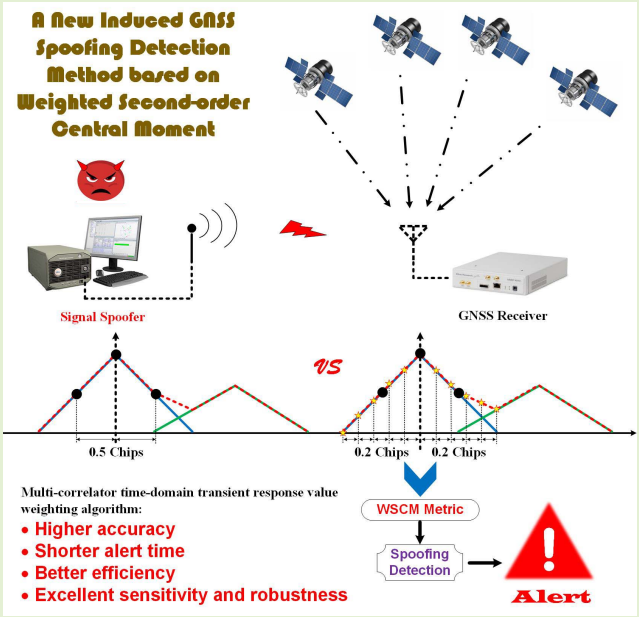
A New Induced GNSS Spoofing Detection Method Based on Weighted Second-Order Central Moment

Wenlong Zhou, Zhiwei Lv, Xu Deng, and Ye Ke

***Abstract*—Global navigation satellite system (GNSS) spoofing causes the victim receiver to deduce false positioning and timing data; this notably threatens navigational safety. Thus, anti-spoofing techniques that improve the reliability of GNSS systems, for which interference detection is critical, are essential. Based on the distortion of tracking loop correlation function symmetry of the target receiver caused by gradual adjustment of induced spoofing signals, we proposed a new induced spoofing detection method that uses the weighted second-order central moment (WSCM) difference in the time-domain transient response of multiple correlators of the left and right peaks to obtain the test statistic, theoretically proving that the test statistic follows Gaussian distribution. The Neyman-Pearson hypothesis test method is used to determine the optimal test threshold and determine whether the receiver is being spoofed. The proposed WSCM-based method for spoofing detection was compared with three conventional methods in Scenarios 4 and 7 of the Texas Spoofing Test Battery database, showing that the detection probability of the proposed method is at least 24.15% higher at a false alarm rate of 10% and is more advantageous at lower false alarm rates and the alert time is shortened by at least 30 seconds, enabling at least a 20% faster detection efficiency. The proposed method overcomes the problem of existing methods, which are associated with difficulties in capturing the subtle time-varying effects of the relative carrier phase between the spoofing and authentic signals; thus, it provides excellent detection accuracy and effectiveness, showing broad potential applicability in GNSS spoofing detection.**



***Index Terms*—GNSS spoofing detection, induced GNSS spoofing, SQM, TEXBAT, weighted second-order central moment.**

I. Introduction

GLOBAL navigation satellite system (GNSS) has widespread applications in various fields of modern society. It is indispensable for various aspects of national economic life, such as power grids, financial systems, communication systems, smart cities, and precision agriculture, as well as for military applications, such as aerospace-associated applications and precision-guided weapons [1], [2]. The importance of GNSS is self-evident; its security and reliability are also receiving widespread attention [3], [4]. Due to the low power and openness of GNSS civil signals, receivers are susceptible to radio frequency interference [5], [6]. This can be divided into unintentional and intentional interference, and the latter can be subdivided into blanketing and spoofing interference. Of these, spoofing interference is more concealed and poses a significant threat to GNSS [7], [8]. Many related periodicals have published successful cases of spoofing attacks [9]–[11], raising awareness regarding the dangers posed by spoofing.

Following the spread of programmable simulators [12] and software-defined radios [13], spoofing has become easier than ever before. Spoofing techniques are popular fields of research. Scholars such as Jafarnia, Psiaka, and Ioannides have comprehensively summarized, classified, and reported available

Manuscript received March 16, 2022; accepted April 26, 2022. Date of publication May 10, 2022; date of current version June 14, 2022. This work was supported in part by the State Key Laboratory of Geo-Information Engineering under Grant SKLGIE2020-Z-2-1 and in part by the National Science Foundation of China under Grant 42174036. The associate editor coordinating the review of this article and approving it for publication was Prof. Chao Tan. *(Corresponding author: Zhiwei Lv.)*

The authors are with the School of Geospatial Information, Information Engineering University, Zhengzhou 450001, China (e-mail: zhouwenlong597@163.com; lvzhiwei@sina.com; dx2018stv@163.com; 465316197@qq.com).

Digital Object Identifier 10.1109/JSEN.2022.3174019

spoofing techniques [14]–[16]. Spoofing can be divided into three types based on implementation difficulty: simplistic, intermediate, and sophisticated. Intermediate spoofing is more effective than simplistic spoofing and more implementable than sophisticated spoofing, which is the most important spoofing jamming mode at present. Induced spoofing is the most harmful type of intermediate spoofing. It gradually separates the lock loop of the target receiver from the authentic signal correlation peak via alterations of the power and code rate of the spoofing signal. It then locks the correlation peak of the spoofing signal, and the victim is spoofed if the target receiver stays locked [17]. The induced spoofing process typically does not alert the user. It is more feasible than sophisticated spoofing and has a higher success rate than simplistic spoofing; hence, it has more severe consequences. Due to its strong concealment and broad applications, induced spoofing has gradually become a mainstream spoofing technique. This makes it a significant target area of study in terms of anti-spoofing techniques, which may include signal detection.

As one such form of detection, signal quality monitoring (SQM) uses correlator output to identify abnormally sharp, flat, or asymmetric correlation peaks in the tracking output; it can be used to detect distortions and abnormalities in GNSS signals [14], [18]. Induced spoofing does not damage the tracking loop lock of the target receiver, Still, there is significant distortion of correlation peak symmetry caused by the interaction of the spoofing and authentic signals. In response to this feature, researchers have developed many effective spoofing detection techniques involving SQM. Specifically, using samples with complex correlation functions of "early" (E), "prompt" (P), and "late" (L) in-phase and quadrature correlator outputs, Phelts firstly introduced the Ratio and Delta metrics. The Delta metric aims to detect correlation peaks, whereas the Ratio metric explicitly detects the presence of "dead zones" (flat correlation peaks) at the peak of the correlation function [18]. He subsequently verified that this could be used to detect spoofing signals. Mubarak *et al.* then proposed the early late phase (ELP) variable to perform detection using the phase delay between the output of the E and L correlators, which has also been identified as a valuable discriminator for detecting multipath and spoofing [19], [20]. The magnitude difference metric proposed by Wesson *et al.* tracks and monitors the difference between the magnitude of the E and L correlators to detect GNSS signal distortion and multipath effects [21]. Other rational spoofing detection metrics include Pirsiavash *et al.*'s proposal to use two-dimensional time-frequency analyses in the code delay and Doppler frequency domains to enhance spoofing detection performance and reliability [22]. However, this method does cause additional computational complexity. Sun *et al.* developed a multi-metric joint detection technique using the Ratio, Delta, and ELP metrics [23], thus combining various SQM metrics into composite metrics to detect spoofing attacks; however, the actual efficacy of this technique was middling. In another study, Wesson *et al.* combined abnormal received power and correlation function distortion to construct a power-distortion detector capable of distinguishing low-power spoofing from ordinary multipath [24]. Thereafter, Gross *et al.* replaced the power-distortion detector's symmetric difference-based distortion measurement with one based on the post fit residuals of the maximum-likelihood estimate of a single-signal correlation function model, which considerably improved classification performance. This improved technique was named the power-distortion maximum likelihood (PD-ML) detector [25]. Compared with a conventional power-distortion detector, the PD-ML detector showed enhanced classification accuracy, but at the expense of additional computational complexity. Subsequently, Benachenhou *et al.* investigated an SQM method based on the fusion of metrics using an OR rule to detect the presence of spoofers, which yielded closed forms of the optimal thresholds and probability of detection [26].

At the core of the above SQM spoofing detection techniques is the comparison of the measured values of E, P, and L in-phase or quadrature correlators with a set threshold and the effective monitoring of the symmetry changes of correlation peaks caused by spoofing signals [27]. However, with the continuous improvement of the spoofing jamming mode, two problems associated with the SQM method are increasingly being exposed: Firstly, in the case of induced spoofing with highly accurate control, slow spoofing process, and good concealment, using the output results of just three correlators to identify distortion in correlation peak symmetry does not provide the required classification accuracy. Khan *et al.* explained this point and proposed the more sensitive approach of using multiple correlators to measure shape distortion [28]; Secondly, however, the precise combination of multiple correlators requires further study. At present, the method of using multi-correlators to improve the detection accuracy simply involves increasing the number of correlators, without the reasonable quantitative combination of a large number of correlator output values, resulting in an insignificant improvement in the detection performance. Therefore, by adopting a multi-correlator design and constructing a more scientific, reasonable, and accurate test statistic, the symmetry distortion of the correlation peak can be quantified more accurately, and the threats and challenges associated with the developing spoofing interference can be more effectively prepared for.

Aiming at the above problems, this study proposes a weighted second-order central moment (WSCM) method to detect induced spoofing that targets the gradual dynamic adjustments process in the distortion of the correlation peak symmetry caused by the interactions among spoofing and authentic signals in the tracking phase. Specifically, firstly, by extending the second-order central moment (SCM) [29] of navigation signal waveforms, the weighting criterion of the time-domain transient response value of multi-correlators is established, and the WSCM test statistic, which can accurately quantify the symmetry of correlation peaks, is constructed. Secondly, the theoretical analyses prove that the difference between the WSCM on both sides of the correlation peak obeys the Gaussian distribution, and the Neyman-Pearson(NP) hypothesis test method is used to determine the optimal test threshold and determine whether the receiver is being spoofed [30]. Finally, the influence of adding multiple correlators is discussed, and the selection range of the correlator logarithm is determined by comprehensively measuring the spoofing detection performance, computational complexity, and other factors. Based on the GNSS-SDR software receiver platform [31], three conventional Ratio metric, Delta metric, ELP metric and WSCM metric are tested and evaluated in Scenario 4 and Scenario 7 of the Texas Spoofing Test

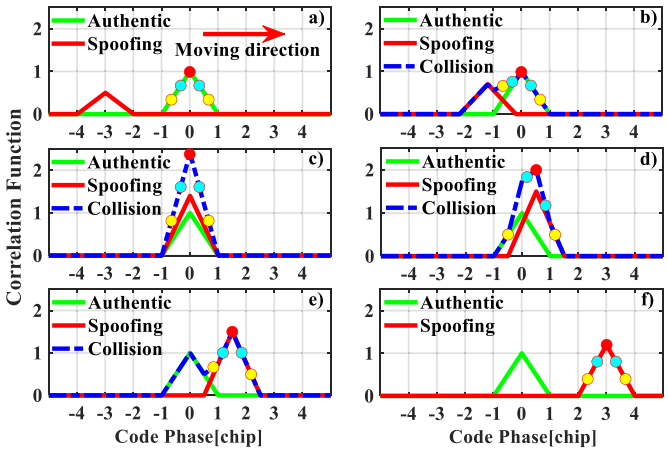


Fig. 1. Correlation peak changes in a spoofing process.

Battery (TEXBAT) dataset [32], [33]. The results show that the algorithm developed for the proposed method dramatically improves alarm speed and reliability, which can primarily be explained as follows: First, it provides rapid detection response speed; spoofing attacks are more rapidly detected. Second, it offers effective detection, with a higher detection probability (P_d) at the same false alarm rate; moreover, it is more advantageous at lower false alarm rates. Third, it is more sensitive to slight deviations in spoofing signals and authentic signals frequency lock, making it better at dealing with higher-level spoofing modes. However, the WSCM-based method achieves this improved performance at the expense of additional computational complexity, which is caused by the addition of additional correlators. Although the performance of the new algorithm is greatly improved at the expense of a part of the computational complexity, it is still of great application value for researching receivers equipped with spoofing detection modules and dealing with intermediate and sophisticated spoofing interference.

II. Induced Spoofing Attack Pattern and Signal Model in the Tracking Phase

A. Induced Spoofing Attack Pattern

Induced spoofing using code phase and power adjustments is subtle and does not unlock the tracking loop of the target receiver. Fig. 1 shows the process of tracking spoofing signals tracking and separating the correlation peak in a receiver.

1) Before the attack, as shown in Fig. 1a, the spoofer detects the antenna of the target receiver to estimate its position and speed and then estimates the satellite navigation signal of the target receiver antenna. It then generates spoofing signals with a lower power at the same frequency as that of the authentic signals but that initially lag it by two chips in the code phase; however, gradually, the spoofer approaches the authentic signals by adjusting the code rate.
2) During the attack, as shown in Fig. 1b, the spoofing signals gradually synchronize with the code phase of the authentic signals. At the same time, the signal power is gradually increased. However, it is still lower than the power of the authentic signals until the spoofing signal reaches the antenna phase center of the target receiver and are aligned with the code phase of the authentic signals (within 0.5 chips), as shown in Fig. 1c. This step is the signal synchronization process. Subsequently, as shown in Figs. 1d and 1e, the power and code rate of the spoofing signals are increased; a higher level of power is used to lift off the authentic signals and the target receiver tracking loop and track the spoofing signals. This step is the signal lift-off process.
3) After the attack, as shown in Fig. 1f, the spoofing signals continue to adjust the code rate to pull away from the authentic signals' correlation peaks until they are approximately two chips ahead. Next, the power is gradually reduced to the normal level, and the spoofer takes complete control of the target receiver.

It can be seen that spoofing signals cause correlation peak distortion in the process of separating the correlation peaks of the authentic signals correlation peak; therefore, spoofing detection can be performed based on correlation peak symmetry.

B. Signal Model in the Tracking Phase

The receiver converts the radio frequency (RF) signals received by a single antenna into the digital intermediate frequency (IF) signals through the front end of the RF. The mixed GNSS digital IF signals received in the tracking phase can be modeled as combinations of digital signals corresponding to different pseudorandom noise (PRN) codes, which can be divided into three parts: the authentic signal, spoofing signal, and noise [34], expressed as

$$\begin{aligned} r(nT_s) = &\sum_{m\in J^a} \sqrt{p_m^a} D_m^a(nT_s-\tau_m^a) c_m^a(nT_s-\tau_m^a) e^{j\phi_m^a + j2\pi f_m^a nT_s} \\ &+ \sum_{q\in J^s} \sqrt{p_q^s} D_q^s(nT_s-\tau_q^s) c_q^s(nT_s-\tau_q^s) e^{j\phi_q^s + j2\pi f_q^s nT_s} \\ &+ \eta(nT_s) \end{aligned} \tag{1}$$

where p, τ, ϕ, and f are the power, code delay, carrier phase, and carrier Doppler frequency, respectively; T_s is the sampling interval; c is the corresponding PRN code sequence at time nT_s; D is the navigation data bits; and $\eta(nT_s)$ is the additive white Gaussian noise with a zero average and variance of σ^2. The subscripts m and q correspond to the PRN signals of the authentic m and spoofing q satellites, respectively; J_a and J_s are the real and spoofing signal sets, respectively; and the superscripts a and s indicate whether the signal being received is an authentic or spoofing signal, respectively.

During the despreading process of the tracking phase receiver, the GNSS receiver correlates the received signal and the local code copy. It then performs low-pass filtering. The correlator output $u_l[k]$ of the l-th signal is expressed as follows:

$$u_l[k] = r(kNT_s) c_l(nT_s - \tilde{\tau}_l^L) e^{-j2\pi \tilde{f}_l^L nT_s} \tag{2}$$

where N is the coherent integration interval, k is the index of coherent integrations, $\tilde{\tau}_l^L$ and $\tilde{f}_l^L$ are the estimated code delay and Doppler frequency, respectively.

The non-coherent tracking receiver associates the received signal with a locally generated copy ($\tilde{\tau}_l^L$ and $\tilde{f}_l^L$) whose Doppler and code delay are close to the authentic signal. When it is in a stable tracking state, the local carrier frequency and code delay of the local code may be assumed to be almost the same as those of the authentic signal

(i.e.,$\Delta f_l^{a,l} \approx 0, \tau_l^a = \tilde{\tau}_l^L$). Since the coherent integration time is usually 1 ms, which is much shorter than the data bit length of D (20 ms), the influence of D on the correlation can be excluded [35]. Therefore, the correlator output can be approximately expressed as follows:

$$\begin{aligned} u_l[k] \simeq & \sqrt{p_l^a} R(\Delta\tau_l^{a,L}) \frac{\sin(\Delta f_l^{a,L} N T_s)}{N \sin(\Delta f_l^{a,L} T_s)} \\ & \times e^{j\pi \Delta f_l^{a,L}[(2k-1)N-1]T_s + j\Delta\phi_{l,0}^{a,L}} \\ & + \sqrt{p_l^s} R(\Delta\tau_l^{s,L}) \frac{\sin(\Delta f_l^{s,L} N T_s)}{N \sin(\Delta f_l^{s,L} T_s)} \\ & \times e^{j\pi \Delta f_l^{s,L}[(2k-1)N-1]T_s + j\Delta\phi_{l,0}^{s,L}} \\ & + \bar{\eta}[kNT_s] \end{aligned} \tag{3}$$

where $\Delta\tau_l^{a,L}$, $\Delta f_l^{a,L}$, and $\Delta\phi_{l,0}^{a,l}$ are the code phase difference, carrier frequency difference, and initial carrier phase difference, respectively, between the l-th authentic signal and local signal; $\Delta\tau_l^{s,L}$, $\Delta f_l^{s,L}$, and $\Delta\phi_{l,0}^{s,l}$ are the code phase difference, carrier frequency difference, and initial carrier phase difference, respectively, between the l-th spoofing signal and local signal; $R(\cdot)$ is the correlation between authentic or spoofing signals and the local signal with the same PRN but different code phase; and $\bar{\eta}[kNT_s]$ is the low-pass filter additive Gaussian noise component with variance σ^2output by the l-th correlator branch, which consists of in-phase (I) and quadrature (Q) noise and residual cross-correlation terms approximated by a zero-mean Gaussian distribution [34].

For the GPS L1 C/A signal, after coherent integration, the normalized cross-correlation function of the local signal and authentic signal ranging code can be expressed as follows:

$$R_\tau(\Delta\tau_l^{a,L}) = \begin{cases} 1 - \left|\dfrac{\Delta\tau_l^{a,L}}{T_c}\right|, & \left|\Delta\tau_l^{a,L}\right| \le T_c \\ 0, & \left|\Delta\tau_l^{a,L}\right| > T_c \end{cases} \tag{4}$$

where T_C denotes the chip duration. Theoretically, when the code phase difference between the spoofing signals and the authentic signals is greater than two chips, the correlation peaks of the two ranging codes will not overlap, the spoofing signals will not affect the authentic signals, and the output of the code domain correlator (assuming the frequency offset $\Delta f_l^{a,L}$ is constant) is a trigonometric function of width $2T_c$ and symmetry with a code offset of zero. Assuming that the spoofing signals initially lag the authentic signals by two chips in the code phase, after coherent integration, the normalized cross-correlation function of the spoofing signals and the authentic signals ranging code can be expressed as follows:

$$R_\tau(\Delta\tau_l^{a,s}) = \begin{cases} 1 - \left|\dfrac{\Delta\tau_l^{a,s} - (2 - \Delta C_l^{a,s} t)}{T_c}\right|, \\ \qquad \left|\Delta\tau_l^{a,s} - (2 - \Delta C_l^{a,s} t)\right| \le T_c \\ 0, \quad \left|\Delta\tau_l^{a,s} - (2 - \Delta C_l^{a,s} t)\right| > T_c \end{cases} \tag{5}$$

where $\Delta C_l^{a,s}$ is the code rate difference between the spoofing and authentic signals. For simplicity, it is assumed that the Doppler frequency of the spoofing signals is the same as that of the authentic signals, which is called a "frequency lock" in previous literature [36]. At this point, the carrier phase offset is approximately zero or a constant. Next, the I and Q components output by the correlator can be modeled as follows:

$$\begin{cases} I_l[k] &= \sqrt{p_l^a} R(\Delta\tau_l^{a,L}) \cos(\Delta\phi_l^{a,L}) \\ & \quad + \sqrt{p_l^s} R(\Delta\tau_l^{a,s}) \cos(\Delta\phi_l^{a,s}) + \eta_I[kNT_s] \\ Q_l[k] &= \sqrt{p_l^a} R(\Delta\tau_l^{a,L}) \sin(\Delta\phi_l^{a,L}) \\ & \quad + \sqrt{p_l^s} R(\Delta\tau_l^{a,s}) \sin(\Delta\phi_l^{a,s}) + \eta_Q[kNT_s] \end{cases} \tag{6}$$

where $\Delta\tau_l^{a,s}$ and $\Delta\phi_l^{a,s}$ are the code and carrier phase differences, respectively, between the authentic signal and spoofing signal. $\eta_I[kNT_s]$ and $\eta_Q[kNT_s]$ are the Gaussian white noise of the I and Q correlation components, respectively; they are uncorrelated. When a spoofing signal does not exist, the Doppler frequency shift error is ignored. In theory, I_l and Q_l follow the Gaussian distribution [23,36], which can be expressed as follows:

$$\begin{cases} \mu_I &= \sqrt{p_l^a} R(dT_c) \cos(\Delta\phi_l^{a,L}), \\ \mu_Q &= \sqrt{p_l^a} R(dT_c) \cos(\Delta\phi_l^{a,L}) \\ \sigma_I^2 &= \sigma_Q^2 = \sigma_0^2 = \dfrac{N_0}{2T_s} = \dfrac{1}{2T_s(C/N_0)}, \\ \sigma_{IQ} &= 0, \Delta\tau_l^{a,L} = dT_c \end{cases} \tag{7}$$

where μ_I and σ_I^2 and μ_Q, and σ_Q^2 are the mean values and variances, respectively, of the I and Q correlator outputs, respectively. It is assumed that the covariance σ_{IQ} of the I and Q correlators is zero. σ_0^2 is the base variance of the post-correlation noise; is the noise power spectral density; and C/N_0 is the carrier to noise ratio of the received signal. It can be seen from equations (6) and (7) that when the receiver works in an incoherent mode and the spoofing signal implements induced spoofing on the tracking loop, the impact on the I and Q branches should be considered.

III. Methodology

A. Review of Conventional SQM Metrics

This study primarily considers the Ratio, Delta, and ELP metrics, which are defined as follows:

- Ratio metric:

$$R_d[k] = \frac{I_{E,d}[k] + I_{L,d}[k]}{2I_P[k]} \tag{8}$$

- Delta metric:

$$\Delta_d[k] = \frac{I_{E,d}[k] - I_{L,d}[k]}{2I_P[k]} \tag{9}$$

- ELP metric:

$$ELP_d[k] = \tan^{-1}\left(\frac{Q_{E,d}[k]}{I_{E,d}[k]}\right) - \tan^{-1}\left(\frac{Q_{L,d}[k]}{I_{L,d}[k]}\right) \tag{10}$$

where $I[k]$ and$Q[k]$ represent the I and Q correlation components, respectively, at discrete time instant k; d is the

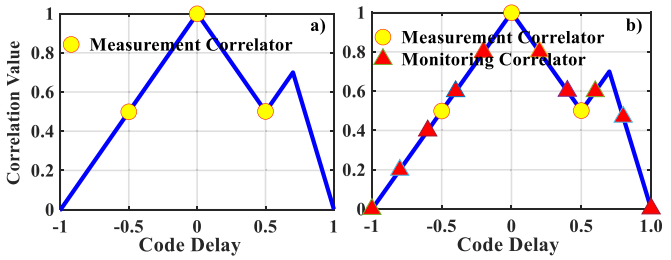


Fig. 2. Measurements on a correlation function. (a) and (b) illustrate the positions of the conventional correlator and the multi-correlator in this study on the correlation function.

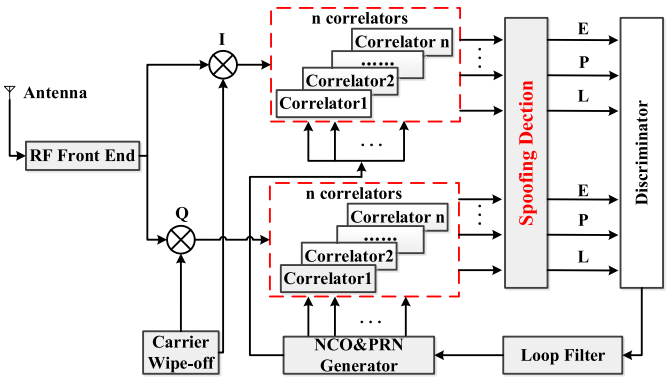


Fig. 3. Block diagram for multi-correlator receiver DLL implementation.

correlator interval; the unit of measurement is one chip; and the space between the early and late correlators and the prompt correlator is 0.5 chips.

The above SQM anti-spoofing detection indicators use the E, L, and P correlator output values to evaluate the correlation peak symmetry; they are cheap and not too complex. However, due to the small number of correlators, they are susceptible to system noise, and also cannot fully quantify the correlation function symmetry, resulting in a lower detection rate under a given false alarm rate. Thus, to an extent, performing spoofing detection using only a set of correlators or detection standards is inaccurate. Given these problems, multi-correlator techniques are more promising and have significant advantages. Using multiple correlator strategies, more detailed data on correlator symmetry can be obtained; this can improve the accuracy of spoofing detection.

B. WSCM Detection Method

Multi-correlator techniques can better obtain the shape of the correlation curve, which helps establish a metric for detecting spoofing. Existing multi-correlator receivers do not rationally adjust correlator spacing measurements or assign weights to available correlator measurement values; because this is very unfavorable with regard to the spoofing detection performance, the development of spoofing detection technologies has gradually encountered a bottleneck that is difficult to circumvent. However, the WSCM method proposed herein should be able to further optimize the spacing and weighting of correlator measurements.

Take each channel set to five pairs of correlators as an example, at chips spacings from the prompt correlator of ±0.2, ±0.4, ±0.6, ±0.8, and ±1.0; Fig. 2 shows the positions of the correlators in the tracking loop on a correlation function when a conventional receiver and a multi-correlator receiver are subjected to spoofing interference.

As shown in Fig. 2a, when spoofing interference is present, conventional receivers are not sensitive to the distortion of correlation peak symmetry due to them having fewer correlators. In contrast, the multi-correlator receiver, as shown in Fig. 2b, has more narrow-band and wide-band correlator pairs; thus, it can respond more completely and quickly to symmetry distortion. Fig. 3 shows the design of the multi-correlator receiver delay-locked loop (DLL).

The shape of the correlation peak curve can directly reflect the influence of signal distortion, multipath effects, band-limit distortion, and satellite navigation signal interference [29]. Based on the characteristics of the SCM of the waveform in the satellite navigation signal, the changes of the correlation peak are analyzed. Assuming that the correlation peak function in a period after normalization is $y = f(x)$, the x-axis sampling point of the correlation peak is x_i, the unit is one chip, and the vertical amplitude of the correlation peak is y_i. For a normalized correlation curve in an ideal state, the maximum value of y_i is 1, and the horizontal ordinate of the highest point of the correlation peak is $x_0 = 0$; thus, the calculation formula for the SCM is

$$Z = \sum_{i=1}^{N} \left| (x_i - x_0) y_i^2 \right| \tag{11}$$

If the number of incoherent integrations is N_{nc}, the value of the detection measurement $V_{d_i}^2$ is

$$V_{d_i}^2 = \frac{1}{N_{nc}} \sum_{n=1}^{N_{nc}} (I_{d_i}^2 + Q_{d_i}^2) \tag{12}$$

where d_i represents the chips spacing between correlators; thus, the SCM metric is

$$\begin{aligned} \text{SCM} &= \sum_{i=1}^{n} \left| (d_i - d_0) V_{d_i}^2 \right| \\ &= d_1 \cdot (I_{d_1}^2 + Q_{d_1}^2) + d_2 \cdot (I_{d_2}^2 + Q_{d_2}^2) \\ &\quad + \ldots + d_n \cdot (I_{d_n}^2 + Q_{d_n}^2) \end{aligned} \tag{13}$$

where $d_0 = 0$ denotes position of the highest point of the correlation peak.

To set the threshold under a pre-defined false alarm rate, it is necessary to fully understand the statistical characteristics of the SCM metric. Note that SCM measurement is a combination of different correlator output values, and the statistical characteristics are extremely complex. To facilitate our analysis, this section first analyzes the SCM metric characteristics under circumstances without spoofing attacks.

We know from equation (7) that $I_{d_i} \sim N(\mu_{I_{d_i}}, \sigma_0^2 \cdot 1)$ and $Q_{d_i} \sim N(\mu_{Q_{d_i}}, \sigma_0^2 \cdot 1)$, and the covariance of the I and Q branch correlator, σ_{IQ}, is zero. Let $x_i = I_{d_i}, x_i' = Q_{d_i}$,

$\mu_i = \mu_{I_{d_i}}$, and $\mu'_i = \mu_{Q_{d_i}}$, i.e.,

$$\boldsymbol{X} = \begin{pmatrix} x_1 \\ x'_1 \\ \cdots \\ x_1 \\ x'_1 \\ \cdots \\ x_n \\ x'_n \end{pmatrix}_{2n\times 1}, \quad \boldsymbol{\mu} = \begin{pmatrix} \mu_1 \\ \mu'_1 \\ \cdots \\ \mu_2 \\ \mu'_2 \\ \cdots \\ \mu_n \\ \mu'_n \end{pmatrix}_{2n\times 1},$$

$$\boldsymbol{V}_0 = \sigma_0^2 \cdot \begin{pmatrix} 1 & 0 & . & . & 0 \\ 0 & \ldots & 0 & . & . \\ . & 0 & 1 & 0 & . \\ . & . & 0 & \ldots & 0 \\ 0 & . & . & 0 & 1 \end{pmatrix}_{2n\times 2n} = \sigma_0^2 \boldsymbol{I}_{2n\times 2n} \tag{14}$$

where $\boldsymbol{V}_0$ is the unit covariance matrix; therefore, $\boldsymbol{X} \sim N_{2n}(\boldsymbol{\mu}, \boldsymbol{V}_0)$, $\mu \neq 0$ and $\sigma_0^2 \neq 0$. Let $\boldsymbol{Y} = \boldsymbol{AX} + \mathbf{b}$, where b is a constant matrix and the coefficient matrix A is an invertible square matrix of order $2n$, which is expressed as

$$\mathbf{A} = \begin{pmatrix} \sqrt{d_1} & 0 & . & . & . & . & 0 & 0 \\ 0 & \sqrt{d_1} & . & . & . & . & 0 & 0 \\ 0 & 0 & \cdots & . & . & . & . & . \\ . & . & . & \sqrt{d_k} & . & . & . & . \\ . & . & . & . & \sqrt{d_k} & . & . & . \\ . & . & . & . & . & \cdots & 0 & 0 \\ 0 & 0 & . & . & . & 0 & \sqrt{d_n} & 0 \\ 0 & 0 & . & . & . & 0 & 0 & \sqrt{d_n} \end{pmatrix}_{2n\times 2n} \tag{15}$$

The covariance matrix V is expressed as

$$\mathbf{V} = \sigma_0^2 \cdot \begin{pmatrix} d_1 & 0 & . & . & . & . & 0 & 0 \\ 0 & d_1 & . & . & . & . & 0 & 0 \\ 0 & 0 & \cdots & . & . & . & . & . \\ . & . & . & d_k & . & . & . & . \\ . & . & . & . & d_k & . & . & . \\ . & . & . & . & . & \cdots & 0 & 0 \\ 0 & 0 & . & . & . & 0 & d_n & 0 \\ 0 & 0 & . & . & . & 0 & 0 & d_n \end{pmatrix}_{2n\times 2n} \tag{16}$$

The quadratic form after linear transformation is $\boldsymbol{Y}^T(\boldsymbol{AVA}^T)^{-1}\boldsymbol{Y} \sim \chi^2(2n, \delta)$, where the noncentral parameter $\delta = (\boldsymbol{A\mu} + \mathrm{b})^{\mathrm{T}}(\boldsymbol{AVA}^{\mathrm{T}})^{-1}(\boldsymbol{A\mu} + \mathrm{b})$. For detailed proof, please see Appendix A.

Taking the constant vector $\boldsymbol{b} = \mathbf{0}$, the expression of the SCM of the multi-correlator is

$$\begin{aligned} SCM &= [\boldsymbol{Y}^T(\boldsymbol{AVA}^T)^{-1}\boldsymbol{Y}]_{b=0} \\ &= (\boldsymbol{AX})^T(\boldsymbol{A}^T)^{-1}\boldsymbol{V}^{-1}\boldsymbol{A}^{-1}\boldsymbol{AX} \\ &= \boldsymbol{X}^T\boldsymbol{A}^T(\boldsymbol{A}^T)^{-1}\boldsymbol{V}^{-1}\boldsymbol{A}^{-1}\boldsymbol{AX} \\ &= \boldsymbol{X}^T\boldsymbol{V}^{-1}\boldsymbol{X} \\ &= \frac{1}{\sigma_0^2}[\frac{1}{d_1}(x_1^2 + x_1'^2) + \frac{1}{d_2}(x_2^2 + x_2'^2) + \ldots + \frac{1}{d_n}(x_n^2 \\ &\quad + x_n'^2)] \end{aligned} \tag{17}$$

The expression $x_i^2 + x_i'^2$ represents the sum of the squares of the I and Q branch outputs with correlator d_i, and the coefficient is expressed as $\beta_i = 1/(\sigma_0^2 \cdot d_i), i = 1, 2 \ldots n$.

The above equations represent the mathematical model of the multi-correlator SCM, but it is evident that only increasing the number of correlators cannot markedly improve the spoofing detection performance. It is necessary to further optimize the weight of the output value of the multi-correlator in the SCM.

The following section focuses on introducing the mathematical model of the WSCM. To construct a more scientific test statistic indicator, this study weights the output value of the multi-correlator, and the weighting coefficient satisfies

$$\begin{cases} \alpha_1 + \alpha_2 + \ldots + \alpha_n = 1, \\ \alpha_i = \dfrac{\beta_i}{\sum\limits_{k=1}^{n} \beta_k}, i = 1, 2 \ldots n \end{cases} \tag{18}$$

Based on equations (17) and (18), this study proposes a WSCM spoofing detection indicator, which is expressed as

$$\begin{aligned} WSCM &= \alpha_1 \cdot (x_1^2 + x_1'^2) + \alpha_2 \cdot (x_2^2 + x_2'^2) + \ldots + \alpha_n \cdot (x_n^2 \\ &\quad + x_n'^2) \\ &= \sum_{i=1}^{n} \alpha_i \cdot (x_i^2 + x_i'^2) \end{aligned} \tag{19}$$

We can see that for $WSCM \sim \chi(2n, \delta)$, its noncentral parameter δ satisfies

$$\begin{aligned} \delta &= [(\boldsymbol{A\mu} + \boldsymbol{b})^T(\boldsymbol{AVA}^T)^{-1}(\boldsymbol{A\mu} + \boldsymbol{b})]_{\boldsymbol{b}=\mathbf{0}} \\ &= (\boldsymbol{A\mu})^T(\boldsymbol{A}^T)^{-1}\boldsymbol{V}^{-1}\boldsymbol{A}^{-1}\boldsymbol{A\mu} \\ &= \boldsymbol{\mu}^T\boldsymbol{A}^T(\boldsymbol{A}^T)^{-1}\boldsymbol{V}^{-1}\boldsymbol{A}^{-1}\boldsymbol{A\mu} \\ &= \boldsymbol{\mu}^T\boldsymbol{V}^{-1}\boldsymbol{\mu} \\ &= \frac{1}{\sigma_0^2}[\frac{1}{d_1}(\mu_1^2 + \mu_1'^2) + \frac{1}{d_2}(\mu_2^2 + \mu_2'^2) + \ldots + \frac{1}{d_n}(\mu_n^2 + \mu_n'^2)] \\ &= \alpha_1 \cdot (\mu_1^2 + \mu_1'^2) + \alpha_2 \cdot (\mu_2^2 + \mu_2'^2) + \ldots + \alpha_n \cdot (\mu_n^2 + \mu_n'^2) \\ &= \sum_{i=1}^{n} \alpha_i \cdot (\mu_i^2 + \mu_i'^2) \end{aligned} \tag{20}$$

Fig. 4 shows the time-domain transient response and statistical analysis results for the WSCM method on both sides of the receiver correlation peaks in the absence of spoofing signals.

Fig. 4 shows that when there are no spoofing signals, the WSCM output of the left and right peaks of the correlation function approximately follow the noncentral chi-square distribution, and the probability density functions (PDFs) of the multi-correlator WSCM with the symmetrical distribution of left and right peaks are roughly the same. This is consistent with the above theoretical proof and demonstrates the rationality and accuracy of the theoretical analysis.

To better measure the correlation peak symmetry, the WSCM of the left peak ($\mathrm{WSCM_E}$) and the WSCM of the right peak ($\mathrm{WSCM_L}$) of the receiver correlation function need to be used as the difference, which is denoted by $\mathrm{WSCM_{E-L}}$. It can be seen from the above proof that when the multiple correlators are symmetrically distributed in the correlation function,$\mathrm{WSCM_E}$ and $\mathrm{WSCM_L}$ follow $\chi(2n, \delta)$. The statistical characteristics of$\mathrm{WSCM_{E-L}}$ need to be defined further.

When $\mathrm{WSCM_E}$ or $\mathrm{WSCM_L}$ follow the noncentral chi-square distribution with 2n degrees of freedom and the noncentral parameter δ, its characteristic function [37] is

$$\varphi_{WSCM}(t) = (1 - 2it)^{-n} e^{\frac{it\delta}{1-2it}} \tag{21}$$

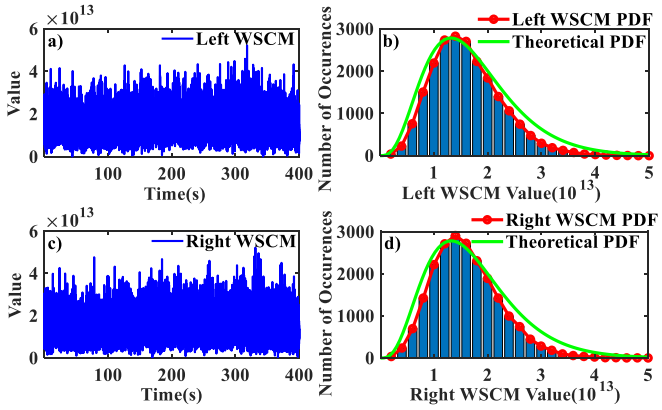


Fig. 4. (a) and (c) represent the time-domain transient response of the left and right WSCM in the non-spoofing scenario, respectively. (b) and (d) represent the measured statistical PDF and theoretical PDF of the left and right WSCM, respectively.

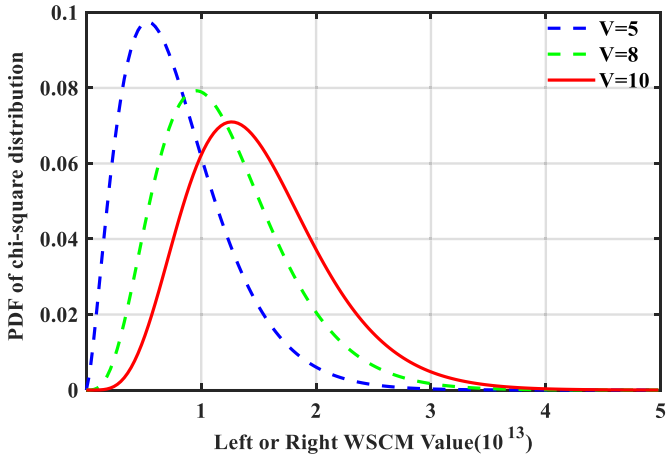


Fig. 5. Chi-square distribution of WSCM under different degrees of freedom.

where i is an imaginary unit and t is a real number. For this function,$\mathrm{WSCM_E}$ and $\mathrm{WSCM_L}$ are independent of each other; thus, the characteristic function of$\mathrm{WSCM_{E-L}}$ can be expressed as

$$\begin{aligned}\varphi_{WSCM_{E-L}}(t) &= \varphi_{WSCM_E}(t)\cdot\varphi_{WSCM_L}(-t)\\ &= \left[(1-2it)^{-n}e^{\frac{it\delta}{1-2it}}\right]\cdot\left[(1+2it)^{-n}e^{\frac{-it\delta}{1+2it}}\right]\\ &= (1+4t^2)^{-n}e^{\frac{-4t^2\delta}{1+4t^2}}\end{aligned} \tag{22}$$

The multi-correlator receiver contains five n pairs of correlators (of E and L), and each correlator contains an I branch and a Q branch. Let the degrees of freedom $V = 2n$. According to the central limit theorem, when according to the central limit theorem, when V tends to infinity, the noncentral chi-square distribution tends to the Gaussian distribution [38]. Fig. 5 shows the simulation graph of the noncentral chi-square distribution PDF varying with V.

In Fig. 5, the greater the degree of freedom, the more closely the WSCM follows the Gaussian distribution. When the number of degrees of freedom is 10 (the red line in the figure), it can be approximated that the single-sided WSCM of the correlation peak function follows the Gaussian distribution, which is consistent with the central limit theorem.

According to the properties of the Gaussian distribution, it can be approximated that $Z_t = WSCM_{E-L} \sim N(\mu, \sigma^2)$. Based on the relationship between the characteristic function and the k-order origin moment, it can be known that the mean value μ of $WSCM_{E-L}$ is

$$\mu = E[Z_t] = (-i)\varphi'_{WSCM_{E-L}}(0) = 0 \tag{23}$$

because

$$E[Z_t^2] = (-i)^2\varphi''_{WSCM_{E-L}}(0) = 8n + 8\delta \tag{24}$$

thus, the variance σ^2 of $WSCM_{E-L}$ is

$$D[Z_t] = E[Z_t^2] - (E[Z_t])^2 = 8n + 8\delta \tag{25}$$

It can be seen from the above section that the spoofing detection statistic $\mathrm{WSCM_{E-L}}$ metric is obtained by calculating the difference between the left and right peak weighted second-order central moments. When there is no spoofing interference, the Gaussian distribution is followed, with a mean value of zero and a variance of $8n + 8\delta$. When distortion occurs, the metric no longer obeys the Gaussian distribution, and this property can be used to effectively detect spoofing signals.

In reality, spoofing detection has to be performed in the presence of correlation peak distortions caused by multipath and thermal noise, which alters the detection index. Both the Ratio metric and Delta metric usually use narrow-band correlators, and the additional correlators of the WSCM metric increase the data test relevance, which means that greater amounts of noise and multipath can be cancelled during the measurement. Moreover, the WSCM metric uses broadband correlators to increase the tolerance to noise and user dynamic characteristics. Furthermore, changes in multipath and thermal noise are unlikely to be consistent with the changes in induced spoofing, because usually, multipath and thermal noise are usually inherently random [19]. As such, the WSCM metric is not sensitive to errors caused by multipath and thermal noise.

C. Range of Correlator Pairs

The implementation of spoofing detection needs to determine the range of the number of correlator pairs n (i.e., n pairs of E and L correlators distributed symmetrically with respect to P) after making a comprehensive trade-off among detection performance, computational complexity, hardware limitations and cost. Because n not only affects the complete quantification degree of the symmetry of correlation function, so as to determine whether spoofing signals can be accurately identified, but also affects the computational complexity that determines the hardware requirements and cost of the receiver.

The number of possible multi-correlator implementations is quite large [18], as the lower limit of spacing between any correlator pair in most practical receivers is 0.1 chips; however, some techniques allow narrower spacings. Although there is no upper limit to spacings, few receivers use correlator pairs with spacings greater than two chips [39]. This still leaves as many as 20 possible correlator spacings, resulting in between 2 and 20 possible correlator pairs. Hence, $2 \le n \le 20$. Next, the selection range of n is further determined according to the detection performance, computational complexity, and other factors of the algorithm.

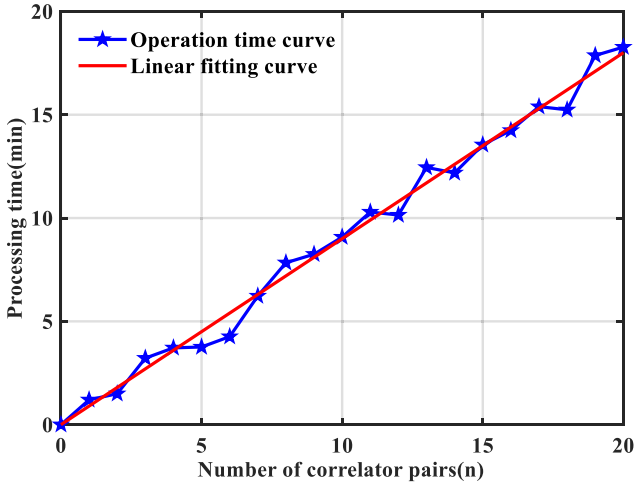


Fig. 6. Variation curve of the operation time with the number of correlator pairs.

TABLE I
STATISTICS OF DETECTION EFFECTS UNDER DIFFERENT CORRELATOR PAIRS

Number of correlator pairs(n)	First alarm time(s)	Spoofing detection rate (%)	Operation time(min)
3	170	76.21	22.4
4	149	82.52	23.8
5	120	93.48	24.5
6	120	93.89	28.2
7	119	92.56	40.6
10	118	94.59	62.8

Firstly, the influence of the change of n on the computational complexity is considered. Fig. 6 shows the change graph of the operation time when the number of correlator pairs ranges from 0 to 20 pairs of the intermediate frequency signal 1 min before the post-processing TEXBAT Clean Static Scenario using the software receiver GNSS-SDR. This experiment only considers the number of correlator pairs n, and the other influencing factors remain the same.

The operation time in the figure changes almost linearly with the number of correlator pairs. The main reason for this is that the increase of n leads to a linear increase in the number of incoherent integration operations between the local signal and the received signal of the receiver. It should be noted that the monitoring correlator does not participate in the positioning settlement.

Secondly, further research is made in combination with the effect of spoofing detection. Fig. 7 shows the time-domain transient response results of the detection statistic $\mathrm{WSCM_{E-L}}$ under the post-processing TEXBAT Scenarios 7 of the software receiver GNSS-SDR, in which spoofing occurs 110 s later. The larger the n, the shorter the reaction time and the more sensitive the method is to the spoofing inference. This is primarily due to the presence of wide-band correlators with larger correlator spacing. However, when $n \geq 5$, the detection reaction time is substantially no longer reduced.

The specific performance of the method in the presence of different numbers of correlator pairs is shown in Table I. It shows the time of the first alarm response of the WSCM algorithm, the spoofing detection probability after 110 s, and

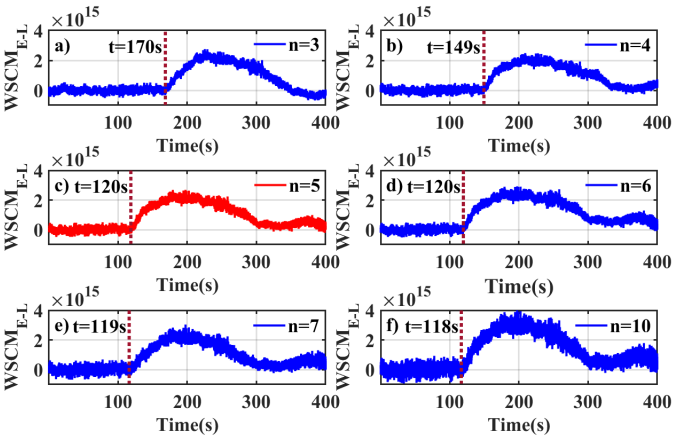


Fig. 7. Time-domain transient response of $\mathrm{WSCM_{E-L}}$ under different correlator pairs.

the results of the total operation time. The analysis shows that when $n \geq 5$, the spoofing alarm response time basically reaches the threshold of approximately 120s, and the detection probability is no longer significantly improved, but the running time continues to increase. Therefore, selecting $n = 5$ is the best; this takes into account the spoofing detection performance but does not require high computational complexity.

Therefore, this study considers five pairs of correlators as an example (n=5) to evaluate the effectiveness of the algorithm. To better evaluate the dynamic changes in the correlation peak of the receiver, the interval between the correlator pairs are equally spaced, and the weights of the correlators are calculated according to equations (17) and (18). Table II contains specific correlator spaces and weights used for the WSCM method. Table II shows the WSCM metric obtained by weighting the output values of the multiple correlators, including the narrow-band correlators with smaller spacing (0.2 chips) and wide-band correlators with larger spacing (1 chip), which facilitate the measurement of changes in correlator peak symmetry.

D. Threshold Calculation

Detecting induced spoofing is a binary hypothesis testing problem. To calculate a reasonable threshold, statistical analysis has been performed to implement a NP detector [30]. Two hypotheses are considered: the null hypothesis, H_0, that is considered when there is no spoofing present, and the alternative hypothesis, H_1, that is considered when the spoofer is present. Based on the above theoretical analysis, the test metric is $Z_t = WSCM_{E-L} \sim N(\mu, \sigma^2)$; therefore, the binary hypothesis test [27] can be expressed as

$$\begin{cases} H_0 : Z_t \cong \mu, Without \quad Spoofing \\ H_1 : Z_t \neq \mu, With \quad Spoofing \end{cases} \tag{26}$$

where Z_t is the measured left and right WSCM deviation of the correlation peak, and μ is the mean value, which is approximately zero here.

To construct the NP detector without a completely defined alternative hypothesis distribution, the likelihood function can be defined from equation (26), as

$$L(Z_t) = |Z_t - \mu| \tag{27}$$

TABLE II
CORRELATION SPACE AND WEIGHTED WSCM COMBINATIONS

Space (T_c)	-1	-0.8	-0.6	-0.4	-0.2	0.2	0.4	0.6	0.8	1
Wei. Comb.	0.088	0.110	0.145	0.219	0.438	0.438	0.219	0.145	0.110	0.088

Using the likelihood function, the probability of false alarm for a given threshold γ can be calculated using the following formula:

$$P_{fa}(\gamma) = \rho(|Z_t - \mu| > \gamma \,|H_0) \tag{28}$$

where γ is the reasonable detection threshold, and the probability of false alarm P_{fa} refers to the probability that the hypothesis of the presence of an induced spoofing attack is accepted. Still, in fact, it does not exist. In terms of the specified carrier-to-noise ratio,C/N_0, the finalP_{fa} can also be considered as a threshold function.

If P_{fa} is given, the detection threshold γ can be determined by inverting the probability function. As the difference between the left and right WSCM peaks without spoofing follows the Gaussian distribution, the threshold γ can be obtained from the following formula:

$$\gamma = \sqrt{2}\sigma erfc^{-1}(2 \cdot P_{fa}) \tag{29}$$

where $erfc^{-1}$ is the inverse Gaussian function. Combining equations (7), (25), and (29), it is evident that the threshold γ is closely related to C/N_0. If C/N_0 is higher, the variance σ^2 is lower; therefore, the threshold is closer to the average value μ. A higher C/N_0 implies less interference to the navigation signal, a better tracking loop, and more accurate measurement results. The WSCM test values calculated in real time are more likely to cluster around a constant μ, implying more minor variance. Unless intermediate spoofing or any other interference occurs, the probability that the WSCM test value Z_t is too far away from μ will be very low [27].

P_d or detection rate can be obtained using the following equation:

$$P_d(\gamma) = \rho(|Z_t - \mu| > \gamma \,|H_1) \tag{30}$$

The detection probability P_d is the probability that the hypothesis of the spoofing attack is accepted and actually exists. In theory, when calculating P_d, we must first know the probability distribution of the detection metric under the spoofing-present situation. However, as its distribution depends on the mode of spoofing attack, and spoofing has time-varying characteristics, the receiver does not know how the power and code phase of the spoofing signal will vary. Moreover, in frequency lock mode, there may be errors in the carrier phase difference, making it impossible for the target receiver to predict the behavior of the spoofer. These factors make it difficult to determine the distribution of WSCM in an induced spoofing environment, and it is impractical to derive the analytical expression of the PDF. A statistical method is often used instead of P_d to calculate the detection rate of the proposed method. P_d is expressed as follows:

$$P_d(\gamma) = \frac{Num\{|Z_t - \mu| > \gamma\}}{N} \tag{31}$$

Thus, P_d is the ratio of the number of samples ($Num\{\cdot\}$) exceeding the threshold γ to the total number of samples (N), when a spoofing signal is present. To obtain P_d, we first used equation (29) to calculate the threshold γ for a given P_{fa}, and then performed spoofing detection within each detection window.

In summary, the spoofing detector can finally be expressed as

$$\begin{cases} |Z_t - \mu| > \gamma \quad Decide H_1 \\ Otherwise \quad Decide H_0 \end{cases} \tag{32}$$

To summarize, the specific implementation strategy of the WSCM method is as follows:

1) Arrange n ($n \geq 3$) pairs of correlators symmetrically at the right and left of the P correlator of each channel of the receiver to obtain the output value of each correlator, The value of n is determined by the computational complexity of the algorithm (refer to Section III Part C).
2) Divide the symmetrically arranged correlators into two groups, E (left peak) and L (right peak), and obtain the WSCM of the left peak $\mathrm{WSCM_E}$ and the WSCM of the right peak $\mathrm{WSCM_L}$according to the weighted calculation of the output values of the correlators in each group respectively. Refer to formula (19) for the calculation method. The weight of each correlator in the weighted calculation is determined by the distance between the corresponding correlator and the P correlator and the noise variance of the output value; and the specific calculation method is as per formula (18).
3) Obtain the difference between $\mathrm{WSCM_E}$ and $\mathrm{WSCM_L}$ to determine the WSCM difference$\mathrm{WSCM_{E-L}}$ between the left and the right peaks. The difference function follows the Gaussian distribution of mean and variance. Refer to formulas (20), (23), and (25) for specific calculation formulas.
4) Use the NP detector to detect the difference: set the false alarm rate in a non-spoofing scenario, calculate the test threshold according to the mean and variance, and compare the$\mathrm{WSCM_{E-L}}$with the test threshold to determine whether there is spoofing interference. When the absolute value of the difference between the $\mathrm{WSCM_{E-L}}$ and the mean value is greater than the test threshold, it is assumed that there is spoofing interference (refer to Section III Part D).

IV. RESULTS AND ANALYSIS

Based on theoretical analysis, this study embedded the proposed WSCM-based spoofing detection method into a GNSS-SDR. The TEXBAT dataset was used to verify the performance of the WSCM detection algorithm in different spoofing scenarios. The detection performance of the WSCM

TABLE III
SUMMARY OF THE TEXBAT GPS SPOOFING TRACES

Scenario Designation	Synchronization	Type	Power Advantage
1: Static Switch	N/A	None	N/A
2: Static Overpowered Time Push	Code Phase Proportional	Time	10
3: Static Matched-Power Time Push	Frequency Lock Mode	Time	1.3
4: Static Matched-Power Pos. Push	Frequency Lock Mode	Position	0.4
5: Dynamic Overpowered Time Push	Code Phase Proportional	Time	9.9
6: Dynamic Matched-Power Pos. Push	Frequency Lock Mode	Position	0.8
7: Static Matched-Power Time Push*	Carrier Phase Aligned	Time	Matched
8: Security Code Estimation and Replay	Carrier Phase Aligned	Time	Matched

algorithm was compared with that of the Ratio metric, Delta metric, and ELP metric algorithms, to evaluate its spoofing detection capabilities.

A. Descriptions of TEXBAT Scenarios

The TEXBAT dataset is the first public spoofing database generated by the Radionavigation Laboratory of the University of Texas at Austin [32], [33]. It includes high-fidelity digital real-time GPS L1 C/A data of two clean scenarios and eight spoofing scenarios. The datasets use a sampling rate of 25 Msps and high-quality front-end filtering, providing a steady-state frequency response with a bandwidth of more than 20 MHz near L1 and test receivers that support anti-spoofing against attacks. Notably, TEXBAT is the only publicly available spoofing test dataset, and it is the de facto standard for testing the anti-spoofing performance of GPS receivers. Table III summarizes the attributes of the eight spoofing scenarios.

In Table III, "Code Phase Proportional" implies that the carrier phase of the spoofing signal is proportional to the code phase change. "Frequency Lock Mode" implies that the initial phase offset between the spoofing signal and the authentic signal remains unchanged throughout the spoofing scenario. "Carrier Phase Aligned" implies that the spoofing signal is accurately aligned with the carrier phase of the authentic signal. "Matched" implies that the spoofing signals are power matched, but exact values are unknown [40].

This study aimed to consider the distortion of the cross-correlation function caused by the mixing of counterfeit signals in the signals generated by a satellite in a more subtle induced spoofing scenario. When a spoofer tries to induce a position or timing deviation in the target receiver by moving the code phase of its counterfeit signals, it can adopt either of two strategies concerning carrier phase generation [32]. In the default mode, the rate of change of the signals' carrier phase is proportional to the rate of change of the corresponding code phase, that is, Scenario 7 and Scenario 8. For this study, Scenario 8 was not considered because it does not involve security code estimation and detection. In an alternative mode, the so-called frequency lock mode, the spoofer keeps any initial phase offset between the counterfeit signals and the authentic signals approximately fixed and maintains this fixed carrier phase offset even while shifting the code phase of its counterfeit signals to induce a position or timing deviation in the target receiver. Being able to lock the relative (counterfeit-to-authentic) carrier phase even while shifting the relative (counterfeit-to-authentic) code phase allows the spoofer to circumvent some spoofing detection strategies [32], namely Scenarios 3, 4, and 6. Of these, Scenario 6 is based on a mobile platform receiver. Still, considering the limitations of receivers and the challenges caused by changes in the natural environment, this is not the focus of this article; therefore, this scenario was not considered. In addition, to better ascertain spoofing detection performance, Scenario 4, with its lower spoofing power than Scenario 3, was selected to evaluate the efficacy of this study's algorithm.

To better verify detection performance in advanced induced spoofing scenarios, this study focuses on using TEXBAT Scenarios 4 and 7 to evaluate spoofing detection. From these two spoofing scenarios, we can observe the changes in detection performance in the frequency lock mode (Scenario 4) and the more complex induced spoofing mode where the carrier and code phases are consistent, and the signals are power matched (Scenario 7).

B. TEXBAT Scenario 4: Frequency Lock Mode

In this mode, Scenario 4 was used to evaluate spoofing detection performance. To fully demonstrate the spoofing implementation process, the GNSS-SDR was improved to obtain the transient response of the receiver correlation function under 61 correlators. The tracking loop correlator was configured at an interval of 0.1 chips. Taking PRN 6 as an example, the specific results are shown in Fig. 8.

The spoofing signals attacked and separated the correlation peak of the authentic signals in frequency-lock mode after approximately 100 s. The tracking loop of the victim receiver was completely locked on the spoofing signals after approximately 300 s. The correlation peak of the authentic signals was more than one chip out. In this process, the spoofer had a low-power advantage of 0.4 dB and tried to maintain a persistent carrier phase offset from the authentic signals. It should be noted that the rate of change of code phase and carrier phase did not maintain a constant ratio, but the relative code phase offset shifted relative to the fixed carrier phase offset. This interaction can cause correlation peak symmetry distortion. The top view in Fig. 8b highlights the problem of large fluctuations at a critical time during the spoofing process. These fluctuations are primarily due to inaccurate frequency locking of the spoofing signals to the authentic signals, resulting in the slow switching of the I and Q branches with each other as well as power leakage.

Fig. 9 shows the time-domain transient response of the conventional SQM metrics and the WSCM metric during spoofing under Scenario 4. It provides the detection thresholds corresponding to a constant false alarm rate of 10%. Before approximately 100 s, there was no apparent change

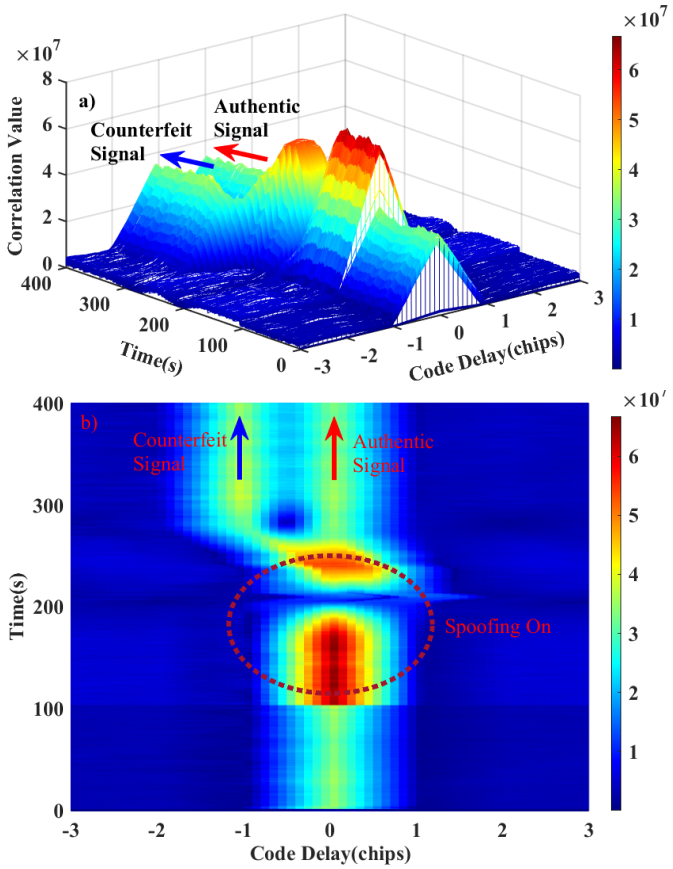


Fig. 8. Navigation-data-free output time history of 61 correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap of PRN 6 (a) and its top view (b) for Scenario 4 of the TEXBAT dataset.

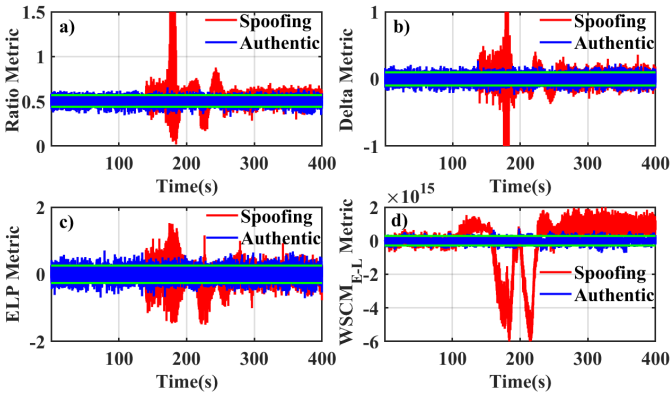


Fig. 9. Comparison of detection results with thresholds for four different detection metrics for Scenario 4 of the TEXBAT dataset. (a) the Ratio Metric, (b) the Delta Metric, (c) the ELP Metric, and (d) the WSCM Metric.

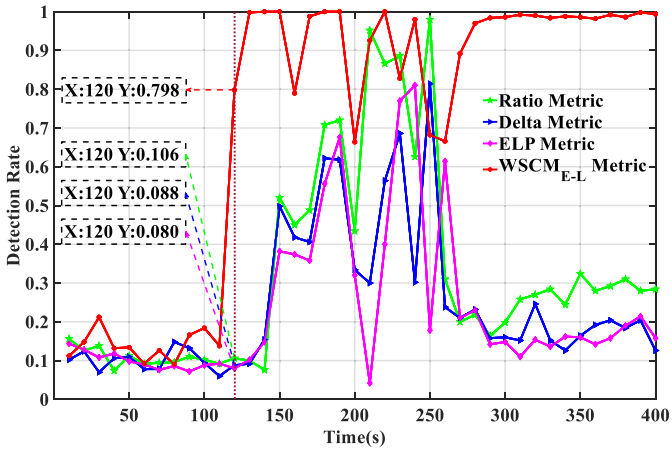


Fig. 10. Comparison of the changing detection rates of four different detection metrics for Scenario 4 of the TEXBAT dataset over time. The false alarm rate was set to 10%.

as no spoofing signals were injected. After 100 s, the interaction between the spoofing signals and authentic signals caused cross-correlation function distortion, and metric values changed significantly. This was especially noticeable between 110 and 250 s. After 250 s, the metric values remain stable because the tracking loop is wholly locked on the spoofing signals. Therefore, significant changes in metric values in this interaction phase can be used to detect the presence of spoofing signals. In addition, it should be noted that compared with the conventional SQM metrics (Fig. 9a-c), the WSCM metric (Fig. 9d) changed more significantly (exceeding the detection threshold) between approximately 110 and 150 s and after approximately 250 s; after 250 s especially, it could better sense minor oscillations of SQM caused by inaccurate frequency locking. therefore, the WSCM metric–based inspection technique is recommended for a faster and more accurate statistical detection of spoofing signals.

To better illustrate the changing detection performance over time, Fig. 10 shows the time-domain change of the detection performance of the conventional SQM metrics and the WSCM metric under a constant false alarm rate of 10%, where the detection time window is 10 s. It can be seen that no spoofing interference occurred between 0 and 100 s, and the P_d of the four metrics was approximately 10%, which is consistent with the set constant false alarm rate of 10%. In the spoofing interference phase from 100 to 250 s, the detection performance of the WSCM metric technique was significantly better than that of conventional SQM metrics, mostly at approximately 80–100%, whereas the detection probabilities of the latter were mostly below 80%. The P_d of the WSCM metric reached 79.8% at 120 s, while that of the conventional SQM metrics were just above 40% at approximately 150 s; therefore, the warning time of the former was approximately 30 s ahead of the latter. Finally, after 250 s, the detection probabilities of the conventional SQM metrics dropped to 10–20% above the constant false alarm rate, but the P_d of the WSCM metric was more than 98%. Therefore, the WSCM metric spoofing detection technique not only reduced the reaction time but also increased the probability of detection, implying it could issue an alarm more rapidly and accurately when spoofing signals were present.

To more comprehensively evaluate the detection performance of the WSCM metric spoofing detection technique, Fig. 11 plots the receiver operating characteristic (ROC) curve of the conventional SQM metrics and the WSCM metric. The WSCM spoofing detection technique was found to possess significant advantages over the conventional metrics. Under the same false alarm rate, the P_d of the WSCM metric was significantly higher than that of conventional metrics, exceeding 90%. On the part of the plot that reflects real-life situations, that is, when a receiver requires a low false alarm

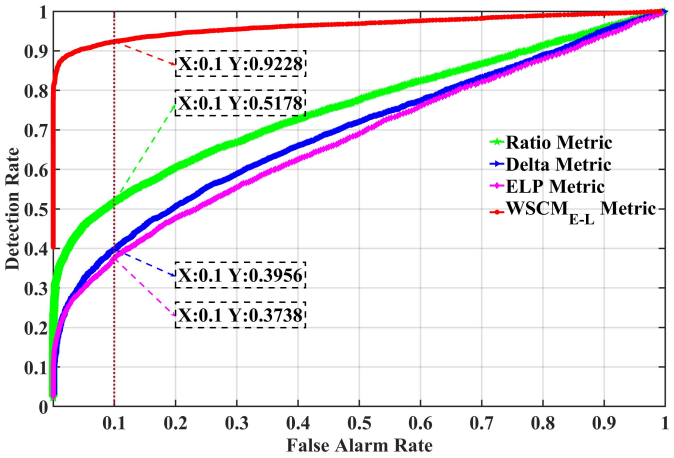


Fig. 11. Comparison of ROC curves for four different detection metrics for Scenario 4 of the TEXBAT dataset.

TABLE IV
THE CALCULATION TIME OF DIFFERENT DETECTION METRICS FOR SCENARIO 4 OF THE TEXBAT DATASET

	Ratio metric	Delta metric	ELP metric	WSCM metric
Operation time(min)	8.21	8.29	10.56	24.69

rate, such as 10%, P_d based on the WSCM technique was 40.5% higher than that of the conventional Ratio metric. Even at a false alarm rate of 0.1%, the P_d of the WSCM spoofing detection technique was still 87.5%, which imparts it a more excellent application value as a receiver spoofing early warning technique.

Table IV shows the receiver running time under four different detection metrics under Scenario 4. Compared with that of the conventional SQM metrics, the WSCM metric increases the computational complexity due to the addition of correlators, and its running time approximately doubles. But as Prof. Psiaki concludes, not all spoofing defense modes are equally effective against all attack modes, and vice versa. Moreover, not all spoofing defense modes have the same implementation cost. If any spoofing defense mode wants to improve its efficacy, it must do so at a certain cost [15]. Furthermore, under the background of highly threatening and destructive induced spoofing, it is worthwhile to ensure the superior performance of the WSCM method in spoofing defense and forgo part of the computational cost.

C. TEXBAT Scenario 7: Matched-Power and Carrier Phase Aligned Mode

This section further evaluates spoofing detection performance under TEXBAT dataset Scenario 7 in the carrier phase-aligned mode. Fig. 12 plots the transient response of the receiver tracking loop correlation function.

It can be seen from Fig. 12 that no spoofing took place between 0 and 110 s, and there was no correlation peak symmetry distortion during that time. From 110 to 150 s, the spoofing signals attacked the receiver tracking loop. During this period, the carrier phase was accurately aligned, and power increased nonlinearly. Between 150 and 400 s, the Doppler frequency of the spoofing signals remained precisely

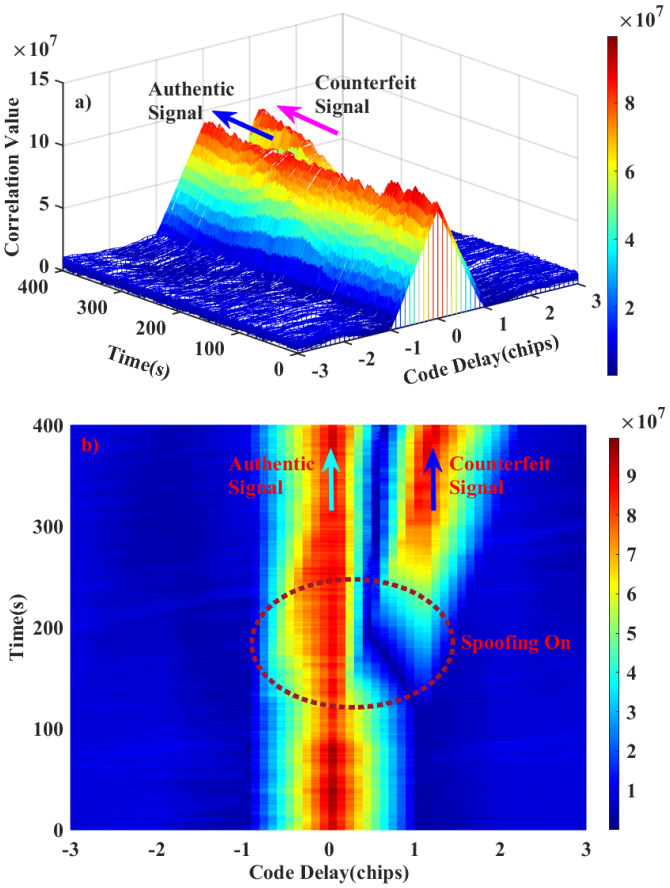


Fig. 12. Navigation-data-free output time history of 61 correlation taps uniformly spaced at an interval of 0.1 C/A code chips and centered at the receiver's prompt tap of PRN 6 (a) and its top view (b) for Scenario 7 of the TEXBAT dataset.

the same as the Doppler frequency of the authentic signals (frequency lock), and the code phase of the spoofing signals were adjusted from 0 at a rate of 1.2 m/s relatives to the corresponding authentic signals, thus gradually separating the authentic signals. After the separation phase, the target receiver's tracking loop locked the spoofed signal, and the final code phase difference between the authentic and spoofing signals was approximately two chips. It can be seen from the top view in Fig. 12b that Scenario 7 had no relative carrier phase effect, compared to that of Scenario 4, when the spoofing and authentic signals were approximately matched in power, and the correlation peak symmetry distortion caused by the interaction of the correlation peaks of the spoofing and authentic signals was not sufficiently prominent. As such, the performance of the spoofing detection techniques was further tested by this spoofing mode.

Fig. 13 shows the time-domain transient response of the conventional SQM metrics and the WSCM metric during spoofing under Scenario 7. It provides the detection thresholds corresponding to a constant false alarm rate of 10%. The response of four detection metrics between 0 and 110 s is the same as their response in the absence of spoofing, implying that there was no spoofing. Between 110 and 400 s, there was a spoofing attack, resulting in correlation peak symmetry distortion. The conventional SQM metrics' responses were smooth overall, whereas the WSCM metric response changed

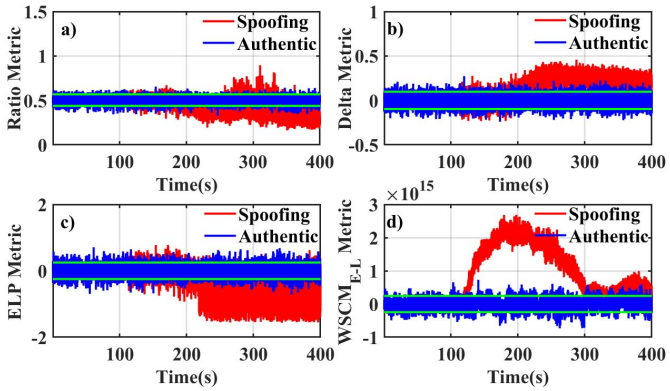


Fig. 13. Comparison of detection results with thresholds for four different detection metrics for Scenario 7 of the TEXBAT dataset. (a) the Ratio Metric, (b) the Delta Metric, (c) the ELP Metric, and (d) the WSCM Metric.

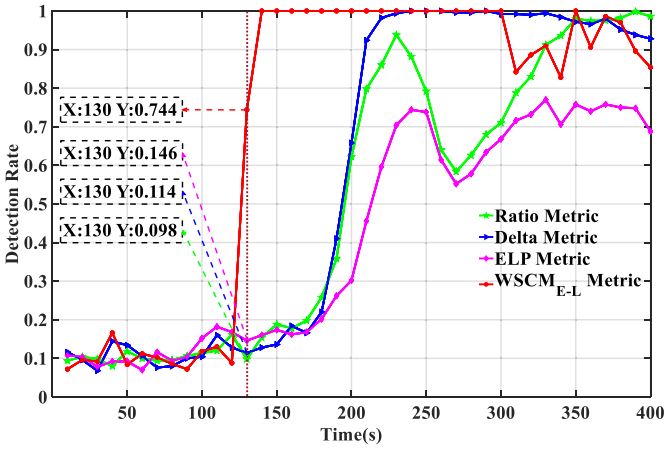


Fig. 14. Comparison of the changing detection rates of the four different detection metrics for Scenario 7 of the TEXBAT dataset over time. The false alarm rate was set to 0.1.

significantly, especially between 110 and 300 s. Moreover, during the carrier phase alignment stage of the spoofing (110 to 150 s), the SQM metrics showed more apparent changes, indicating that the detection performance of the SQM metrics was superior. Compared with that in Scenario 4, the overall response of the four metrics was minor. This is probably because Scenario 7 uses more subtle carrier phase alignment, and has more minor power advantage. However, the impact on WSCM metric detection performance was not as noticeable.

Fig. 14 shows the detection performance characteristics over time of the conventional SQM metrics and the WSCM metric throughout the spoofing process under a constant false alarm rate of 10% where the detection time window is 10 s. It can be seen that the P_d of the four detection techniques between 0 and 110 s was close to 10%, which is consistent with the false alarm rate. After 110 s, the WSCM-based detection technique first showed an enormous response at 130 s, with a P_d of 74.4%. In comparison, the three conventional SQM metrics only had a significant response when close to 200 s; therefore, the response time of the former was 70 s ahead of the latter. Second, during the spoofing process, the P_d of the WSCM metric reached 100% between 140 and 300 s,

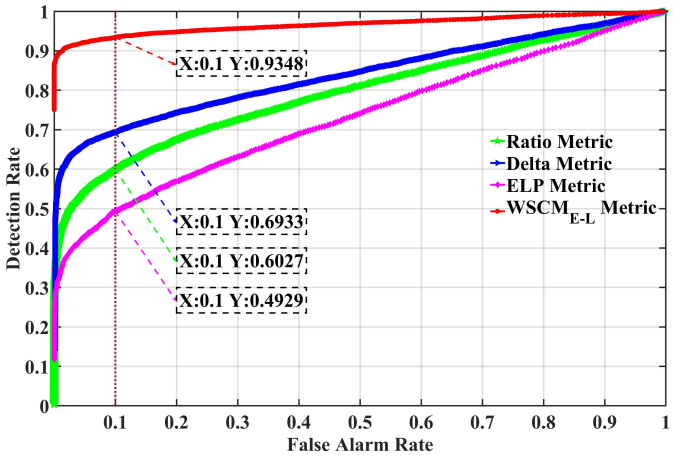


Fig. 15. Comparison of ROC curves for four different detection metrics for Scenario 7 of the TEXBAT dataset.

TABLE V
THE CALCULATION TIME OF DIFFERENT DETECTION METRICS FOR SCENARIO 7 OF THE TEXBAT DATASET

	Ratio metric	Delta metric	ELP metric	WSCM metric
Operation time(min)	8.39	8.52	10.78	24.51

and after 300 s, it remained above 80%. This P_d was significantly better than that of three conventional SQM metrics. Compared with that in Scenario 4, the performance of the four detection techniques was slightly worse in the initial phase of spoofing, but the detection performance significantly improved in the later phase. As Scenarios 4 and 7 differed in terms of their frequency-lock mode, we could not fairly compare the performance of the detection techniques in these two scenarios. Nevertheless, the WSCM-based detection technique still showed excellent spoofing detection performance in both scenarios, indicating that this technique has certain advantages in terms of providing an early warning of a spoofing attack.

Finally, Fig. 15 shows the ROC curve of the conventional SQM metrics and the WSCM metric under Scenario 7. Compared with that of the conventional metrics, the ROC curve of the WSCM metric was closer to the upper left corner, indicating better overall detection performance and that the P_d was higher under the same false alarm rate, basically all above 90%. In addition, under a false alarm rate of 10%, the P_d of the Delta metric, which had better detection performance, increased by 24.15%. The better detection performance of the WSCM metric was more notable when the false alarm rate of the receiver was meager, as it is required to be in practice. In addition, the detection performance of the WSCM metric did not change significantly compared to that in Scenario 4, indicating that the WSCM-based technique is reliable and had an improved ability to deal with complex spoofing techniques.

Table V shows the receiver running time under four different detection metrics under Scenario 7, and its overall performance is consistent with that of Scenario 4. Compared with that of the conventional SQM metrics, the running time of the WSCM metric was approximately doubled, further showing

that the WSCM metric improves the detection performance at the expense of the computational complexity.

V. Conclusion

Aiming at the problem that the conventional SQM algorithm has low spoofing detection resolution and imperfect quantification index of correlator output value, which leads to the poor detection performance of intermediate or sophisticated spoofing interference, based on the influence of induced spoofing on the symmetry of correlation function of receiver tracking loop, this study, for the first time, adopted the design of a multi-correlator time-domain transient response value weighting algorithm, and proposed a new spoofing detection method based on WSCM that can be used to detect intermediate or sophisticated spoofing interference. A series of experiments with the TEXBAT were performed to verify the effectiveness of the proposed algorithm. The results demonstrate that the proposed method not only shortened the spoofing alert time by at least 30 s, but also increased detection efficiency by 20%. Moreover, under different false alarm rates, the P_d basically exceeded 90%. When the false alarm rate was 10%, the P_d increased by at least 24.15% higher than that of the SQM metrics, and the P_d improved more evidently under the condition of low false alarm rate. However, the WSCM-based method achieves this improved performance at the expense of additional computational complexity, which is caused by the addition of additional correlators.

The new algorithm can better detect the subtle time-varying influence caused by spoofing interference that not only has high detection accuracy, but also has high sensitivity and good resolution and robustness for intermediate or sophisticated spoofing interference. Although the performance of the new algorithm is greatly improved at the expense of part of the computational complexity, it is still of great application value for studying receivers equipped with spoofing detection modules and dealing with intermediate and sophisticated spoofing interference.

Appendix A

The quadratic distribution of n-dimensional normal random vector after linear transformation:

Suppose an n-dimensional normal random vector $\boldsymbol{X} \sim N_n(\boldsymbol{\mu}, \boldsymbol{V})$, where $\boldsymbol{V} > 0$, A is an invertible square matrix of order n, and b is a constant vector, then the random variable (regarded as the quadratic form of the random vector after linear transformation) satisfies

$$(\boldsymbol{AX}+\boldsymbol{b})^T(\boldsymbol{AVA}^T)^{-1}(\boldsymbol{AX}+\boldsymbol{b}) \sim \chi^2(2n,\delta) \tag{i}$$

where the noncentral parameter

$$\delta = (\boldsymbol{A\mu}+\boldsymbol{b})^{\mathrm{T}}(\boldsymbol{AVA}^{\mathrm{T}})^{-1}(\boldsymbol{A\mu}+\boldsymbol{b}) \tag{ii}$$

Proof: Because $\boldsymbol{X} \sim N_n(\boldsymbol{\mu}, \boldsymbol{V})$, so $E(\boldsymbol{AX}+\boldsymbol{b}) = \boldsymbol{AEX}+\boldsymbol{b} = \boldsymbol{A\mu}+\boldsymbol{b}D(\boldsymbol{AX}+\boldsymbol{b}) = D(\boldsymbol{AX}) = \boldsymbol{A}D(\boldsymbol{X})\boldsymbol{A}^T = \boldsymbol{AVA}^T$; therefore, the random vector $\boldsymbol{AX}+\boldsymbol{b} \sim N_n(\boldsymbol{A\mu}+\boldsymbol{b}, \boldsymbol{AVA}^T)$. Because $\boldsymbol{V} > 0$, from the positive definite matrix decomposition, we know that $\boldsymbol{V} = \boldsymbol{CC}^T$ (C is the invertible square matrix), so

$$\boldsymbol{AVA}^T = \boldsymbol{ACC}^T\boldsymbol{A}^T = \boldsymbol{AC}(\boldsymbol{AC})^T \tag{iii}$$

Knowing that A and C are reversible, so $\boldsymbol{AC}$ is reversible. Let $\boldsymbol{Y} = (\boldsymbol{AC})^{-1}(\boldsymbol{AX}+\boldsymbol{b})$, that is, $\boldsymbol{AX}+\boldsymbol{b} = (\boldsymbol{AC})\boldsymbol{Y}$, where

$$\begin{aligned} E\boldsymbol{Y} &= E[(\boldsymbol{AC})^{-1}(\boldsymbol{AX}+\boldsymbol{b})] = (\boldsymbol{AC})^{-1}(\boldsymbol{A\mu}+\boldsymbol{b}) && \text{(iv)}\\ D\boldsymbol{Y} &= D[(\boldsymbol{AC})^{-1}(\boldsymbol{AX}+\boldsymbol{b})] \\ &= (\boldsymbol{AC})^{-1}D(\boldsymbol{AX}+\boldsymbol{b})((\boldsymbol{AC})^{-1})^T \\ &= (\boldsymbol{AC})^{-1}\boldsymbol{AC}(\boldsymbol{AC})^T((\boldsymbol{AC})^{-1})^T = \boldsymbol{I} && \text{(v)} \end{aligned}$$

Proving that

$$\boldsymbol{Y} = (\boldsymbol{AC})^{-1}(\boldsymbol{AX}+\boldsymbol{b}) \sim N_n((\boldsymbol{AC})^{-1}(\boldsymbol{A\mu}+\boldsymbol{b}), \boldsymbol{I}_n) \tag{vi}$$

then

$$\begin{aligned} &(\boldsymbol{AX}+\boldsymbol{b})^T(\boldsymbol{AVA}^T)^{-1}(\boldsymbol{AX}+\boldsymbol{b}) \\ &\quad= (\boldsymbol{AX}+\boldsymbol{b})^T(\boldsymbol{AC}(\boldsymbol{AC})^T)^{-1}(\boldsymbol{AX}+\boldsymbol{b}) \\ &\quad= (\boldsymbol{AX}+\boldsymbol{b})^T[(\boldsymbol{AC})^{-1}]^T(\boldsymbol{AC})^{-1}(\boldsymbol{AX}+\boldsymbol{b}) \\ &\quad= [(\boldsymbol{AC})^{-1}(\boldsymbol{AX}+\boldsymbol{b})]^T[(\boldsymbol{AC})^{-1}(\boldsymbol{AX}+\boldsymbol{b})] \\ &\quad= \boldsymbol{Y}^T\boldsymbol{Y} \sim \chi(n,\delta) \end{aligned} \tag{vii}$$

By definition, the noncentral parameter is

$$\begin{aligned} \delta &= [(\boldsymbol{AC})^{-1}(\boldsymbol{A\mu}+\boldsymbol{b})]^T[(\boldsymbol{AC})^{-1}(\boldsymbol{A\mu}+\boldsymbol{b})] \\ &= (\boldsymbol{A\mu}+\boldsymbol{b})^T((\boldsymbol{AC})^T)^{-1}(\boldsymbol{AC})^{-1}(\boldsymbol{A\mu}+\boldsymbol{b}) \\ &= (\boldsymbol{A\mu}+\boldsymbol{b})^T(\boldsymbol{AVA}^T)^{-1}(\boldsymbol{A\mu}+\boldsymbol{b}) \end{aligned} \tag{viii}$$

References

[1] S. Bian, Y. Hu, and B. Ji, "Research status and prospect of GNSS anti-spoofing technology," *Scientia Sinica Inf.*, vol. 47, no. 3, pp. 275–287, 2017.

[2] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," *IEEE Access*, vol. 8, pp. 165444–165496, 2020.

[3] M. G. Amin, A. Broumandan, P. Closas, and J. L. Volakis, "Vulnerabilities, threats, and authentication in satellite-based navigation systems," *Proc. IEEE*, vol. 104, no. 6, pp. 1169–1173, Jun. 2016.

[4] S. M. Sánchez-Naranjo *et al.*, "GNSS vulnerabilities," in *Multi-Technology Positioning*, J. Nurmi, E. S. Lohan, H. Wymeersch, G. Seco-Granados, O. Nykänen, Ed. New York, NY, USA: Springer, 2017, pp. 55–77. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-3-319-50427-8_4#citeas

[5] A. Jafarnia-Jahromi, A. Broumandan, S. Daneshmand, and G. Lachapelle, "Vulnerability analysis of civilian L1/E1 GNSS signals against different types of interference," in *Proc. 28th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Tampa, FL, USA, 2015, pp. 3262–3271.

[6] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, "Effective GPS spoofing detection utilizing metrics from commercial receivers," in *Proc. Int. Tech. Meeting The Inst. Navigat.*, Reston, VI, USA, Feb. 2018, pp. 672–689.

[7] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Division Inst. Navigat.*, Savannah, GA, USA, 2008, pp. 2314–2325.

[8] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Crit. Infrastruct. Protection*, vol. 5, no. 3, pp. 146–153, 2012.

[9] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle," *GPS World*, vol. 23, no. 8, pp. 30–33, Aug. 2012.

[10] M. L. Psiaki, T. E. Humphreys, and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," *IEEE Spectr.*, vol. 53, no. 8, pp. 26–53, Aug. 2016.

[11] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *J. Inst. Navigat.*, vol. 64, no. 1, pp. 51–66, 2017.

[12] "Spirent federal systems," *GPS World*, vol. 24, no. 5, p. 18, 2013.

[13] K. Borre, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*, 11th ed. Berlin, Germany: Birkhäuser, 2007. [Online]. Available: https://www.ocf.berkeley.edu/~marsy/resources/gnss/A%20SoftwareDefined%20GPS%20and%20Galileo%20Receiver.pdf
[14] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navigat. Observ.*, vol. 2012, pp. 1–16, Jul. 2012.
[15] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.
[16] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016.
[17] W. Wang, N. Li, R. Wu, and P. Closas, "Detection of induced GNSS spoofing using S-curve-bias," *Sensors*, vol. 19, no. 4, p. 922, Feb. 2019.
[18] R. E. Phelts, "Multicorrelator techniques for robust mitigation of threats to GPS signal quality," Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 2001.
[19] O. M. Mubarak and A. G. Dempster, "Performance comparison of ELP and DELP for multipath detection," in *Proc. 22nd Int. Tech. Meeting Satell. Division Inst. Navigat.*, Savannah, GA, USA, 2009, pp. 2276–2283.
[20] O. M. Mubarak and A. G. Dempster, "Analysis of early late phase in single- and dual-frequency GPS receivers for multipath detection," *GPS Solutions*, vol. 14, no. 4, pp. 381–388, Feb. 2010.
[21] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2011, pp. 2646–2656.
[22] A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Two-dimensional signal quality monitoring for spoofing detection," in *Proc. ESA/ESTEC NAVITEC Conf.*, Noordwijk, The Netherlands, 2016, pp. 14–16.
[23] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, and W. Feng, "GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations," *IEEE Access*, vol. 6, pp. 66428–66441, 2018.
[24] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.
[25] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 1, pp. 469–475, Feb. 2019.
[26] K. Benachenhou and M. L. Bencheikh, "Detection of global positioning system spoofing using fusion of signal quality monitoring metrics," *Comput. Electr. Eng.*, vol. 92, Jun. 2021, Art. no. 107159.
[27] A. M. Khan, N. Iqbal, A. A. Khan, M. F. Khan, and A. Ahmad, "Detection of intermediate spoofing attack on global navigation satellite system receiver through slope based metrics," *J. Navigat.*, vol. 73, no. 5, pp. 1–17, Apr. 2020.
[28] A. M. Khan and A. Ahmad, "Global navigation satellite systems spoofing detection through measured autocorrelation function shape distortion," *Int. J. Satell. Commun. Netw.*, vol. 40, no. 2, pp. 148–156, Sep. 2021.
[29] C. He, "Research on evaluation methods of GNSS signal quality and the influence of GNSS signal on ranging performance," Ph.D. dissertation, Nat. Time Service Center, Univ. Chin. Acad. Sci., Nat. Time Service Center, Chin. Acad. Sci., Beijing, China, 2013.
[30] K. Steven, "Statistical decision theory I," in *Fundamentals of Statistical Signal Processing: Detection Theory*, vol. 2, 11th ed. Providence, RI, USA: PTR Prentice Hall, 1993, pp. 60–89. [Online]. Available: http://www.phptr.com
[31] C. Fernández-Prades, J. Arribas, P. Closas, C. Aviles, and L. Esteve, "GNSS-SDR: An open source tool for researchers and developers," in *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2011, pp. 780–794.
[32] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques," in *Proc. 25th Int. Tech. Meeting Satell. Division Inst. Navigt.*, Nashville, TN, USA, 2012, pp. 3569–3583.
[33] T. E. Humphreys. (Mar. 2016). *The University of Texas at Austin*. TEXBAT data sets 7 and 8. [Online]. Available: http://radionavlab.ae.utexas.edu/datastore/texbat/texbat_ds7_and_ds8.pdf
[34] A. Jafarnia-Jahromi, "GNSS signal authenticity verification in the presence of structural interference," Ph.D. dissertation, Dept. Geomatics Eng., Univ. Calgary, Calgary, AB, Canada, 2013.
[35] Y. Gao, Z. Lv, and L. Zhang, "Asynchronous lift-off spoofing on satellite navigation receivers in the signal tracking stage," *IEEE Sensors J.*, vol. 20, no. 15, pp. 8604–8613, Aug. 2020.
[36] A. J. Jahromi, A. Broumandan, S. Daneshmand, G. Lachapelle, and R. T. Ioannides, "Galileo signal authenticity verification using signal quality monitoring methods," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Barcelona, Spain, Jun. 2016, pp. 1–8.
[37] H. Cheng, M. Du, and Y. Zhao, "Two important non-central distributions of multivariate statistical analysis," *J. Guiyang College Nat. Sci.*, vol. 10, no. 3, pp. 1–4, Sep. 2015.
[38] H. Liu, "The limiting distributions of a sequence of independent chi-square distribution," *J. Jingchu Univ. Tech.*, vol. 34, no. 3, pp. 45–46, Jun. 2019.
[39] A. J. van Dierendonck, P. Fenton, and T. Ford, "Theory and performance of narrow correlator spacing in a GPS receiver," *Navigation*, vol. 39, no. 3, pp. 265–283, Sep. 1992.
[40] A. Ranganathan, "Physical-layer techniques for secure proximity verification & localization," Ph.D. dissertation, Dept. Sci. Elect. Electron. Eng., ETH Zurich, Zurich, Switzerland, 2016.

Wenlong Zhou received the B.S. degree in navigation engineering from Information Engineering University, Zhengzhou, Henan, China, in 2020, where he is currently pursuing the M.S. degree.

He has published several articles on satellite navigation data processing and satellite navigation anti-spoof technology. His current research interests include satellite navigation signal processing and satellite navigation spoofing countermeasures.

Zhiwei Lv received the Ph.D. degree in space geodetic survey and navigation from Information Engineering University, Zhengzhou, Henan, China, in 2010.

He is currently a Professor at Information Engineering University. He has published several articles on satellite navigation data processing and space geodetic surveys. His current research interests include satellite navigation data processing and space geodetic surveys.

Xu Deng received the B.S. degree in navigation engineering from Information Engineering University, Zhengzhou, Henan, China, in 2019, where he is currently pursuing the M.S. degree.

He has published several papers on satellite navigation data processing and anti-spoof technology. His current research interest includes satellite navigation spoofing countermeasures.

Ye Ke received the B.S. degree in software engineering from East China Jiaotong University, Nanchang, Jiangxi, China, in 2015. He is currently pursuing the M.S. degree with Information Engineering University, Zhengzhou, Henan, China.

He has published several articles on satellite navigation data processing and satellite navigation anti-spoofing technology. His current research interest includes satellite navigation anti-spoofing technology.