detect the multiple faults in GNSS/Inertial Navigation System (INS) Integration [11], [12]. When the changes in the measurements are not significant, the technique is inapplicable. Baseband signal processing techniques detect the variances produced by baseband signal processing, which are easily obtained, and can mitigate intermediate spoofing only at the expense of modifying or re-designing the signal processing algorithms of the receiver; therefore, it has become a hot topic.

Baseband signal processing techniques can also be divided into three types: signal power detection techniques, bit latency predictor techniques and signal quality monitoring techniques. Signal power detection techniques assume that the power of the counterfeit signal is higher than that of the authentic signal; therefore, when the power is larger than a certain threshold, it is considered to be a counterfeit signal [13]–[15]. This method requires a large difference between the two signals, and it is only valid in the acquisition stage. For intermediate spoofing, the powers of two signals may be similar, and in GNSS receivers, the acquisition stage is a transitory process. Therefore, the application of this method is limited. Moreover, when the signal's interval is small, the method is also limited. The bit latency predictor technique was proposed by TE Humphreys [1]. To generate counterfeit signals, the spoofer needs to predict the navigation message; therefore, the target receiver can check those bits in the navigation message that are special and difficult to predict. When the duration of the navigation message is 20 ms, to find an exception, a long observation time is required; therefore, the timeliness of this method is limited. Signal quality monitoring techniques check the disturbance of the tracking loop caused by counterfeit signals [1], [16], [17]. When the spoofing is performing its hauling process, the tracking loop will be disturbed because of signal overlap; thus, it can detect the change using methods such as Ratio Test Metrics [17]. However, the two signals do not overlap in most cases, and there is no such disturbance; therefore, this method needs to wait until the disturbance occurs, which is a waste of detection time. This means that the method cannot address the condition wherein the signal's interval is large, and thus, the timeliness of this method is also limited. All the methods that fall under the baseband signal processing techniques above can be used to detect intermediate spoofing, although they all have their own limitations, mainly concerning real-time detection and detection ranges.

Multimodal detection is a well-known method used to detect multiple signals, and it is often used in the acquisition stage. An acquisition module can be divided into a capturing process (acquisition stage) and a searching process, in which the capturing process captures new signals and the searching process polls all the satellites that are being tracked. Therefore, the capturing process is very short, and if the counterfeit signal enters the receiver after the capturing process, multimodal detection is not useful. Unfortunately, multimodal detection is typically used in the capturing process, and the receiver is typically performing the capturing process. Therefore, its timeliness is also limited. However, if we can use multimodal detection during the searching process, we can solve the problem of timeliness, and the detection result would be in near real time.

In this paper, we schedule an acquisition module into a searching process and utilize multimodal detection to detect intermediate spoofing. When the acquisition module does not need to find new signals, which means that it is performing the searching process, the module monitors the signals that are being tracked by a receiver and obtains the correlation values. If there are at least two peaks above a threshold in the correlation values, we declare that there are counterfeit signals. Most of the time, the acquisition module is performing the searching process, and multimodal detection can address the condition of arbitrary signal intervals and thus ensures real-time spoofing detection. Therefore, the method provides near real-time detection and extends the detection range in terms of the signal's interval and the counterfeit signal's power. Then, we provide a performance calculation method

in terms of both theory and empirical formula and analyze the effects of primary factors. The results show that the method can detect a counterfeit signal when the counterfeit signal is close to an authentic signal in terms of signal power and when the signal's interval is small; moreover, it provides near real-time detection. In addition, the empirical formula represents further quantitative research.

The paper is organized as follows. In section 2, the signal model and the spoofing detecting method are introduced. Section 3 presents the performance analysis of the method, including evaluation standard and empirical formula. Numerical and simulation results are provided in section 4, and conclusions are drawn in section 5.

II. SIGNAL MODEL AND METHOD

A. SIGNAL MODEL

The GPS C/A code signal is modeled as Eq. (1) [5]. Here, A is the signal's amplitude, $C(n)$ is the C/A code, $D(n)$ is the navigation message, f_i is the carrier frequency, φ is the carrier phase, and $w(n)$ is noise, which is assumed to be additive white Gaussian noise (*AWGN*).

$$s'_{IF}(n) = AC(n)D(n)\cos(2\pi f_i n + \varphi) + w(n) \tag{1}$$

To spoof a GPS receiver, an intermediate spoofer generates a counterfeit signal that has the same carrier frequency but a different code phase compared with the authentic signal to be spoofed [1]. In the GPS receiver, both the counterfeit signal and the authentic signal are received. Therefore, the received signal can be modeled as Eq. (2). Here, α is the amplitude ratio of the counterfeit signal to the authentic signal, which is determined by the spoofing-to-signal ratio (*SSR*) and can be expressed as Eq. (3). Δ_c is the signal's interval between the counterfeit signal and the authentic signal and can be either positive or negative, which means that the code phase of the counterfeit signal can be either advancing or hysteretic. φ' is the carrier phase of the counterfeit signal.

$$\begin{aligned} s_{IF}(n) &= AC(n)D(n)\cos(2\pi f_i n + \varphi) + \alpha AC(n-\Delta_c) \\ &\quad D(n-\Delta_c)\cos(2\pi f_i n + \varphi') + w(n) \end{aligned} \tag{2}$$

$$\alpha = 10^{SSR/20} \tag{3}$$

During acquisition, the receiver generates a local signal $C'(n)e^{j2\pi f_i n}$ and accumulates the signal's power via coherent integration and non-coherent integration. The corresponding in-phase and quadrature correlation results are shown in Eq. (4) and Eq. (5), respectively. Then, the envelope I^2+Q^2 is formed and utilized as the detection variance to judge whether there is a counterfeit signal. The envelope is shown in Eq. (6), where $R(\tau)$ is the correlation function, which is given by Eq. (7); τ is the interval of both the local code and the received code; f_d is the Doppler shift; T is the coherent time; w_I, w_Q are the *AWGN*; and w_I, $w_Q \sim N(0, \sigma^2)$.

$$\begin{aligned} I &= \sum_{n=0}^{N-1} s'_{IF}(n+\tau)C(n)\cos(2\pi f_i n) \\ &\approx AD(n)R(\tau)sinc(f_d T)\cos(\varphi) + w_I \end{aligned} \tag{4}$$

$$\begin{aligned} Q &= \sum_{n=0}^{N-1} s'_{IF}(n+\tau)C(n)\sin(2\pi f_i n) \\ &\approx AD(n)R(\tau)sinc(f_d T)\sin(\varphi) + w_Q \end{aligned} \tag{5}$$

$$I^2 + Q^2 \approx (AR(\tau)sinc(f_d T))^2 + w_I^2 + w_Q^2; \tag{6}$$

$$R(\tau) = \begin{cases} \tau + 1, & -1 \le \tau < 0 \\ -\tau + 1, & 0 \le \tau \le 1 \\ 0, & others \end{cases} \tag{7}$$

Thus, using Eq. (2), via the same method, the in-phase branches and quadrature branches are given as Eq. (8) and Eq. (9).

$$\begin{aligned} I &\approx AD(n)R(\tau)sinc(f_d T)\cos(\varphi) + \alpha AD(n-\Delta_c) \\ &\quad R(\tau-\Delta_c)sinc(f_d T)\cos(\varphi') + w_I \end{aligned} \tag{8}$$

$$\begin{aligned} Q &\approx AD(n)R(\tau)sinc(f_d T)\sin(\varphi) + \alpha AD(n-\Delta_c) \\ &\quad R(\tau-\Delta_c)sinc(f_d T)\sin(\varphi') + w_Q \end{aligned} \tag{9}$$

For intermediate spoofing, which is shown in section 1, to guarantee the validity and safety of spoofing, the power of the counterfeit signal is only slightly higher than that of the authentic signal, and the total power of the signals should not be excessively attenuated when their interval is very small (less than 2 code phases; thus, the correlation peaks are overlapping). Otherwise, the tracking loop may become unlocked because of the lower *CNR*. Therefore, when the interval is very small, they are completely synchronous, and the carrier phase's interval is approximately 0, i.e., $\varphi' - \varphi \approx 0$ [1], [17]. Thus, the envelope $I^2 + Q^2$ is given as Eq. (10).

$$I^2 + Q^2 \approx \begin{cases} (\alpha R(\tau-\Delta_c) + R(\tau))^2 (Asinc(f_d T))^2 \\ +w_I^2 + w_Q^2, \quad |\Delta_c| < 2 \\ (\alpha^2 R(\tau-\Delta_c)^2 + R(\tau)^2 + 2\alpha R(\tau-\Delta_c) \\ R(\tau)\cos(\varphi' - \varphi))(Asinc(f_d T))^2 \\ +w_I^2 + w_Q^2, \quad others \end{cases} \tag{10}$$

By comparing Eq. (10) with Eq. (6), we can see that the *CNR*, the *SSR*, the signal's interval, and the carrier phase's interval influence the envelope. Thus, when there is a counterfeit signal, envelop distortion occurs. We can therefore use the multimodal detection method to detect whether there is a counterfeit signal.

B. PRINCIPLE OF THE METHOD

As discussed in section 2, acquisition generates local spread spectrum code, and when the code phase and frequency are both aligned with the received signal, a clear correlation peak can be obtained. Currently, there are two types of detection strategies [18]: one strategy finds the maximum, and the other strategy finds the first value larger than a threshold. Both strategies do not consider the effect of counterfeit signals; therefore, they can only find one peak. If there is a counterfeit signal as in Eq. (2), the detection variance changes as Eq. (10). We can see two correlation peaks in the envelope $I^2 + Q^2$; therefore, we can define a new strategy to detect spoofing.

To detect spoofing, the detection principle has to be changed. For conventional acquisition wherein there are no

counterfeit signals, acquisition is a binary hypothesis test problem that distinguishes noise and signal via the Neyman-Person principle [5]. However, when spoofing is involved, the acquisition changes to a ternary hypothesis test problem that distinguishes noise, a single signal and two signals. In addition, the hypothesis test problem can be described as Eq. (11).

$$\begin{cases} H0 : I^2 + Q^2 \approx w_I^2 + w_Q^2 \\ H1 : as \quad equation \quad (6) \\ H2 : as \quad equation \quad (10) \end{cases} \tag{11}$$

Based on Eq. (11), we can find that both H1 and H2 involve the authentic signal; however, H2 also involves a counterfeit signal. Therefore, detection can be divided into two steps. First, we need to distinguish between noise and signal; then, if signals can be found, we need to determine the number of signals. Thus, a threshold can be used to distinguish between noise and signal. If the detection variance is larger than a threshold, we conclude that there are signals. In addition, multimodal detection is used to distinguish a single signal and two signals; if there are at least two peaks, we conclude that there is a counterfeit signal. The method is shown in Fig. 2. When performing the searching process, the acquisition module monitors the channels being tracked and searches each code phase and frequency. Once there are at least two peaks above the threshold, we conclude that there is a counterfeit signal. The steps are as follows:

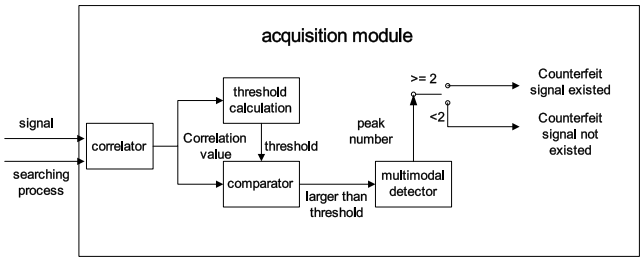

FIGURE 2. Block diagram of the method.

a) When the acquisition module is performing the searching process, the correlator collects information (code phase and Doppler frequency) from a tracking channel and re-searches the fixed frequency and all code phases. Thus, it obtains a group of correlation results, which represent the envelope in Eq. (10).

b) We can find the *CNR* and noise power from the tracking channel. If we determine the probability of false alarm (P_{fa}) of H0 to H1, we can calculate the threshold [5]. Then, we obtain the correlation values that are larger than the threshold.

c) According to the results obtained from step b), we utilize multimodal detection to detect the number of peaks, in which a peak is defined as a point that is larger than its two adjacent points. If the number of peaks is greater than or equal to 2, we conclude that there is a counterfeit signal in a channel and then alarm the receiver. Thus, the receiver can eliminate this channel and continue to operate.

III. PERFORMANCE ANALYSES

A. EVALUATION STANDARD

If the received signal contains a counterfeit signal and we can find it using the above method, we consider our detection as successful. The probability can be defined as the successful probability of anti-spoofing (*SPAS*), which is the evaluation standard. As discussed in section 2, the *CNR*, the *SSR*, the signal's interval and the carrier phase's interval influence the envelope; therefore, the *SPAS* can be expressed as a function of these factors.

We divide the quantitative evaluation into two steps: the first step is being able to detect two signals, and the second step is the performance of multimodal detection based on the signal's interval and the carrier phase's interval. The two steps are assumed to be independent. Because of the good autocorrelation characteristics of GPS C/A code [5], we assume that detecting the authentic signal and detecting the counterfeit signal are independent. Therefore, the *SPAS* can be expressed as Eq. (12), where not all factors are expressed explicitly:

$$P_d = P_d^s P_d^j f(\Delta_c) \tag{12}$$

in which P_d is the *SPAS*; P_d^s is the detection probability of the authentic signal; P_d^j is the detection probability of the counterfeit signal; and $f(\Delta_c)$ is a function reflecting the influence of multimodal detection. Thus, by calculating P_d^s, P_d^j and $f(\Delta_c)$, we can obtain the performance of the method.

B. DETECTION PROBABILITY OF SIGNAL

As discussed in section 2, the envelope $I^2 + Q^2$ is the detection variance. When the local signal and the received code are not aligned in the code phase, the envelope $I^2 + Q^2$ follows a chi-square distribution. Otherwise, it follows a non-central chi-square distribution. The corresponding probability density functions can be unified as Eq. (13) and Eq. (14), respectively [5]:

$$p_n(x, d) = \begin{cases} \frac{x^{\frac{d}{2}-1} e^{-\frac{x}{2}}}{(2^{\frac{d}{2}} \Gamma(\frac{d}{2}))}, & x \geq 0 \\ 0, & others \end{cases} \tag{13}$$

$$p_s(x, d, \lambda) = \begin{cases} e^{-\frac{x+\lambda}{2}} 0.5 (\frac{x}{\lambda})^{\frac{d}{4}-\frac{1}{2}} I_{\frac{d}{2}-1}(\sqrt{\lambda x}), & x \geq 0 \\ 0, & others \end{cases} \tag{14}$$

where d denotes the degrees of freedom, which is determined by non-coherent integration times $NA = \frac{d}{2}$; $\Gamma(\frac{d}{2})$ is the Gamma function; λ represents the non-central parameter and is equal to the *CNR* of a single signal; and $I_{\frac{d}{2}-1}(\sqrt{\lambda x})$ is a modified Bessel function.

Thus, if the P_{fa} of H0 to H1 is known, we can obtain the threshold (*TH*) using Eq. (15), and the detection probabilities are expressed as Eq. (16) and Eq. (17). Therefore, the threshold *TH* (determined by the *CNR* and P_{fa} of H0 to H1) is also

a factor that influences the assessment result

$$P_{fa} = \int_{TH}^{\infty} p_n(x, d)dx \tag{15}$$

$$P_d^s = \int_{TH}^{\infty} p_s(x, d, \lambda)dx \tag{16}$$

$$P_d^j = \int_{TH}^{\infty} p_j(x, d, \lambda)dx. \tag{17}$$

C. PERFORMANCE OF MULTIMODAL DETECTION

If there are at least two peaks above a preset threshold, we consider the spoofing detection successful. Therefore, its probability $f(\Delta_c)$ is relative to the number of points. If we decrease the code phase's search step Δ_s in the acquisition module, we can obtain more points and a greater opportunity to detect two peaks. Thus, the search step is another factor that influences the performance.

Now, we shall analyze the influence of multimodal detection. The relations between correlation values and the signal's interval are shown in Fig. 3.

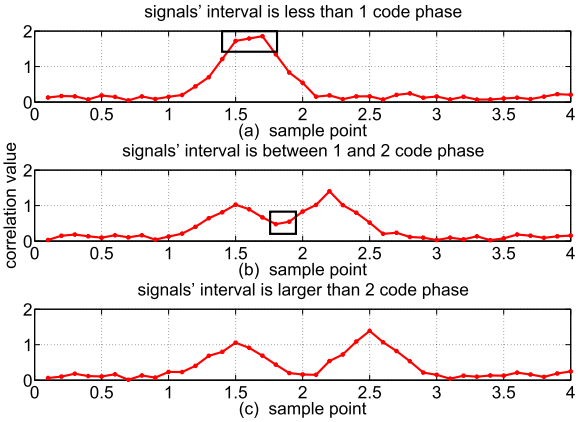

FIGURE 3. Relations between correlation values and the signal's interval.

For intermediate spoofing, the receiver usually works at a proper *CNR*. Therefore, we can assume that, when there is no overlap between the two signals, which is depicted by points outside the black box of Fig. 3, the arrangement of the sample points in $R(\tau)$ will not change. Therefore, the detection results can only be influenced by points in the black box of Fig. 3. Thus, in Fig. 3(a), $f(\Delta_c)$ can be described as the probability of having at least two peaks in the black box. In Fig. 3(b), $f(\Delta_c)$ is the sum of the probability of the following two conditions: (a) points in the black box have at least one point that is less than one, and thus, we can always find multiple peaks, and (b) all points are greater than one but there are at least two peaks. In Fig. 3(c), regardless of the value of the carrier phase's interval, we can always find two peaks. Therefore, $f(\Delta_c)$ is approximately 1.

Now, we shall analyze the calculation method of $f(\Delta_c)$ in Fig. 3(a) and Fig. 3(b), in which the signal's interval $|\Delta_c| < 2$. From section 3, we know that, if there is no counterfeit signal, the maximum envelope $I^2 + Q^2$ follows a non-central chi-square distribution with non-central parameter λ. In addition, when there is a counterfeit signal, the maximum envelope follows Eq. (10). In Fig. 3(a) and Fig. 3(b), the envelope is $(R(\tau) + \alpha R(\tau - \Delta_c))^2$ times the original from Eq. (6) and Eq. (10); therefore, the points also follow a non-central chi-square distribution with non-central parameter $(R(\tau) + \alpha R(\tau - \Delta_c))^2\lambda$. In addition, in Fig. 3(a) and Fig. 3(b), $R(\tau)+\alpha R(\tau - \Delta_c)$ can be expressed by Eq. (18) and Eq. (19), as shown at the bottom of this page, respectively.

Because of the overlap, points in the black box of Fig. 3 are not independent; however, they all follow non-central chi-square distributions, and their non-central parameter is a sample of $((\alpha - 1)\tau + \alpha + 1 - \alpha\Delta_c)^2\lambda$ based on Eq. (18) and Eq. (19). Therefore, their probability densities are unified as Eq. (20) and Eq. (21). We know that the mean is the sum of the non-central parameter and the degrees of freedom [19]; therefore, the covariance can be calculated as Eq. (22), as shown at the bottom of the next page

$$\gamma = ((\alpha - 1)\tau + \alpha + 1 - \alpha\Delta_c)^2\lambda \tag{20}$$

$$p_s'(x, d, \gamma) = e^{-\frac{x+\gamma}{2}} 0.5(\frac{x}{\gamma})^{\frac{d}{4}-\frac{1}{2}} I_{\frac{d}{2}-1}(\sqrt{\gamma x}) \tag{21}$$

where $x(m)$ is the covariance and $C(i)$ is a sample of the local signal. Based on Eq. (22), we can obtain the correlation matrices as Eq. (23) and Eq. (24), where i,j represent the element's position in the matrices and M is the number of

$$R(\tau) + \alpha R(\tau - \Delta_c) = \begin{cases} \tau + 1, & -1 \le \tau < \Delta_c - 1 \\ (\alpha + 1)\tau + \alpha + 1 - \alpha\Delta_c, & \Delta_c - 1 \le \tau < 0 \\ (\alpha - 1)\tau + \alpha + 1 - \alpha\Delta_c, & 0 \le \tau < \Delta_c \\ -(\alpha + 1)\tau + \alpha + 1 + \alpha\Delta_c, & \Delta_c \le \tau < 1 \\ \alpha(-\tau + \Delta_c + 1), & 1 \le \tau < 1 + \Delta_c \\ 0, & otherwise \end{cases} \tag{18}$$

$$R(\tau) + \alpha R(\tau - \Delta_c) = \begin{cases} \tau + 1, & -1 \le \tau < 0 \\ -\tau + 1, & 0 \le \tau < \Delta_c - 1 \\ (\alpha - 1)\tau + \alpha + 1 - \alpha\Delta_c, & \Delta_c - 1 \le \tau < 1 \\ \alpha(\tau - \Delta_c + 1), & 1 \le \tau < \Delta_c \\ \alpha(-\tau + \Delta_c + 1), & \Delta_c \le \tau < 1 + \Delta_c \\ 0, & otherwise \end{cases} \tag{19}$$

search points in a code, which is related to the reciprocal of the code phase's search step Δ_s.

$$\rho_{ij} \approx 1 - |i-j|/M \tag{23}$$

$$M = \lfloor \Delta_s / 1.023 \rfloor \tag{24}$$

Now, we have obtained the probability density of each point and their correlation matrices; however, the joint probability density function is difficult to represent explicitly (unless we assume it follows a Gaussian distribution, in which case we can use Eq. (21), Eq. (22) and Eq. (23) to derive it). Now, assume that the probability density is $p(X)$, where $X = (x_1, x_2, \cdots x_n)$ is a multidimensional variance. In Fig. 3(a), $f(\Delta_c)$ can be expressed as Eq. (25), and in Fig. 3(b), $f(\Delta_c)$ follows Eq. (26).

$$f(\Delta_c) = 1 - \Sigma_{i=1}^{n} \oint_{j<i, 0<x_j<x_{j+1}} \int_{0}^{\infty} \oint_{t>i, x_t>x_{t+1}>0} P(X) d_x \tag{25}$$

$$f(\Delta_c) = 1 - \Sigma_{i=1}^{n} \oint_{j<i, 0<x_j<x_{j+1}} \int_{1}^{\infty} \oint_{t>i, x_t>x_{t+1}>1} P(X) d_x \tag{26}$$

Eq. (25) and Eq. (26) illustrate the effect of multimodal detection but are difficult to calculate; therefore, in Eq. (27), as shown at the bottom of this page, we propose an empirical formula through massive experiments. Thus, we can calculate the *SPAS* through Eq. (12) to Eq. (17), Eq. (20), Eq. (21) and Eq. (27). In the following, we first analyze the performance with Monte Carlo simulations and then verify the validity and scope of the empirical formula.

IV. PERFORMANCE EVALUATION

Based on the analysis in section 2 and section 3, we know that the signal's interval, the *SSR*, the *CNR* of the received signal and the P_{fa} of H0 to H1 influence the probability density function of the signal, and the search step influences the number of points involved in the calculation. They are all primary factors influencing the method's performance. In addition, the carrier phase's interval is also a factor; however, under intermediate spoofing when the multimodal detection method is utilized, it produces a minimal effect. Thus, in this section, we will only focus on the primary factors.

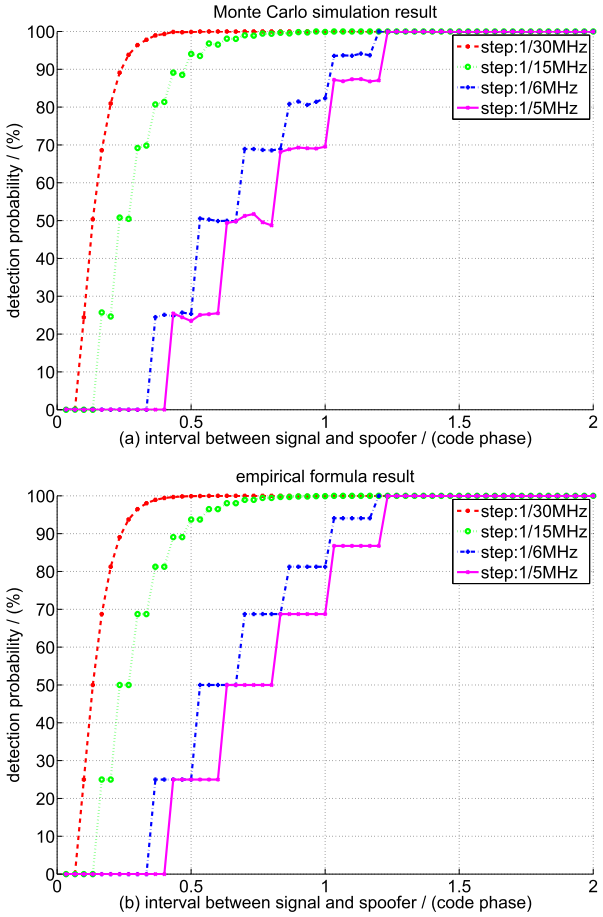

FIGURE 4. Effect of search step and signal interval. Here, the carrier-to-noise ratio is 44 dBHz, the spoofing-to-signal ratio is 0 dB, and the probability of false alarm is set to 1e-7.

The following results are obtained when the Monte Carlo simulation is run 10000. Other parameters are illustrated in the figures.

A. EFFECT OF SEARCH STEP AND SIGNAL'S INTERVAL

Fig. 4(a) presents the Monte Carlo simulation results and the effects of the search step and signal's interval, and Fig. 4(b) presents the empirical formula results.

From Fig. 4(a), we can see the following: (a) As the overlap of the two signals decreases, the influence of the two signals on each other decreases, and we can easily find

$$\begin{aligned} x(m) &= E(\overline{I^2(k) + Q^2(k) I^2(k+m) + Q^2(k+m)}) = E([2A(R(\tau) + R(t-\Delta_c))(n_I(k) + n_Q(k)) + n_I^2(k) + n_Q^2(k) - d] \\ &\quad [2A(R(\tau) + R(t-\Delta_c))(n_I(k+m) + n_Q(k+m)) + n_I^2(k+m) + n_Q^2(k+m) - d]) \\ &\approx 4A^2(2-\Delta_c)^2 E(n_I(k) n_I(k+m) + n_Q(k) n_Q(k+m)) \propto \Sigma_{i=1}^{N} x(i) w(i) \Sigma_{i=1}^{N-m} x(i+m) w(i+m) \\ &\propto \Sigma_{i=1}^{N-m} C(i) C(i+m) \propto N - m \end{aligned} \tag{22}$$

$$f(\Delta_c) \approx \begin{cases} 1 - \frac{\lceil \Delta_s \Delta_c \rceil}{2^{\lceil \Delta_s \Delta_c \rceil - 1}} e^{(\alpha-1)(0.12 \lceil \Delta_s \Delta_c \rceil^2 - 0.3 \lceil \Delta_s \Delta_c \rceil + 0.12)}, & 0 \le \Delta_c \le 1 \\ 1 - \frac{\lfloor \Delta_s (2-\Delta_c) \rfloor}{2^{\lfloor \Delta_s (2-\Delta_c) \rfloor - 1}} e^{13\alpha - 12.3} \left(\int_1^{\infty} p_s'(x, d, \gamma) d_x \right)^{\frac{\lfloor \Delta_s (2-\Delta_c) \rfloor}{2}}, & 1 < \Delta_c < 1 + \frac{1}{\Delta_s} \\ 1, & others \end{cases} \tag{27}$$

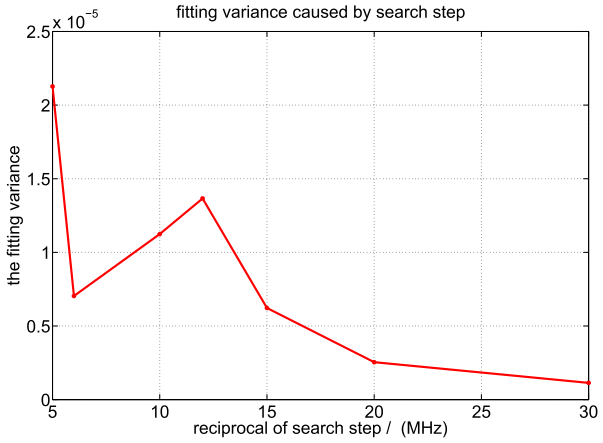

FIGURE 5. Effect of search step on fitting variance.

two or more peaks. Thus, the *SPAS* increases as the signal's interval increases. (b) The number of points in the calculation increases when the code phase's search step decreases; therefore, the randomness of the multiple points increases. Then, the detection performance improves correspondingly; therefore, the *SPAS* increases. (c) The *SPAS* is directly related to the number of points in the black box of Fig. 3, and thus, the curve in Fig. 4(a) is a ladder. When the number of points is greater than a threshold, which is less than 3, we can never find two peaks; therefore, the method is inapplicable and represents a bound of this method. (d) When the signal's interval is larger than some value between 0 and 2, we can always obtain a successful detection, and the value is relative to the search step. Let Eq. (27) equal 0, and thus, we can obtain the value. If we want to improve the *SPAS*, we need a large signal interval and small search step, where the signal interval is not controlled by the receiver, and a small search step means a large number of calculations. Moreover, regardless of the signal's interval, the method can detect spoofing. Therefore, detection can occur at any time, which is proof that the method offers real-time performance.

By comparing Fig. 4(a) and Fig. 4(b), we can see that the curves fit well. Fig. 5 is the fitting variance of the *SPAS*. It demonstrates that the empirical formula is very close to the simulation results. Moreover, we can find that, as long as the search step is less than 1/2.046 MHz, which is the Nyquist sampling frequency of the C/A code signal, the empirical formula is applicable.

B. EFFECT OF SSR AND SIGNAL INTERVAL

Fig. 6 shows the effect of the *SSR* and the signal interval. Figs. 6(a) and (b) are the Monte Carlo simulation results and the empirical formula results, respectively. From Fig. 6(a), we can find the following: (a) The non-central parameter of the points in the black box of Fig. 3 is a sample of $((\alpha-1)\tau+\alpha+1-\alpha\Delta_c)^2\lambda$, and the *SSR* represents the slope. A larger slope indicates a lower probability of peaks; therefore, the *SPAS* increases with decreasing *SSR*. (b) When the *CNR* is sufficiently large, as long as there is one point between the

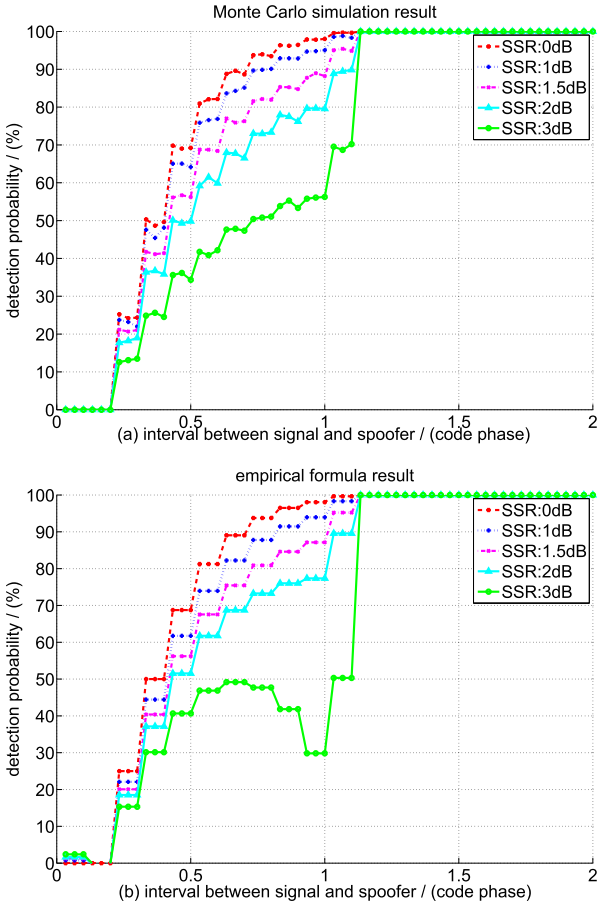

FIGURE 6. Effect of spoofing-to-signal ratio and signal interval. Here, the carrier-to-noise ratio is 44 dBHz, the search step is 1/10 MHz, and the probability of false alarm is set to 1e-7.

two correlation peaks in Fig. 3(b), we can easily find two peaks. The number of points is only relative to the search step; therefore, the *SSR* cannot influence the value more so than when the *SPAS* is approximately equal to 1. Overall, the *SSR* is not controlled by the receiver. When this value is sufficiently large and the signal's interval is sufficiently small, the multimodal method is inapplicable, and we require assistance from other methods to detect counterfeit signals.

By comparing Fig. 6(a) with Fig. 6(b), we can see that the curves do not fit very well in some cases. To evaluate the fitting effect, Fig. 7 shows the fitting variance of the *SPAS*. Fig. 7(a) shows that, if the *SSR* is less than 3 dB, we can use the empirical formula. In Fig. 6, if the *SSR* is approximately 3 dB and the signal's interval is between 0.8 and 1.2 code phases, the curve cannot be fit well. As shown in Fig. 7(b), there is a large gap in the fitting results. If the fitting error of a single point is required to be less than 2 percent, the empirical formula fits well when the *SSR* is between -2.2 dB and 2.2 dB.

C. EFFECT OF CNR AND SIGNAL INTERVAL

Fig. 8 shows the effect of the *CNR* and signal interval. Figs. 8(a) and (b) present the Monte Carlo simulation results and empirical formula results, respectively. From Fig. 8(a), we can find the following: (a) When the *CNR* is higher,

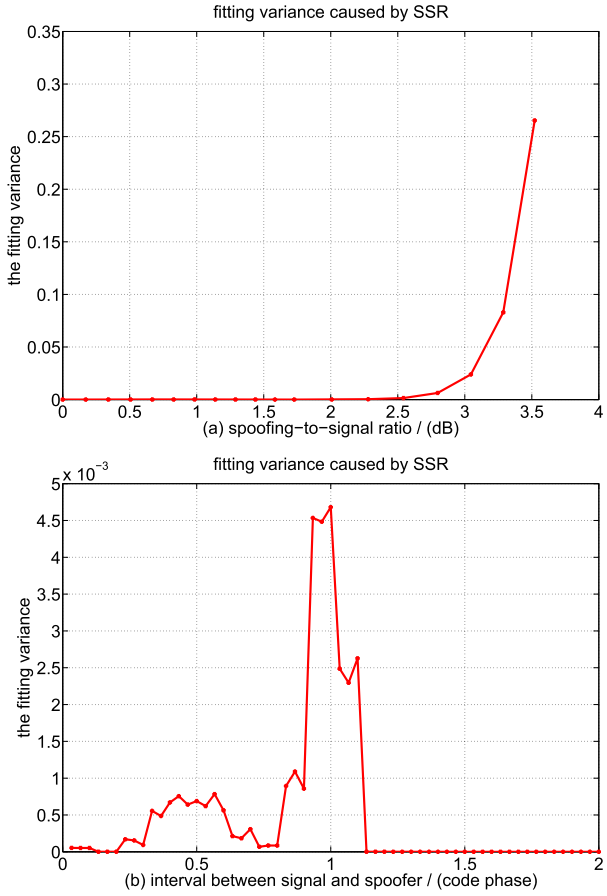

FIGURE 7. Effect of spoofing-to-signal ratio on fitting variance.

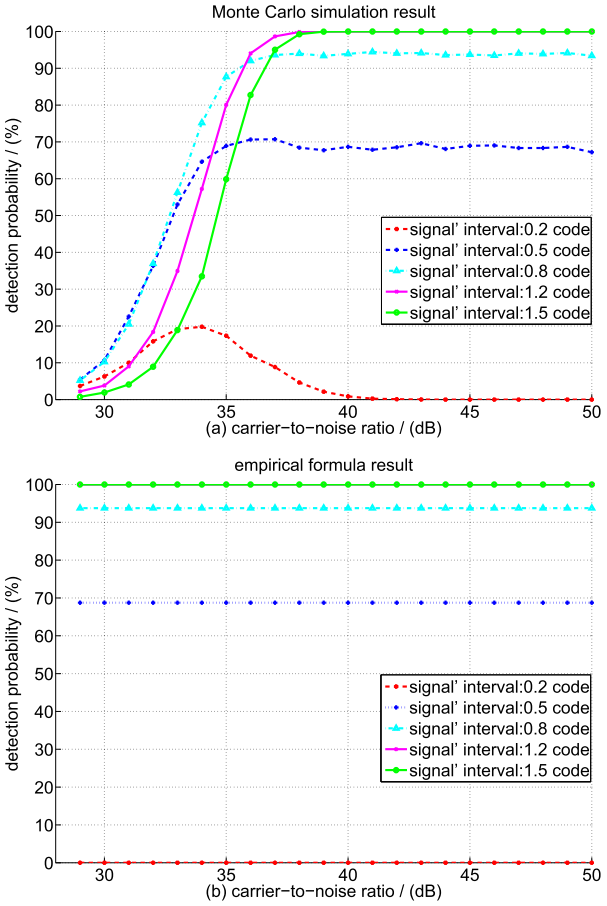

FIGURE 8. Effect of carrier-to-noise ratio and signal interval. Here, the spoofing-to-signal ratio is 0 dB, the search step is 1/10 MHz, and the probability of false alarm is set to 1e-7.

for a fixed *CNR*, the *SPAS* increases as the signal's interval increases, which is the same as above. In contrast, when it is lower, we cannot draw a conclusion for why our assumption is invalid, which means that the assumption that the points outside the black box of Fig. 3 cannot influence the detection results requires a higher *CNR*. (b) When the *CNR* is sufficiently high such that we can ignore the effects of points outside the black box of Fig. 3, the assumption is true. Thus, because our method finds two peaks and because the influence of the *CNR* on every point is the same, for a fixed signal interval, the *SPAS* is almost constant. Overall, if the *CNR* is larger than 37 dBHz, the *SPAS* cannot be improved by increasing the *CNR*.

By comparing Fig. 8(a) and Fig. 8(b), we can see that the curves cannot fit very well when the *CNR* is low. Fig. 9 shows the fitting variance of the *SPAS* and proves this conclusion. Therefore, when the *CNR* is larger than 37 dB, we can say that the empirical formula works well and that the fitting error of a single point is less than 2 percent.

D. EFFECT OF THE FALSE ALARM PROBABILITY OF H0 TO H1

Fig. 10 shows the effect of P_{fa} of H0 to H1 and the signal interval. Figs. 10(a) and (b) present the Monte Carlo simulation results and empirical formula results, respectively.

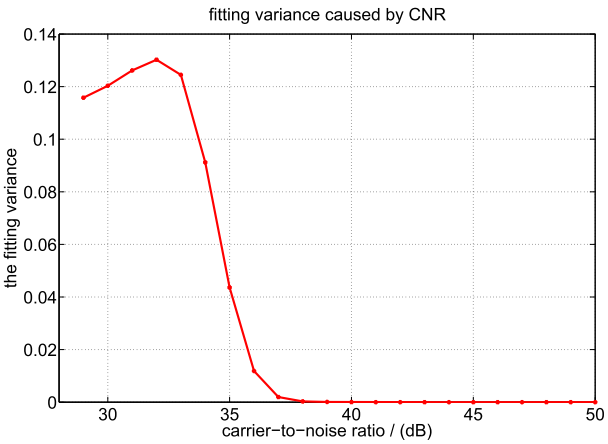

FIGURE 9. Effect of carrier-to-noise ratio on fitting variance.

From Fig. 10(a), we can find the following: (a) To achieve successfully detection, we need to find two peaks in the correlation results above a preset threshold. If the P_{fa} is not sufficiently low, which means that the threshold based on Eq. (15) is not larger than the smaller peak, the detection result will not change. Hence, for a fixed signal interval, there is a range of P_{fa} in which the *SPAS* remains unchanged. Under the simulation conditions, the range is larger

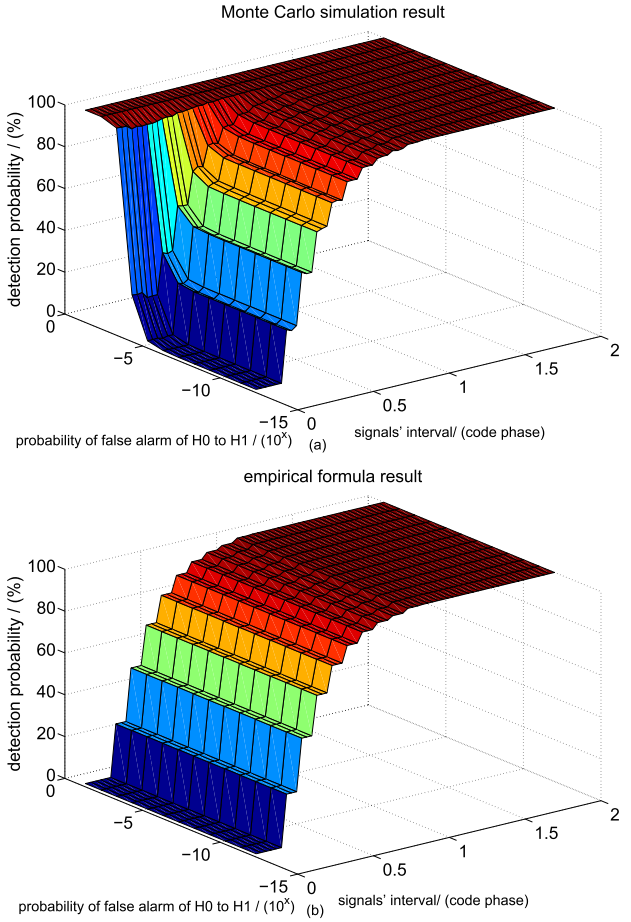

FIGURE 10. Effect of false alarm probability and signal interval. Here, the carrier-to-noise ratio is 44 dBHz, the spoofing-to-signal ratio is 0 dB, and the search step is 1/10 MHz.

than 1e-4. (b) When the P_{fa} exceeds 1e-4, the *SPAS* increases. Under this condition, the *SPAS* cannot reflect the method's performance because of the incorrect judgment. One method for decreasing the rate of incorrect judgments is to increase the detection time N. (c) When P_{fa} is lower than a given value, the threshold is larger than the smaller peak, which means that we have lost a peak. Therefore, the *SPAS* decreases, and the method is invalid. In our experiment, we do not give the value because, in practical applications, P_{fa} has a reasonable scope. Overall, if P_{fa} falls within an appropriate range, it cannot influence the *SPAS*, as discussed in the following subsection.

By comparing Fig. 10(a) and Fig. 10(b), we can see that, if the range of P_{fa} is larger than 1e-4, the curves can fit quite well. Fig. 11 shows the fitting variance of the *SPAS* and demonstrates the above. Therefore, when P_{fa} falls within this range, the empirical formula performs well. Moreover, as long as a receiver selects an appropriate P_{fa}, the empirical formula is valid.

E. SCOPE OF THE EMPIRICAL FORMULA

There are many factors that influence the anti-spoofing performance of the method. Generally, when in an appropriate range, the search step and the spoofing-to-signal ratio have a negative influence, which means that increasing the

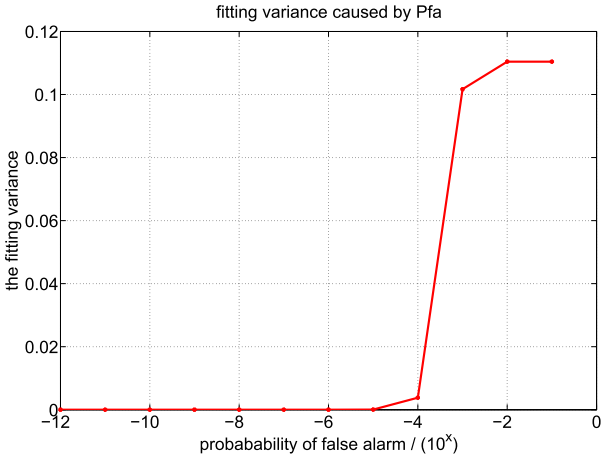

FIGURE 11. Effect of false alarm probability on fitting variance.

spoofing-to-signal ratio or search step will cause the successful probability of anti-spoofing to decrease. The signal's interval has a positive influence, which means that increasing the signal's interval will cause the probability of successful anti-spoofing to increase. The carrier-to-noise ratio and the probability of false alarm do not influence the performance of the method. In a receiver, the search step, the carrier-to-noise ratio and the probability of false alarm are controllable in a sense; therefore, we can improve the anti-spoofing performance by decreasing the search step, although this requires a large number of calculations and substantial hardware resources. To evaluate the performance easily, we can use the empirical formula under the condition that the search step is less than 1/2.046 MHz, the spoofing-to-signal ratio is from -2.2 dB to 2.2 dB, the carrier-to-noise ratio is larger than 37 dB, and the range of the probability of false alarm is larger than 1e-4. Moreover, the fitting error of a single point is less than 2 percent.

V. CONCLUSIONS

Spoofing is a serious threat to GNSS, and corresponding research is of great significance. In this paper, we utilize multimodal detection method to detect intermediate spoofing in an acquisition module during its searching process. Through the quantitative analysis, we obtain 5 primary factors influencing the successful probability of anti-spoofing, and the proposed empirical formula can describe the method's performance very well within a certain scope. Typically, the acquisition module is in the searching process, and the method can address different signal intervals; therefore, it provides real-time detection. Moreover, when a signal's interval is larger than a certain value, which is less than 2 code phases, the successful probability of anti-spoofing is almost 100 percent, which is an excellent result. The results are desirable for designing anti-spoofing receivers. In future research, we will study the method's performance under atypical conditions such as lower carrier-to-noise ratios and higher spoofing-to-signal ratios.

REFERENCES

[1] T. E. Humphreys, M. L. Psiaki, and B. W. O'hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. ION GNSS Int. Tech. Meeting Satellite Division*, vol. 55. 2008, p. 56.
[2] B. Motella *et al.*, "Performance assessment of low cost GPS receivers under civilian spoofing attacks," in *Proc. 5th ESA Workshop Satellite Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2010, pp. 1–8.
[3] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in *Proc. ION GNSS Meeting*, vol. 3, 2012, pp. 3591–3605.
[4] T. H. Kim, C. S. Sin, and S. Lee, "Analysis of effect of spoofing signal in GPS receiver," in *Proc. 12th Int. Conf. Control Autom. Syst. (ICCAS)*, Oct. 2012, pp. 2083–2087.
[5] B. Parkinson and J. Spilker, *The Global Positioning System: Theory Application*. Washington, DC, USA: AIAA, 1996.
[6] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proc. ION Int. Tech. Meeting*, 2009, pp. 124–130.
[7] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," in *Proc. ION GNSS12 Conf.*, 2012, pp. 1233–1243.
[8] K. D. Rao, M. N. S. Swamy, and E. I. Plotkin, "Anti-Spoofing filter for accurate GPS navigation," in *Proc. 13th Int. Tech. Meeting Satellite Division Inst. Navigat. (ION GPS)*, 2000, pp. 1536–1541.
[9] Y. Gao, "A new algorithm of receiver autonomous integrity monitoring (RAIM) for GPS navigation," in *Proc. 4th Int. Tech. Meeting Satellite Division Inst. Navigat. (ION GPS)*, 1991, pp. 887–896.
[10] Y. Jiang and J. Wang, "A new approach to calculate the vertical protection level in A-RAIM," *J. Navigat.*, vol. 67, no. 4, pp. 711–725, 2014.
[11] L. Yang, J. Wang, N. L. Knight, and Y. Shen, "Outlier separability analysis with a multiple alternative hypotheses test," *J. Geodesy*, vol. 87, no. 6, pp. 591–604, 2013.
[12] M. Alqurashi and J. Wang, "Performance analysis of fault detection and identification for multiple faults in GNSS and GNSS/INS integration," *J. Appl. Geodesy*, vol. 9, no. 1, pp. 35–48, 2015.
[13] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," in *Proc. 5th ESA Workshop Satellite Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2010, pp. 1–6.
[14] H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. ION GNSS*, 2005, p. 13.
[15] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/No estimates," in *Proc. 25th Int. Tech. Meeting Satellite Division Inst. Navigat. (ION GNSS)*, 2012, pp. 2875–2884.
[16] M. Fantino, A. Molino, P. Mulassano, M. Nicola, and M. Rao, "Signal quality monitoring: Correlation mask based on ratio test metrics for multipath detection," in *Proc. Int. Global Navigat. Satellite Syst. Soc. (IGNSS) Symp.*, 2009, pp. 1–3.
[17] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. Lo Presti, "Signal quality monitoring applied to spoofing detection," in *Proc. 24th Int. Tech. Meeting Satellite Division Inst. Navigat. (ION GNSS)*, 2001, pp. 1888–1896.
[18] D. Borio, L. Camoriano, and L. Lo Presti, "Impact of GPS acquisition strategy on decision probabilities," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 44, no. 3, pp. 996–1011, Jul. 2008.
[19] Wikipedia. *Noncentral Chi-Squared Distribution*, accessed on Apr. 2013. [Online]. Available: http://en.wikipedia.org/wiki/Noncentral_chi-square_distribution

JING LI was born in Beijing, China, in 1978. He received the B.Sc. and M.Sc. degrees in electrical engineering from Dalian Maritime University, China. He is currently the Doctor candidate in School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests include the fields of GNSS reliance and vulnerabilities and Maritime Search and Rescue (MSR).

JIANTONG ZHANG was born in Heibei, China, in 1977. He received the Ph.D. degree in geoinformatics from the Technical University of Munich. He is currently a Senior Researcher with the Department of Navigation, China Transportation Telecommunications and Information Center. His research interests are multi-GNSS constellation, GNSS integrity, and map-matching.

SHOUFENG CHANG was born in Henan, China, in 1981. He received the master's degree from Peking University, China. He is currently an Engineer with the Beijing Satellites Navigation Center. His research interests include software GNSS receiver and GNSS applications.

MENG ZHOU was born in Hunan, China, in 1980. She received the Ph.D. degree from the Department of Electronic Engineering, Tsinghua University, China. She is currently an Engineer with the Beijing Satellites Navigation Center. Her research interests include GNSS receiver and GNSS antispoofing.