Robust Spoofing Detection for GNSS Instrumentation Using Q-Channel Signal Quality Monitoring Metric

Chao Sun, Joon Wayn Cheong, *Member, IEEE*, Andrew G. Dempster, *Senior Member, IEEE*, Hongbo Zhao, *Member, IEEE*, Lu Bai, and Wenquan Feng, *Member, IEEE*

***Abstract*— Signal quality monitoring (SQM) has been proven to be a simple and effective means for the detection of spoofing attacks for global navigation satellite system (GNSS) instruments. Some prevalent SQM metrics include Ratio and Delta metrics. However, such SQM metrics have inherent defects, such as limited spoofing detection accuracy and low robustness due to the false alarms caused by environmental effects, such as multipath. The construction of conventional SQM metrics is mainly based on the in-phase correlator outputs in the tracking loop of a GNSS instrument. It is known that the interaction between spoofing and authentic signals will cause leakage of correlation energy to the quadrature channel. This article proposes a new SQM metric using this abnormal quadrature channel energy as the primary indicator. A spoofing and multipath discrimination scheme based on intersatellite cross-check is further developed. The detection performance of the quadrature channel-based SQM metric is verified in spoofing and multipath scenarios using the well-known Texas Spoofing Test Battery (TEXBAT) dataset and real multipath data collected in Beihang University, respectively. Results demonstrate that the proposed method achieves a higher than 95% detection rate for the TEXBAT Scenario 2 with P_{fa} of 10^{-2} and an averaging time of 4 s, showing better detection sensitivity and robustness compared with conventional I-channel SQM metrics.**

***Index Terms*— Global navigation satellite systems (GNSSs), multipath, Q-channel, signal quality monitoring (SQM), spoofing detection.**

I. Introduction

GLOBAL navigation satellite systems (GNSSs) have been extensively used to provide position, velocity, and time (PVT) information for civil and military users. Critical infrastructure, such as telecommunication networks and electric distribution systems [1], [2], also rely heavily on the time and frequency synchronization from GNSS. Therefore, GNSS has become a globally available and vital time and space reference.

However, GNSS is vulnerable and is easily interfered with by spoofing or multipath effects because of its open signal structure and low signal power [3], [4]. The positioning and timing capability of GNSS are based on precisely measuring the signal propagation delay from satellites to a GNSS-capable instrument. Deliberate spoofing can lead the target GNSS instrument imperceptibly to generate false position solutions or time information by transmitting a set of counterfeit GNSS signals to replace the authentic signals in the target GNSS instrument [5], [6]. It severely threatens the security and integrity of civil GNSS applications. Therefore, the development of countermeasures against spoofing threats has attracted significant interest in the GNSS community.

Previous work has reviewed the state of the art for spoofing detection and mitigation techniques [5]. The performance of GNSS timing under spoofing conditions is studied, and the effectiveness of various techniques to enhance receiver robustness is tested [7]. Here, we generalize the spoofing detection methods into two main categories.

The first category is the receiver autonomous spoofing detection methods using a single antenna. They can be implemented either in the code and carrier tracking loops or after the GNSS pseudorange measurements have been produced. The former methods detect spoofing by utilizing specific features of the counterfeit signals. Such methods include signal quality monitoring (SQM) [8]–[17] and its variant—the moving variance-based method [18], [19], C/N0 monitoring [20], [21], Doppler anomaly monitoring [22], subspace projection [23], and distribution checks of correlator outputs [24], [25]. The latter methods perform consistency checks among different measurements, such as ephemeris data or clock offset change [26]. Wang and Hespanha [2] proposed an antispoofing approach by checking the update consistency with histories and across distributed nodes in phasor measurement units (PMUs)

The other category relies on external measurement assistance, such as requiring an antenna array [27]–[30], GNSS/INS integrated navigation, and dual-receiver correlation [31]. Methods in this category achieve good antispoofing capability;

Manuscript received March 8, 2021; revised July 20, 2021; accepted July 26, 2021. Date of publication August 5, 2021; date of current version August 26, 2021. This work was supported in part by the Youth Program of National Natural Science Foundation of China (NSFC) under Grant 62001015 and Grant 61901015, in part by the China Postdoctoral Science Foundation under Grant 2020M670095, and in part by the Australian Research Council (ARC) Linkage Funding under Grant LP140100252. The Associate Editor coordinating the review process was Jingyu Hua. *(Corresponding author: Hongbo Zhao.)*

Chao Sun, Hongbo Zhao, Lu Bai, and Wenquan Feng are with the Department of Electrical and Information Engineering, Beihang University, Beijing 100191, China (e-mail: sunchao@buaa.cn; bhzhb@buaa.edu.cn; lubai@buaa.edu.cn; buaafwq@buaa.edu.cn).

Joon Wayn Cheong and Andrew G. Dempster are with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 1466, Australia (e-mail: cjwayn@unsw.edu.au; a.dempster@unsw.edu.au).

Digital Object Identifier 10.1109/TIM.2021.3102753

especially, GNSS integrated with INS or LiDAR can effectively bridge GNSS outages because of spoofing or blocking [32]–[34]. The algorithm complexity and hardware cost are both high, which limits their applications. In addition, some other approaches have also been found to be effective for spoofing detection and mitigation, such as cryptographic modulation of the civil GNSS signals [35], multimodal detection [36], and parameter measurement methods [37], [38].

The SQM technique is much favored for multipath and spoofing detection due to its simplicity and efficacy [39]. The SQM metrics are measured using the outputs of correlators already implemented in all code tracking loops in GNSS instruments, requiring no external dependencies. To effectively detect the distortion of the correlation function, different SQM metrics have been developed. The Delta test metric and the Ratio test metric are two of the representatives of the SQM techniques [40]. Cavaleri *et al.* [9] analyzed the effect of a spoofing attack on code and carrier tracking and explained the strategy to apply the Ratio test metric. Detailed performance assessments related to the Ratio or Delta metric have been done over a set of spoofing scenarios [10]. A kind of early late phase (ELP) SQM metric was also developed by detecting the phase difference of early and late correlators under spoofing [11]. Jahromi *et al.* [12] evaluated the effect of interaction between authentic and spoofing signals on correlator outputs in a typical Galileo receiver. Different code domain-based SQM metrics were used to detect a distorted correlation peak during a spoofing attack. Yang *et al.* [13] investigated the effect of different factors on spoofing detection performance using SQM metrics, such as the number of correlators in multicorrelator mode and the signal-to-noise ratio (SNR). Pini *et al.* [14] developed spoofing detection techniques based on combining the Ratio test with some extra pairs of correlators for spoofing detection. In addition, the SQM technique was also combined with distortion monitoring to distinguish spoofing from multipath and jamming [15] but at the expense of an additional power monitoring module. The false alarm rate was acceptable for a single channel but not low enough when detection was carried out over multiple channels. Maximum-likelihood estimation was used in [16] to improve the method in [15], but it required at least 11 correlator outputs to maintain a reasonable level of theoretical detection performance, which increases computational complexity.

The authors' previous work [17] investigated multiple SQM metric joint detection. Three conventional SQM metrics, i.e., Delta, Ratio, and ELP, are considered. The core of [17] is to derive the generalized expression of SQM metrics and, on this basis, develop strategies of combining different SQM metrics to boost spoofing detection performance. However, for practical applications, the conventional SQM metrics and metric combinations based on one pair of correlators face the following two main challenges:

A. Challenge 1: Sensitivity to Varying Relative Carrier Phase

Manfredini *et al.* [10] and Sun *et al.* [17], [19] emphasize that the SQM metric-based techniques suffer from performance loss under the frequency-unlocked cases of the Texas Spoofing Test Battery (TEXBAT) dataset. Typically, we need to perform averaging over the raw SQM metric values to smooth system thermal noise. However, when a spoofing attack occurs, the raw SQM metric value will fluctuate beyond its nominal range because of the varying relative carrier phase between the authentic and the counterfeit signals. This fluctuation is nonperiodic, with a larger than usual variance statistic. An averaging operation will cover up the outliers of the SQM metric, making it less easy to detect.

B. Challenge 2: Sensitivity to Multipath Environments

In urban environments, multipath is one of the dominating error sources for GNSS applications [4], [41], [42]. Similar to spoofing, multipath can also introduce distortion of the correlation function. It may cause a false alarm in an SQM-based spoofing detection instrument and deteriorate its performance. Thus, the current SQM-based methods are not robust enough in multipath environments.

To overcome the above drawbacks and be motivated by the need for a more reliable SQM-based approach, this work proposes a new metric by measuring the Q-channel correlation energy. The novelty and contribution of this manuscript are as follows. First, we propose a new Q-channel-based SQM metric that is based on capturing the abnormal energy in the Q-channel during a spoofing attack, rather than just the I-channel amplitude (i.e., Delta and Ratio metrics) and phase difference (i.e., ELP). It is classified into the "energy" category of the SQM metric. It improves performance by averaging the raw SQM metric values. Second, an intersatellite cross-check scheme is developed to distinguish spoofing from multipath without using multiple correlators or additional power monitoring. The scheme can guarantee robustness against multipath at the expense of some acceptable computation complexity.

This article is organized as follows. Section II briefly reviews the challenges of conventional SQM metrics. In Section III, the new Q-channel SQM metric is presented. The theoretical probability of false alarm (Pfa) and threshold setting are derived. Also, an intersatellite cross-check scheme is developed to distinguish spoofing from multipath. Its ability to detect spoofing has been validated using the TEXBAT dataset and multipath data collected at Beihang University. The experiment results are given in Section IV.

II. Challenges of Conventional SQM Metric

As mentioned in Section I, the conventional SQM metrics suffer from two main problems in practical applications. This section first recalls the typical spoofing attack pattern and then gives a detailed explanation of the weakness of conventional SQM metrics to better show the motivation of this work.

A. Spoofing Attack Pattern and Signal Model

Intermediate spoofing, identified as an efficient spoofing attack method, can launch a spoofing attack without interrupting the regular functioning of a GNSS receiver. The basic principle and attack pattern have been introduced in [11] and [43]. Fig. 1 visualizes the changing process of the

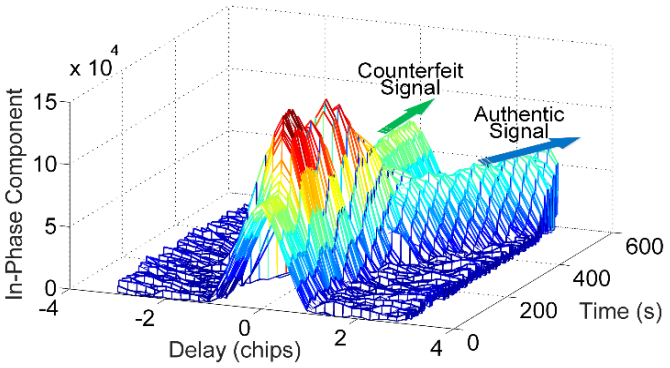

Fig. 1. Typical changing process of in-phase correlation peak under a spoofing attack.

correlation peak in the victim receiver during the spoofing attack. The typical steps of launching an intermediate spoofing attack can be concluded as three stages. In the first stage, the counterfeit signals are generated with the same code delay and Doppler shift as the authentic signal, to ensure that the fake correlation functions are perfectly aligned with the authentic ones. In the second stage, the spoofer gradually increases the power of the spoofing signals to exceed the corresponding authentic signals' power level. In the last stage, the spoofer slowly leads the counterfeit signals away from the authentic signals to manipulate the victim receiver to a wrong position.

Spoofing's effect can be characterized by three parameters: the amplitude, time delay, and phase difference of counterfeit signal relative to the authentic signal. Assuming that the incoming signal is a binary phase shift keying (BPSK) signal, it can be modeled as

$$\begin{aligned} s(t) &= s_0(t) + s_{\mathrm{sp}}(t) + \sum_{i=1}^{P} s_i(t) \\ &= Ac(t-\tau_0)\cos(w_0 t + \varphi_0) + \alpha_{\mathrm{sp}} Ac\big(t-\tau_{\mathrm{sp}}\big) \\ &\quad \times \cos\big(w_0 t + \varphi_{\mathrm{sp}}\big) + \sum_{i=1}^{P} \alpha_i Ac(t-\tau_i)\cos(w_0 t + \varphi_i) \end{aligned} \tag{1}$$

where $s_0(t)$ is the LOS with time delay τ_0 and carrier phase φ_0, $s_{\mathrm{sp}}(t)$ is the spoofing signal, and $s_i(t)$ denotes the ith multipath signal. A is the amplitude of the LOS, $c(t)$ represents the pseudorandom code. α_{sp}, τ_{sp}, and φ_{sp} denote the relative amplitude attenuation, time delay, and phase of spoofing signal. α_i, τ_i, and φ_i denote the relative amplitude attenuation, time delay, and phase for reflected path i, respectively. P is the total number of multipath signals. For the sake of brevity and clarity, the time delay τ_0 and the carrier phase difference φ_0 of the LOS are both zero, and the amplitude attenuation factor α_0 is 1.

Generally, the authentic signal, spoofing signal, and multipath signals are all down-converted and correlated with the local replica in the tracking loop. Fig. 2 illustrates the typical scheme of a tracking loop, where the I-channel correlator outputs, $I_E(t)$, $I_L(t)$, and $I_P(t)$, and Q-channel correlator outputs, $Q_E(t)$, $Q_L(t)$, and $Q_P(t)$, are generated. These correlator

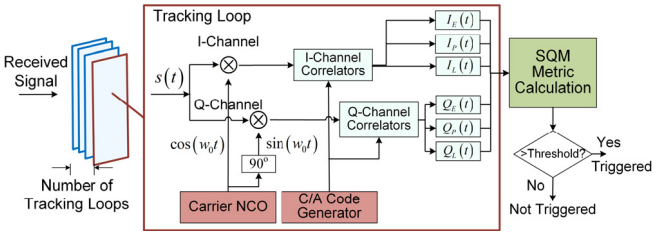

Fig. 2. Typical scheme of the tracking loop for a GNSS receiver.

outputs are then used to calculate the SQM metrics. Ignoring the noise, the complex form of normalized correlation function can be expressed as

$$\begin{aligned} R(\tau) &= R_0(\tau)e^{j\varphi_e} + \alpha_{\mathrm{sp}} R_0\big(\tau-\tau_{\mathrm{sp}}\big)e^{j\left(\varphi_e+\varphi_{\mathrm{sp}}\right)} \\ &\quad + \sum_{i=1}^{P} \alpha_i R_0(\tau-\tau_i)e^{j(\varphi_e+\varphi_i)} \end{aligned} \tag{2}$$

where φ_e denotes the difference of carrier phase between the LOS and the locally generated carrier, and $R_0(\tau)$ is the normalized autocorrelation function of an ideal BPSK modulation signal defined as

$$R_0(\tau) = \begin{cases} 1-|\tau|/T_c & |\tau|/T_c \\ 0, & |\tau|/T_c \end{cases} \tag{3}$$

where T_c denotes the chip duration. Then, the in-phase and quadrature channel correlator outputs I and Q are written as

$$\begin{aligned} I &= R_0(\tau)\cos(\varphi_e) + \alpha_{\mathrm{sp}} R_0\big(\tau-\tau_{\mathrm{sp}}\big)\cos(\varphi_e+\varphi_{\mathrm{sp}} \\ &\quad + \sum_{i=1}^{P} \alpha_i R_0(\tau-\tau_i)\cos(\varphi_e+\varphi_i) \end{aligned} \tag{4}$$

$$\begin{aligned} Q &= R_0(\tau)\sin(\varphi_e) + \alpha_{\mathrm{sp}} R_0\big(\tau-\tau_{\mathrm{sp}}\big)\sin(\varphi_e+\varphi_{\mathrm{sp}}) \\ &\quad + \sum_{i=1}^{P} \alpha_i R_0(\tau-\tau_i)\sin(\varphi_e+\varphi_i). \end{aligned} \tag{5}$$

B. Challenge 1: Sensitivity to the Varying Relative Carrier Phase

The conventional definitions of Delta and Ratio metrics are given as follows:

$$\mathrm{Delta}(t) = \frac{I_E(t) - I_L(t)}{2I_P(t)} \tag{6}$$

$$\mathrm{Ratio}(t) = \frac{I_E(t) + I_L(t)}{2I_P(t)} \tag{7}$$

where the Delta metric was designed to detect asymmetries of the correlation peak, while the Ratio test aims at detecting the presence of a "deadzone" at the top of the correlation function. Here, t means the correlator outputs are varying with time.

Spoofing is detected by comparing the value of the Delta or Ratio metric with a preset threshold. Once the threshold is surpassed, a spoofing-present decision is made. It is worth noting that spoofing detection should be used in conjunction with spoofing mitigation techniques to improve receiver robustness. In this article, we mainly focus on the topic of

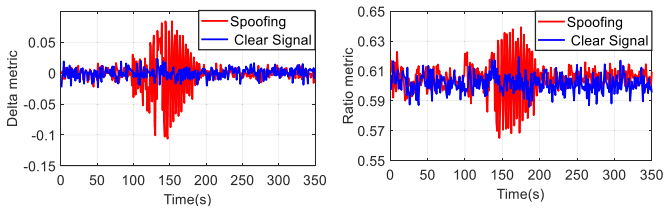

Fig. 3. Fluctuation of I-channel SQM metrics for TEXBAT Scenario 2 without averaging. Left: Delta metric. Right: Ratio metric.

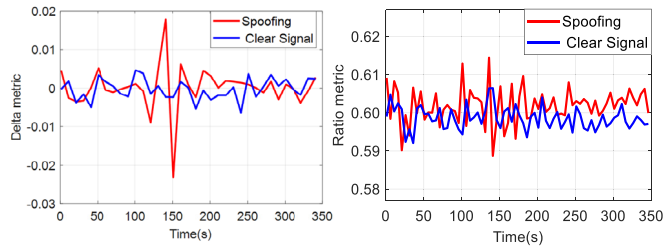

Fig. 4. I-channel SQM metrics for TEXBAT Scenario 2 after 5-s averaging. Left: Delta metric. Right: Ratio metric.

spoofing detection. Several methods have been proposed to retrieve the victim receiver's true position after spoofing is detected, such as [44] and [45]. In another of the authors' publications [45], a method using dual-receiver direct positioning was proposed. It can recover authentic GPS L1 C/A signals under spoofing and remove the spoofing effect from the victim receiver. An extra reference receiver, which is presumed to be secure, is required.

From (6) and (7), we can see that the construction of the above SQM metrics is based purely on the early, late, and prompt correlator outputs of the in-phase channel, i.e., $I_E(t)$, $I_L(t)$, and $I_P(t)$. Without any spoofing or multipath, the tracking loop ensures that all energy is maintained in the in-phase channel. The victim receiver is stably tracking the authentic signal $s_0(t)$, and φ_e is approximately equal to 0. Then, $Q(t)$ is noise only.

When spoofing is present, in most cases, this relative carrier phase φ_{sp} varies constantly and randomly. This is because it is almost impossible to implement a spoofing attack with a perfectly aligned carrier phase. As the relative carrier phase φ_{sp} is varying, the energy of the authentic-counterfeit composite signal will fluctuate. Under such conditions, the tracking loop cannot stably track the authentic signal, so φ_e is no longer 0. The correlator outputs defined by (4) and (5) also change with time. Delta and Ratio metrics, composed of I-channel correlator outputs, will fluctuate around a mean value. Significant oscillations can be observed in the metrics due to the drifting carrier phase that stops the SQM-based detection instrumentation providing stable spoofing detection performance. Even worse, the effect of oscillation on the metric is like system noise, so the operation of averaging noise also reduces the abnormal amplitude of each SQM metric, deteriorating the performance of the spoofing detection instrumentation.

Fig. 3 shows the time-domain transient responses for the conventional I-channel Delta and Ratio metrics to a

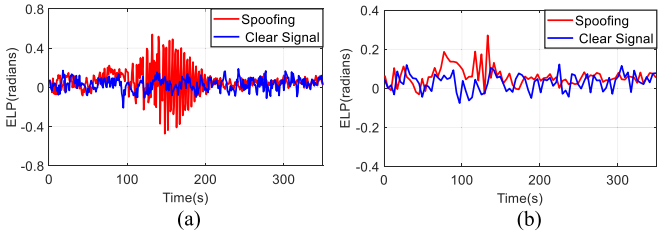

Fig. 5. Value of ELP metric for TEXBAT Scenario 2 (a) without averaging and (b) after 5-s averaging.

frequency-unlocked spoofing attack (TEXBAT Scenario 2). The y-axis illustrates the varying value of SQM metrics. Here, the correlator spacing d between the early or late correlator and the prompt correlator is set to 0.4 chips. When spoofing is absent, according to (3), we have $I_E(t) \approx I_L(t) \approx 0.6$, and $I_P(t) \approx 1$; then, the typical value of the Delta metric is 0, and the typical value of the Ratio metric is 0.6. However, when spoofing is present, the interaction between the authentic and counterfeit signals causes distortion of the correlation function of the admixture signal between 100 and 200 s, which results in significant fluctuations of the conventional SQM metrics around their corresponding typical values.

From Fig. 4, it can be observed that the I-channel SQM metrics after 5-s averaging become insignificant although the noise is reduced. Thus, averaging of raw SQM metrics does not achieve performance improvement.

Note that ELP is another kind of SQM metric. It is defined by

$$\text{ELP}(t) = \arctan\left(\frac{Q_E(t)}{I_E(t)}\right) - \arctan\left(\frac{Q_L(t)}{I_L(t)}\right) \tag{8}$$

where $Q_E(t)$ and $Q_L(t)$ denote the Q-channel early and late correlator outputs. Although the ELP metric contains Q-channel components, it also faces the problems that Delta and Ratio metrics face. During the interaction of spoofing and authentic signals, Q_{-d}/I_{-d} and Q_{+d}/I_{+d} both change around 0. According to the property of the arc-tangent function, the value of the ELP metric will also fluctuate around 0.

Fig. 5 illustrates the value of the ELP metric for a frequency-unlocked spoofing attack. It demonstrates our analysis above; namely, the moving averaging operation does not improve the metric detection performance. Thus, ELP faces the same challenge as Delta and Ratio metrics.

C. Challenge 2: Sensitivity to Multipath Environments

Another main challenge to an SQM-based spoofing detector is the high false alarm risk caused by environmental effects, such as multipath. As shown in Fig. 6, spoofing signals and multipath components are both replicas of the line-of-sight (LOS) component, essentially. Thus, it is highly challenging for GNSS instruments to discriminate between an overlapping spoofing correlation peak and a specular multipath scenario. More specifically, the spoofing detection flag may be raised even if GNSS instruments are operating in a multipath environment [46].

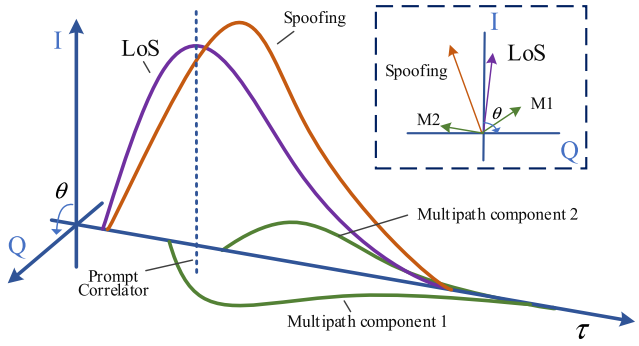

Fig. 6. Admixture of authentic, counterfeit, and multipath signals.

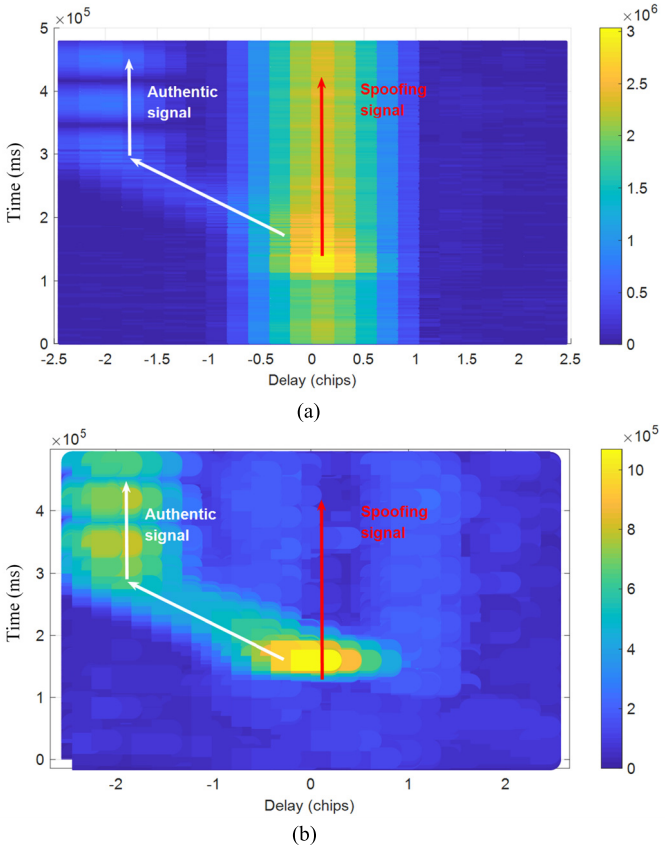

Fig. 7. Delay-temporal plot of (a) I-channel and (b) Q-channel correlation functions in the presence of a spoofing attack.

The signal models in (1)–(5) demonstrate the similarity between spoofing and multipath. The spoofing component in the correlation function (2), i.e., $\alpha_{\rm sp}R_0(\tau-\tau_{\rm sp})e^{j(\varphi_e+\varphi_{\rm sp})}$, has the same structure of that of the ith multipath component $\alpha_i R_0(\tau-\tau_i)e^{j(\varphi_e+\varphi_i)}$. Then, multipath will also trigger an SQM-based detector that is designed to detect spoofing. It should be noted that there are several differences between spoofing and multipath.

1) To guarantee the success of spoofing, the relative amplitude attenuation $\alpha_{\rm sp}$ needs to be larger than 1, while α_i is smaller than 1 since the reflection causes power loss to multipath signals as long as the LOS is not attenuated.

2) A spoofing attack tends to be continuous over time, i.e., $\alpha_{\rm sp}$ and $\tau_{\rm sp}$ generally change slowly and stably, while a multipath event might be characterized by a faster dynamic, especially in dynamic urban scenarios.

3) Typically, a successful spoofing attack attempts to spoof all visible satellite signals to mislead a target receiver into generating a false position, while, in real dynamic scenarios, the multipath tends not to affect all the satellites in view at once. In this article, the last point of difference is employed to discriminate between spoofing and multipath.

III. New Q-Channel SQM Metrics

A. Mathematical Expression

In the spoofing-absent condition, the signal energy mainly concentrates in the in-phase channel, so the Q-channel output is almost noise; whereas, in the spoofing-present condition, because of the carrier-phase difference between the authentic and spoofing signals, the Q-channel correlator output will contain some abnormal energy, as shown in Fig. 7, which can be measured to detect spoofing attacks.

In this article, we define a new SQM metric using Q-channel signal components. Its definition is given as follows:

$$m_{\rm SQM}=\frac{\sqrt{Q_{-d}^2(t)+Q_{+d}^2(t)}}{I_p(t)} \tag{9}$$

where $Q_{-d}(t)$ and $Q_{+d}(t)$ represent the early and late correlator outputs of the quadrature channel, respectively. d is the correlator spacing between early or late correlator and prompt correlator.

The essence of the proposed metric is to directly use the Q-channel energy to perform spoofing detection, and the smoothing problem is then avoided. Besides, in the spoofing-absent condition, the typical value of Q-channel energy is 0, but the typical value of I-channel energy is large and nonzero, as shown in Fig. 3. When spoofing is present, even very weak abnormal energy can immediately appear in the Q-channel. Thus, monitoring the abnormal energy within the Q-channel is much easier than monitoring within the I-channel. Therefore, we use Q-channel energy rather than that in the I-channel. In addition, the proposed SQM metric is still normalized by $I_p(t)$, which is to facilitate the detection threshold setting and comparison with other SQM metrics.

Generally, the effect of d on the proposed Q-metric is not significant. The typical value of correlator spacing d is within the range of 0.1∼0.5 chips for common GNSS receivers. When there is no spoofing or multipath, the Q-channel outputs are only noise no matter what d is. When spoofing or multipath is present, the quadrature channel early and late correlator outputs, $Q_{-d}(t)$ and $Q_{+d}(t)$, will no longer be only noise. Take early correlator output $Q_{-d}(t)$ as an example; it is defined by

$$Q_{-d}=R_0(-dT_c)\sin(\varphi_e)+\alpha_{\rm sp}R_0\big(-dT_c-\tau_{\rm sp}\big)\sin(\varphi_e+\varphi_{\rm sp})+\sum_{i=1}^{P}\alpha_i R_0(-dT_c-\tau_i)\sin(\varphi_e+\varphi_i). \tag{10}$$

When d varies, the value of $Q_{-d}(t)$ and $Q_{+d}(t)$ will change accordingly. However, other parameters, such as φ_e,

α_{sp}, τ_{sp}, $\varphi_{sp}\alpha_i$, τ_i, φ_i, and the number of multipaths P, are all changing dramatically and even randomly under real spoofing or multipath scenarios. Thus, correlation spacing d itself is not so critical for the final Q-channel SQM value. It will not overturn the comparison results between the proposed metric and other conventional metrics. Thus, for brevity, we just fix the value of d to 0.4 chips for all experiments in this article.

B. Statistical Distribution

Here, we derive the theoretical distributions of our proposed metric in the absence of a spoofing attack. This analysis can provide instructions about how to set proper detection thresholds to meet the preset false alarm probability. We first rewrite m_{SQM} as

$$m_{\mathrm{SQM}} = \frac{\sqrt{Q_{-d}^2(t) + Q_{+d}^2(t)}}{I_p(t)} = \sqrt{\left(\frac{Q_{-d}(t)}{I_p(t)}\right)^2 + \left(\frac{Q_{+d}(t)}{I_p(t)}\right)^2}. \tag{11}$$

In the normal condition, $Q_{-d}(t)$, $Q_{+d}(t)$, and $I_p(t)$ all follow Normal distribution. Thus, $(Q_{-d}(t)/I_p(t))$ and $(Q_{+d}(t)/I_p(t))$ are both ratios of two Gaussian distributed variables. Generally, the two ratios do not follow normal distributions anymore. According to the theoretical derivation in paper [17], we can obtain the conclusion that the above two ratios approximately follow Normal distributions. We directly adopt this conclusion here, and then, the next step is to derive the statistical parameters, including mean value and variance.

Based on [17, eq. (11)], for any SQM metric in the form of (x/y), its variance can be computed by

$$\sigma_{\mathrm{sqm}}^2 = \frac{1}{\mu_y^2}\sigma_x^2 + \frac{\mu_x^2}{\mu_y^4}\sigma_y^2 - 2\frac{\mu_x}{\mu_y^3}\sigma_{xy} \tag{12}$$

where μ_x and μ_y are the mean values of x and y, respectively. σ_x^2 and σ_y^2 represent the variance of x and y, respectively. σ_{xy} denotes the covariance of x and y. For easy analysis, we denote

$$\begin{cases} x = Q_{-d} \\ y = I_P \end{cases}. \tag{13}$$

When there is no spoofing, we can obtain

$$\begin{cases} \mu_x = 0 \\ \mu_y = R(0) \end{cases}. \tag{14}$$

Then, we have $\mu_1 = \mu_x/\mu_y = 0$. The covariance of x and y, σ_{xy}, can be computed by

$$\sigma_{xy} = \sigma_{yx} = E\{(Q_{-d} - E[Q_{-d}]) \cdot (I_p - E[I_p])\} = \sigma_{Q_{-d}I_p}. \tag{15}$$

As I- and Q-channel outputs can be seen as independent of each other, their covariance $\sigma_{Q_{-d}I_p}$ is equal to 0. The variance of x and y, σ_x^2 and σ_y^2, can be directly given as $\sigma_x^2 = \sigma_y^2 = \sigma_0^2$. σ_0^2 is the base variance of the postcorrelation noise given by

$$\sigma_0^2 = \frac{1}{2T_{\mathrm{int}}(C/N_0)} \tag{16}$$

where T_{int} is the coherent integration period to compute the correlation outputs. C/N_0 is the carrier-to-noise ratio of the received signal. Then, we have

$$\begin{cases} x = Q_{-d} & y = I_P \\ \mu_x = 0 & \mu_y = R(0) \\ \sigma_x^2 = \sigma_0^2 & \sigma_y^2 = \sigma_0^2 \\ \sigma_{xy} = 0 \end{cases}. \tag{17}$$

Thus, the variance of $Q_{-d}(t)/I_p(t)$ is computed as

$$\sigma_1^2 = \frac{1}{R(0)^2}\sigma_0^2 + 0 - 0 = \sigma_0^2 \tag{18}$$

while, for the other ratio $Q_{+d}(t)/I_p(t)$, we can easily obtain that its mean value μ_2 and variance σ_2^2 are also 0 and σ_0^2, respectively.

From the above analysis, we know that $Q_{-d}(t)/I_p(t)$ and $Q_{+d}(t)/I_p(t)$ approximatively follow the same Normal distribution of $N(0, \sigma_0^2)$, and the noise is independent of each other. According to the definition of the Rayleigh distribution [47], if two independent normal random variables have zero means and equal variances, then the modulus of the two variables is distributed Rayleigh. Therefore, we have that m_{SQM} follows the Rayleigh distribution for H_0 hypothesizes. Thus, we can directly obtain that the mean value of m_{SQM} is $(0.5\pi)^{1/2}\sigma_0$ and the variance is $(4-\pi)\sigma_0^2/2$ according to the properties of Rayleigh distributions. Its probability density function (pdf) is given as follows:

$$p(m_{\mathrm{SQM}}|\mathrm{H}_0) = \frac{m_{\mathrm{SQM}}}{\sigma_0^2}\exp\left(-\frac{m_{\mathrm{SQM}}^2}{2\sigma_0^2}\right), \quad m_{\mathrm{SQM}} \geq 0 \tag{19}$$

and the cumulative pdf (CDF) is written by

$$F(m_{\mathrm{SQM}}|\mathrm{H}_0) = 1 - \exp\left(-\frac{m_{\mathrm{SQM}}^2}{2\sigma_0^2}\right), \quad m_{\mathrm{SQM}} \geq 0. \tag{20}$$

Thus, for a certain threshold, m_{th}, P_{fa} can be computed as follows:

$$P_{\mathrm{fa}} = 1 - F(m_{\mathrm{th}}|\mathrm{H}_0) = \exp\left(-\frac{m_{\mathrm{th}}^2}{2\sigma_0^2}\right). \tag{21}$$

To verify the correctness of the above statistics of our proposed metric, we further run 10^4 simulation trials and plot the histograms of the Q-channel metric value in the absence of spoofing. Fig. 8 illustrates the comparison between the derived theoretical pdf curves and the histograms in the absence of spoofing. The PDF curve has been aligned with the peak of the histogram for convenient comparison. We can see that the theoretical PDF curve of the Q-channel metric is well-matched with the simulation results, which demonstrates that the estimated statistics presented above are reliable.

C. Moving Averaging

As mentioned in Section II, the averaging mechanism has the potential to boost the performance of the proposed Q-channel SQM metric. The raw Q-channel metric only captures the features and variation within one correlator output, whereas the moving averaging captures the variations and

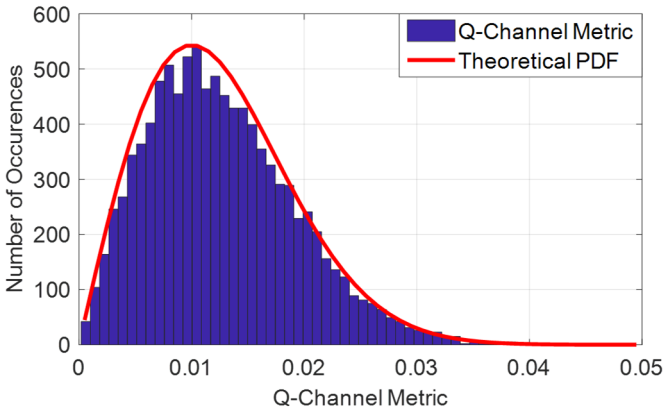

Fig. 8. Histograms and theoretical PDF curves for the proposed Q-channel metric.

features over several correlator outputs. The SQM metric after moving averaging is expressed as

$$M_Q(n) = \frac{1}{w} \sum_{i=(n-1)*k+1}^{(n-1)*k+w} m_{\mathrm{SQM}}(i), \quad n = 1, 2, \ldots, N \quad (22)$$

where w denotes the length of the sliding window to obtain a subset of data. N is the total number of such windows. The window shifts forward by a fixed sliding interval k, and the mean value is computed over these data subsets in sequence. This process is repeated over the entire dataset and, finally, creates a series of mean values.

Then, hypothesis testing can be performed on the averaged results. Although $m_{\mathrm{SQM}}(i)$ follows a Rayleigh distribution, according to the central-limit theorem, the statistical distribution of the mean value of multiple $m_{\mathrm{SQM}}(i)$, i.e., $M_Q(n)$, can be approximately regarded as a Gaussian distribution. Its mean value is identical with the original mean value of m_{SQM}, i.e., $(0.5\pi)^{1/2}\sigma_0$; its variance becomes w times the original variance of m_{SQM}, i.e., $w \cdot (4-\pi)\sigma_0^2/2$. Thus, $M_Q(n)$ approximately follows the Normal distribution of $N((0.5\pi)^{1/2}\sigma_0, w \cdot (4-\pi)\sigma_0^2/2)$.

For $M_Q(n)$, the expression of the threshold for a preset P_{fa} is given by

$$M_{\mathrm{TH}} = \sqrt{\frac{\pi}{2}}\sigma_0 + \sqrt{w \cdot (4-\pi)\sigma_0^2}\, erfc^{-1}(2 \cdot P_{\mathrm{fa}}) \quad (23)$$

where $erfc^{-1}()$ represents the inverse function of the Gauss error function. When $M_Q(n) > M_{\mathrm{TH}}$, a spoofing-presence decision is made; otherwise, a spoofing-absence decision is reached.

D. Satellite Cross-Check to Distinguish Spoofing From Multipath

In practical applications, when the Q-channel SQM metric is triggered, we need to further determinate whether it has detected multipath or spoofing. Once multipath is wrongly determined as spoofing, the spoofing detector will send out a false alarm.

However, consistency among satellites is different under spoofing and multipath environments, which can be utilized here to discriminate the two circumstances. The effect of multipath depends on the surroundings. For satellites with different elevation angles and azimuth angles, they typically suffer from multipath effects to differing extents. In addition, for a moving receiver with changing surroundings, the multipath effect on an individual satellite will also vary with time. On the contrary, the spoofer typically needs to spoof all visible satellites of the target GNSS receiver to guarantee the success of a spoofing attack. All visible signals are affected uniformly by corresponding counterfeit signals. Hence, this consistency among different satellites can be employed to distinguish spoofing from multipath.

Enlightened by the above analysis, the following strategy is presented to enhance the robustness of our proposed spoofing detector against multipath. The integral process is illustrated in Fig. 9. First, K visible satellites are stably tracked and chosen for detection. For each satellite, the Q-channel SQM metric value is calculated by (9). Then, we perform a moving averaging using (22) to obtain $M_Q(n)$. For a preset $\mathrm{P_{fa}}$, the detection threshold value M_{TH} is computed by (23). After that, $M_Q(n)$ is compared with M_{TH} to determine if the current satellite is triggered. Finally, a cross-check is carried out among K detection results. A spoofing-present decision is made if all Q-channel metrics of K visible satellites exceed their thresholds simultaneously; a multipath-present decision is made if some, but not all Q-channel metrics are triggered; a clear-signal decision is made if all Q-channel metrics are not triggered.

It should be noted that this decision strategy is effective when all visible satellites are spoofed, while, for a spoofing attack that only spoofs a small portion of visible satellites, the above strategy will be invalid. However, this kind of spoofing is not the usual case. If the spoofer only spoofs a part of visible satellites, the authentic and counterfeit signals are all tracked by the target receiver. Since the spoofer does not know exactly which satellites are finally involved in the positioning calculation, it cannot achieve full control of the target receiver. Thus, we here only consider the spoofing attack where all visible satellites are spoofed.

We also assume that spoofing and multipath are not present simultaneously. For a complex scenario where spoofing and multipath are both present, the cross-check scheme is also effective. This is because spoofing is more dangerous than multipath. As the spoofing is already present, the coexistence of multipath will not cause false alarm, but it can improve the spoofing detection probability. Thus, it is definitely acceptable in real applications.

When K satellites are used in cross-check, the overall Pfa can be simply written as

$$P_{\mathrm{fa}} = \prod_{i=1}^{K} P_{\mathrm{fa},i}, \quad i = 1, 2, \ldots, K \quad (24)$$

where $\mathrm{P_{fa},}_i$ denotes the false alarm probabilities of the SQM metrics of the ith satellite. Here, we assume the SQM metrics to be independent of each other, and $\mathrm{P_{fa},}_i$ is set to an identical value. Thus, when the overall Pfa of the cross-check-based

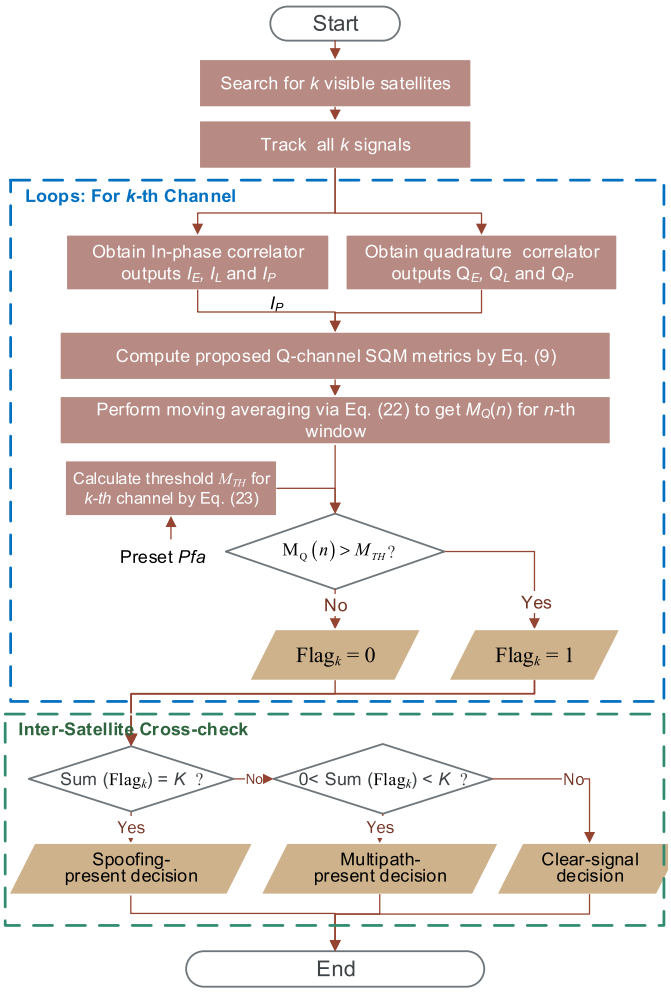

Fig. 9. Flowchart of the proposed intersatellite cross-check scheme.

spoofing detector is required to have a preset value $P_{\text{fa,set}}$, we can preset $P_{\text{fa},i} = (K)(P_{\text{fa,set}})^{1/2}$.

E. Computational Complexity Analysis

The cross-check detection algorithm can be divided into three steps: Q-channel metric calculation, moving averaging, and cross-check operation. Let C_{sqm} denote the required computational load for one-time Q-channel metric calculation. According to the definition in (9), C_{sqm} is equal to two squares, one addition, one division, and one square root calculation.

The calculation of the numerator $(Q^2_{-d}(t) + Q^2_{+d}(t))^{1/2}$ is nonlinear, which causes an increase in computational burden to some extent. However, a GNSS instrument generally performs many square root calculations in functions, such as signal detection in the acquisition stage, and noncoherent integration and phase discrimination in the tracking stage. For feasible implementation, the above calculation is typically performed in software in the microprocessor of a GNSS instrument [48]. Therefore, extra computation of $(Q^2_{-d}(t)+Q^2_{+d}(t))^{1/2}$ will not make a significant impact.

Also, to further reduce the computational load, the square root calculation can be replaced with the approximation obtained via Robertson's method [48], namely,

$$\sqrt{Q^2_{-d}(t) + Q^2_{+d}(t)} \approx \max \times \left(|Q_{-d}(t)| + \frac{1}{2}|Q_{+d}(t)|, \frac{1}{2}|Q_{-d}(t)| + |Q_{+d}(t)|\right). \quad (25)$$

Then, C_{sqm} requires only two multiplications, two additions, and one division.

In the second step, the implementation of moving averaging operation with a w-point window size requires a total of w Q-channel metric values. The moving averaging operation via (22) itself contains w-1 additions. Thus, a total of w-1 additions plus $w * C_{\text{sqm}}$ are required to judge if a visible satellite is spoofed.

In the last step, we perform cross-check over all K visible satellites. The computational load increases up to K times of the value mentioned above. The essence of the cross-check operation itself is a summation operation, namely, Sum(Flag_k). Thus, additional K-1 additions are required. Therefore, the total computational complexity $C_{\text{crosscheck}}$ for one cross-check detection contains $K(w-1)+K-1$ additions plus $wK * C_{\text{sqm}}$, namely,

$$C_{\text{crosscheck}} = (wK - 1) \quad \text{Adds} + wK * C_{\text{sqm}}. \quad (26)$$

Typically, the correlator outputs for the Q metric calculation are generated every millisecond in receivers. Thus, samples of K satellites over w ms are required for one-time cross-check detection. In real applications, the cross-check is carried out periodically to detect potential spoofing attacks in real time. In general, running the algorithm once a second is reasonable. As the detection algorithm is based on low-rate correlator outputs, rather than on intermediate frequency digital samples at a high rate, such as 40 MHz, the overall computational load is definitely acceptable and feasible for commercial devices

It is also worth noting that, even if no cross-check is implemented, the spoofing detection algorithm is still performed over all K visible satellites. Thus, the computational increase is not caused by the proposed cross-check scheme. The cross-check scheme itself only brings extra K-1 additions, which is almost negligible for the hardware, such as mobile devices or advanced high-sensitivity receivers.

IV. Hardware-Based Experiment Results

To further verify the effectiveness of our proposed Q-channel SQM for both spoofing and multipath detection, we evaluated it over a spoofing dataset and a multipath data. The spoofing dataset used in Section IV-A is the TEXBAT dataset, which was publicly provided by researchers from The University of Texas at Austin to demonstrate the vulnerability of GNSS [43]. In Section IV-B, we collected a real multipath data on the campus of Beihang University. This section presents the detailed experiment settings and corresponding evaluation results over the above datasets.

A. Spoofing Detection Using TEXBAT Dataset

In this section, we evaluate the spoofing detection performance using both conventional I-channel SQM metrics and

TABLE I
TEXBAT: SCENARIOS' SUMMARY

Scenario Description	Spoofing Type	Platform Mobility	Frequency Lock
1: Static switch	N/A	Static	Unlocked
2: Static frequency unlocked	Time	Static	Unlocked
3: Static frequency locked	Time	Static	Locked
4: Static frequency locked	Position	Static	Locked
5: Dynamic frequency unlocked	Time	Dynamic	Unlocked
6: Dynamic frequency locked	Position	Dynamic	Locked

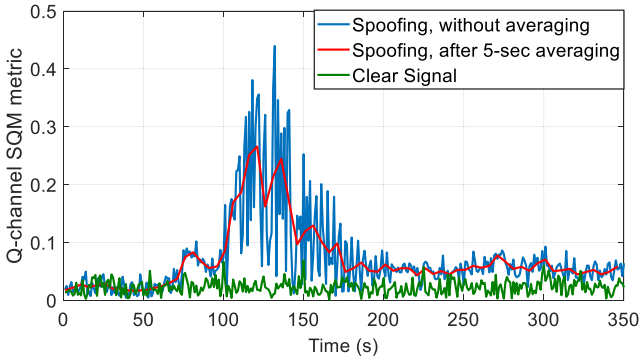

Fig. 10. Q-channel SQM metric response to the TEXBAT Scenario 2.

the proposed Q-channel metric over the TEXBAT dataset. The TEXBAT dataset is a well-known test battery of real cases publicly provided by The University of Texas at Austin. Table I lists all the six spoofing cases of the TEXBAT dataset [43]. We can see that both Scenarios 2 and 5 are for the frequency-unlocked mode, and Scenarios 3 and 6 are for the frequency-locked mode. The main difference between Scenarios 2 and 5 or between Scenarios 3 and 6 is the platform mobility. In principle, the platform mobility only minimally changes the relative phase and frequency relationship between the counterfeit signal and the authentic signal, so the performance of the proposed method over Scenarios 5 and 6 is close to Scenarios 2 and 3, respectively. For brevity, we focus the performance evaluation using Scenarios 2 and 3.

In Scenario 2, a frequency-unlocked spoofing attack is launched from 100 to 200 s. The carrier phase offset between the counterfeit and authentic signals is always changing over time. The relative code phase between the authentic signal and spoofing signal gets larger stably from 0 chips to 2 chips. After the interaction stage, the tracking loop of the target GNSS receiver eventually locks on the counterfeit signal. Scenario 3 differs from Scenario 2 in which the initial relative carrier phase between counterfeit signal and its authentic counterpart is fixed. It continues to maintain this fixed carrier phase offset even if the code phase of the counterfeit signal shifts.

The time-domain transient responses for the proposed Q-channel SQM metric to a frequency-unlocked spoofing attack are illustrated in Fig. 10. The interaction between the authentic and counterfeit signals causes the increase of metric amplitude reflecting abnormal signal fluctuations between 100 and 200 s. Notice that, for the intervals prior to 100 s and after the 200-s mark, the final metric values maintain steady behavior. This is because either the authentic signal or the counterfeit signal is locked in by the tracking loop. Also, we can see that, when the raw SQM values are averaged for 5 s, the transient response becomes more detectable and smoother, which represents more stable and outstanding spoofing detection.

B. Performance Evaluation via Receiver Operation Characteristic Curves

To evaluate the spoofing detection performance of the Q-channel SQM method, we plot the receiver operation characteristic (ROC) curves of the proposed method and compare them with those of the conventional Delta, Ratio, and ELP metrics. The ROC curve is a graphical tool for investigating the discriminatory power of a detection method. As shown in Fig. 11, the vertical axis represents the spoofing detection probability of a metric, while the horizontal axis represents predefined false alarm probability. For a good detector, the ROC curve will close to the top left corner of the figure as much as possible. The signal segment to calculate ROC curves is from 80 to 250 s. It is obvious that the conventional Delta, Ratio, and ELP metrics have very similar ROC performance for a spoofing scenario in the frequency unlock mode. The overall detection rates of the three SQM metrics are far from satisfactory for practical applications, whereas the proposed Q-channel SQM metric outperforms the conventional SQM metrics in terms of spoofing detection.

Also, the performance of the Q-channel SQM metric increases with increasing averaging time. When the averaging time is set to 4 s, the probability of detection is more than 95% for P_{fa} of 10^{-2}. This means that it can better employ moving averaging to improve detection probability and, thus, outperforms conventional SQM metrics. On the contrary, the conventional SQM metrics, i.e., Delta, Ratio, and ELP metrics, obtain little performance gain by increasing averaging time.

Furthermore, we evaluated the performance of the proposed method under the frequency-locked scenario, i.e., TEXBAT scenario 3. The comparison between Scenarios 2 and 3 helps us analyze the effect of the relative carrier phase on detection performance. Fig. 12 illustrates ROC curves for the frequency-locked case in an identical setup as in Fig. 11. Since the drift problem of the relative carrier phase between spoofing and authentic signals is largely relieved in this scenario, the conventional metrics do not suffer from value fluctuation due to the drifting relative carrier phase. Thus, the three conventional metrics achieve a higher detection probability compared with the corresponding results in Fig. 11. Also, as the averaging time gets larger from 1 to 4 s, the detection probability of the Ratio metric increases slightly from 0.7 to 0.8 for $P_{\text{fa}} = 0.1$. This means that the averaging operation is slightly effective for boosting the detection probability under the frequency-locked scenario, whereas, for Delta and ELP metrics, the effect of moving averaging is insignificant.

It can also be observed from Fig. 12 that the proposed Q-channel SQM metric still exhibits better detection capability

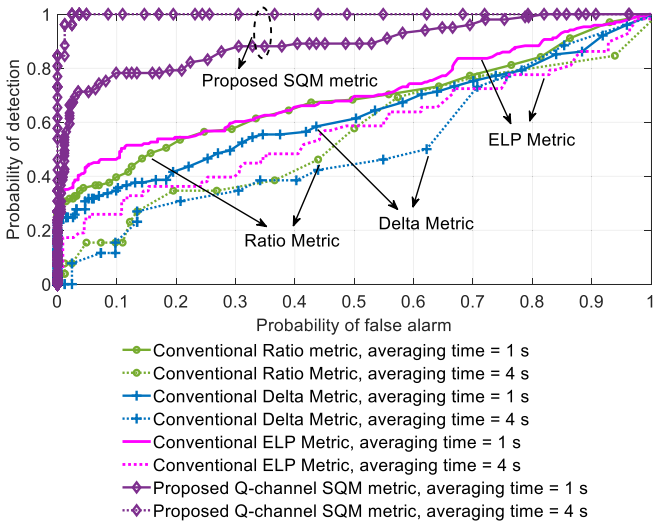

Fig. 11. ROC performance comparison for TEXBAT Scenario 2 (frequency-unlocked mode).

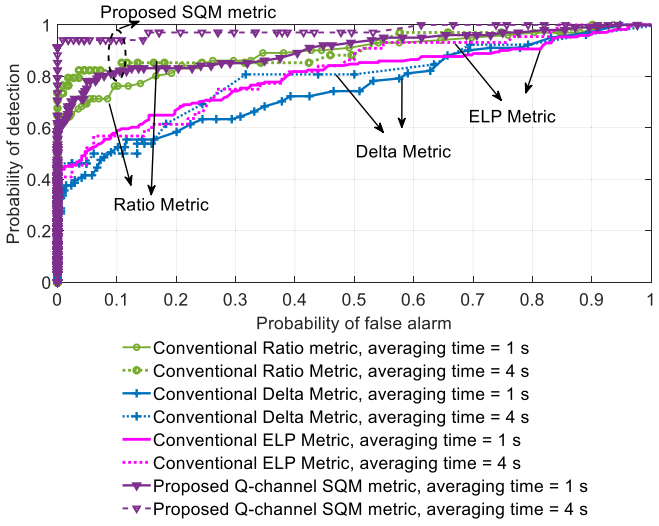

Fig. 12. ROC performance comparison for TEXBAT Scenario 3 (frequency-locked mode).

than the conventional SQM metrics. Especially, for the case of averaging time = 4 s, it achieves a detection probability of more than 0.9 for $P_{\text{fa}} = 0.01$. Thus, the Q-channel SQM metric is still the optimal metric for frequency-locked scenarios.

C. Multipath Detection Performance Using Beihang Multipath Dataset

As mentioned above, multipath and spoofing signals have very similar mathematic models. Thus, the proposed Q-channel SQM metric is also effective for multipath detection. To validate its performance under multipath circumstances, we collected real GPS L1 coarse/acquisition (C/A) code signals with a GNSS data collector. It can down-convert the received signals to an intermediate frequency, digitally sample them, and then store the raw data into a hard disk for postprocessing. The detailed parameter settings of the GNSS data collector are given in Table II. The sampling rate is set to 40 MHz, and the two-sided signal bandwidth is $4 * 2.046$ MHz. The total signal length is 250 s. Finally, a software-defined radio (SDR) GNSS instrument is utilized to process the data and test the proposed SQM metric at a correlator output rate of 1000 correlations/s. It is a modified version of a well-known MATLAB GPS software receiver developed by Borre *et al.* [49].

TABLE II
PARAMETER SETTINGS OF THE DATA COLLECTOR

Parameters	Value
A/D sampling rate	40 MHz
Data-width	4 bits
GNSS Signal	GPS L1 C/A code
Frequency Point	L1: 1575 MHz
Two-sided signal bandwidth	4*2.046 MHz
Signal Length	250 seconds

The surroundings of the signal collection site are illustrated in Fig. 13. It is in the playground of Beihang University, Beijing. The clear signals were collected at Position A, the center of the playground. The reflections and obstructions from buildings and trees are avoided to the most extent. On the west of the playground, there is the spectator stand. As no equipment can be used to get precise knowledge of multipath for each satellite, we designed the following multipath data collection experiment. The multipath data were collected by moving the signal collector along the spectator stand from Point B to Point C. This can guarantee that only visible satellites in the western sky can be affected by multipath since there is a spectator stand on the west. The satellites in the other directions will not be affected severely by multipath. It helps us judge whether the multipath detection results are correct.

The positioning results and sky plot are illustrated in Fig. 14. Fig. 14(a) shows the coordinates variations in the native coordinate system, i.e., the East North Up (ENU) system. We can see that the coordinates in the east and up directions fluctuate around 0, which means that the data collector kept still in east and height directions, while the coordinate in the north direction increases from –65 to 65 m, which means that the data collector moved north for about 130 m. The positioning results are then illustrated in Fig. 14(b). They are distributed along a straight line of length 130 m in the south–north direction. The mean position is also marked with the red plus sign in the center of the figure. The coordinates of latitude and longitude of the mean position are also given in Fig. 14(b). Fig. 14(c) illustrates the sky plot. A total of five satellites are visible at the relevant moment. The pseudorandom noise (PRN) 14 and PRN 32 are in the northwestern sky. Because of the obstruction of the spectator stand, the satellites in the western sky with elevation angles smaller than 40° are invisible. The rays transmitted by PRNs 14 and 32 are reflected by the spectator stand's uneven surface. Thus, they suffer from the multipath effect, whereas the signal of PRN 12 is LOS from the perspective of the user receiver, so it is almost free from the influence of multipath.

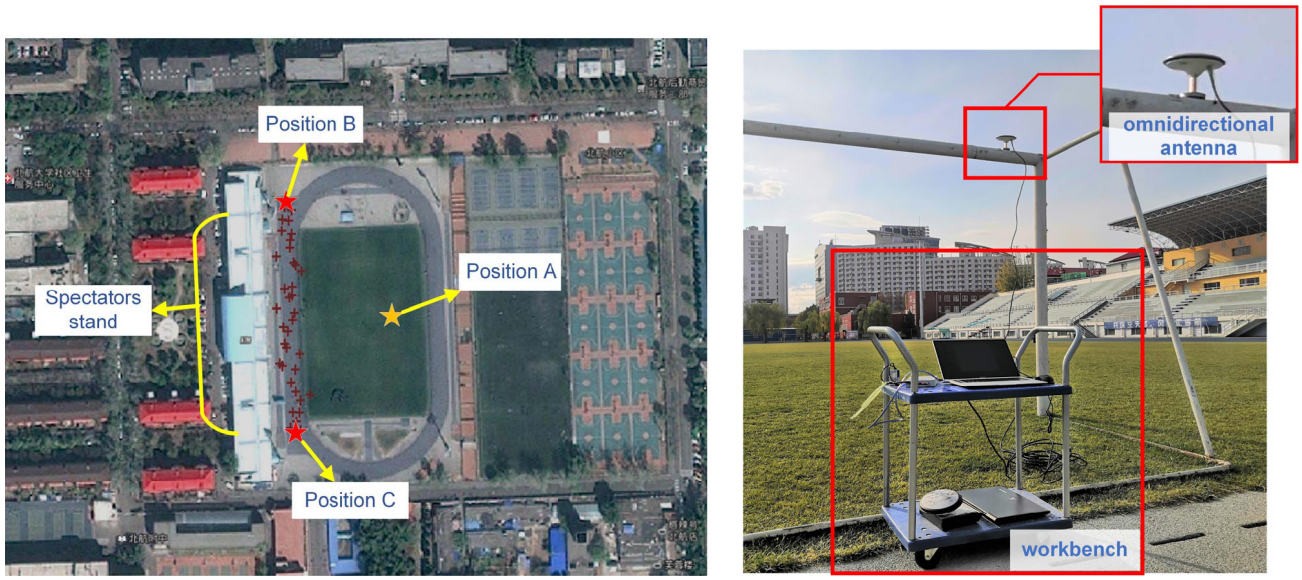

Fig. 13. (a) Multipath data collection workbench. (b) Scene of multipath data collection experiment.

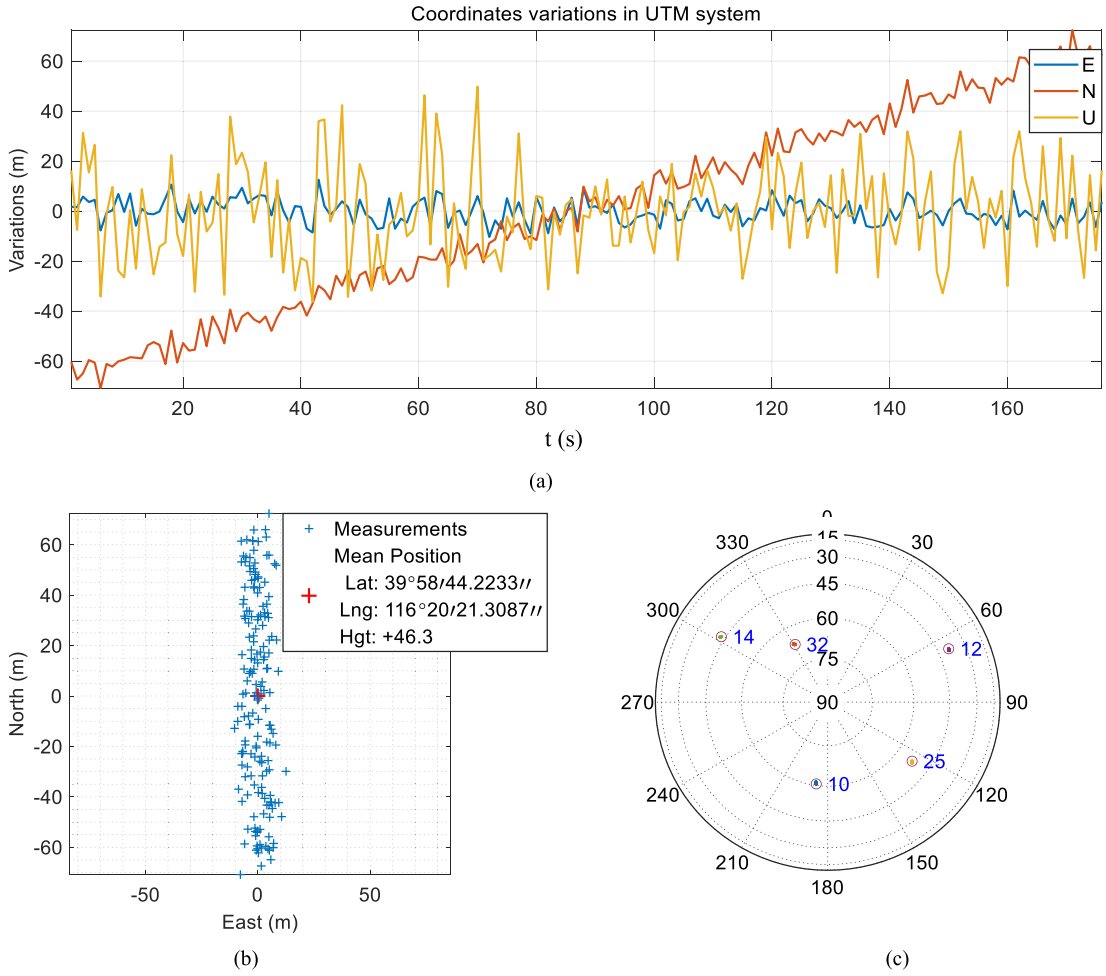

Fig. 14. Positioning results and sky plot of the Beihang multipath data. (a) Coordinates variations in the ENU system. (b) Estimated positions in the UTM system. (c) Sky plot (mean PDOP: 5.3588).

The above analysis is confirmed by the time-domain transient responses of the Q-channel metric in Fig. 15. It is obvious that the value of the Q-channel metric for PRN 14 is much larger than the case of clear signal. Thus, PRN 14 suffers from severe multipath because the spectator stand on the west of the playground reflects the signals. In contrast, the signal

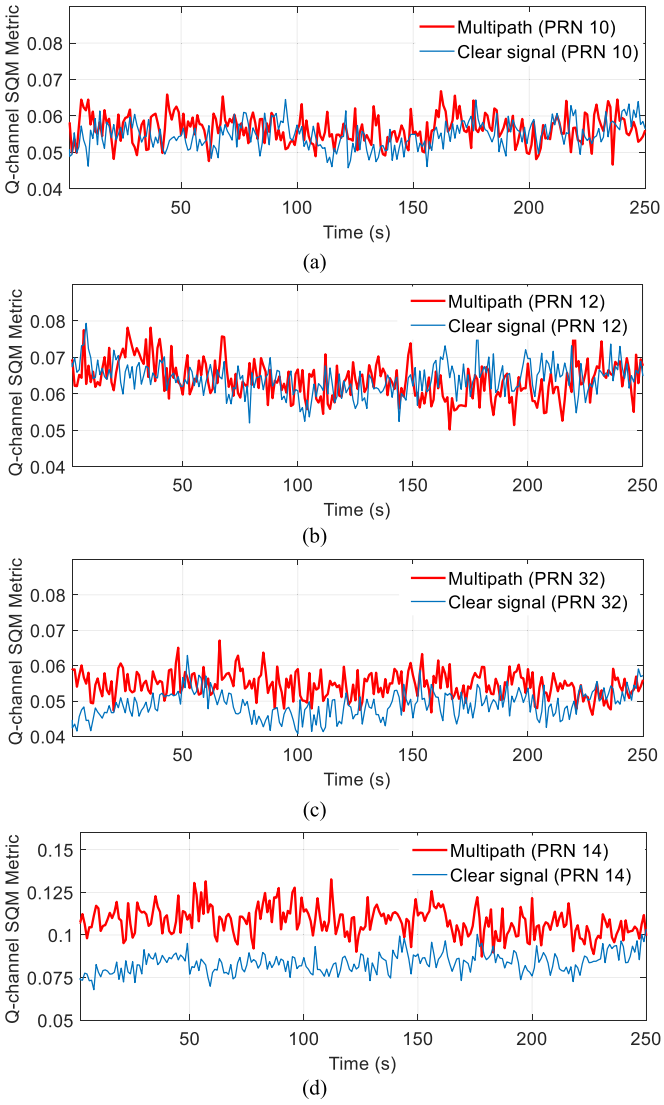

Fig. 15. Time-domain transient responses of the Q-channel metric for four different visible satellites. (a) PRN 10 (elevation angle = 61°). (b) PRN 12 (elevation angle = 40°). (c) PRN 32 (elevation angle = 67°). (d) PRN 14 (elevation angle = 42°).

quality of PRN 12 is not affected by multipath although it has almost the same elevation angle as PRN 14. That is because PRN 12 is in the eastern sky. It is quite open with no obstructions. In this case, the proposed Q-channel SQM metric successfully identifies the multipath.

Fig. 16 shows the ROC curves calculated using PRN 14 of the multipath dataset. Similar to the results of the spoofing dataset, the proposed Q-channel SQM metric shows a significant performance advantage over the conventional I-channel ratio and delta metrics. Especially, when the averaging time is set to 4 s, the detection probability of the Q-channel metric is almost 100% for P_{fa} larger than 0.05. Thus, the Q-channel metric exhibits high multipath detection capability.

Considering PRN14 is severely affected by multipath, the multipath mitigation can be implemented by removing PRN 14 from the positioning solution calculation. The estimated positions with and without removing PRN 14 are shown in Fig. 17. It is obvious the distribution of estimated positions

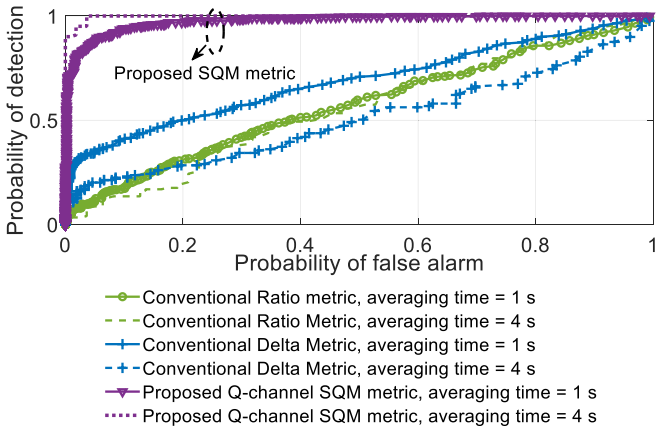

Fig. 16. ROC performance comparison for the Beihang multipath dataset (PRN 14).

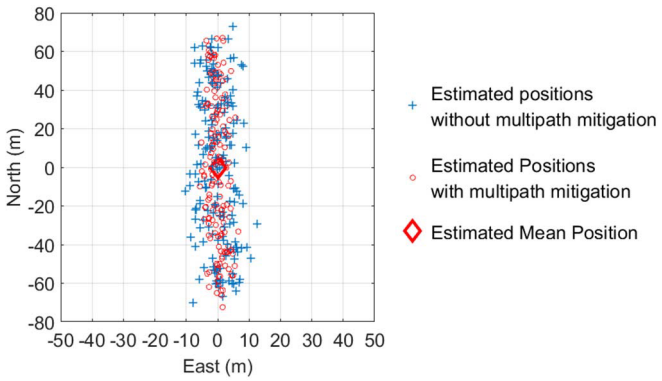

Fig. 17. Comparison of estimated positions with and without removing PRN 14.

at every moment after removing PRN 14 is more centralized compared with the results without multipath mitigation.

D. Cross-Check to Enhance Detection Robustness

Furthermore, we tested the performance of the cross-check scheme on the TEXBAT dataset and the Beihang multipath data. Two experiments were carried out. In the first experiment, we evaluate the results of cross-check with two satellites. For the multipath scenario, PRN 14 and 12 are employed for evaluation, where PRN 14 has an azimuth angle of 302° and PRN 12 has an azimuth angle of 65°. The azimuth angle difference between the two PRNs is about 237°, which is relatively large, while, for spoofing, we choose PRNs 13 and 23 of Scenario 2 for evaluation. P_{fa} in the tests is set to 10^{-3}, and the averaging time is set to 2 s uniformly.

From Fig. 18(a), we can see that PRN 14 flags a spoofer detection in most epochs but is, in fact, most likely triggered by multipath. It results in a 90.3% false alarm rate for a spoofing detector, which is unacceptably high. However, when cross-check is performed using both PRNs 12 and 14, the false alarm is significantly suppressed, as shown in Fig. 18(b). In contrast, Fig. 18(c) and (d) illustrates that the overall detection ratio after cross-check is maintained at 100% during a spoofing attack (true spoofing onset occurs from 100 to 170 s).

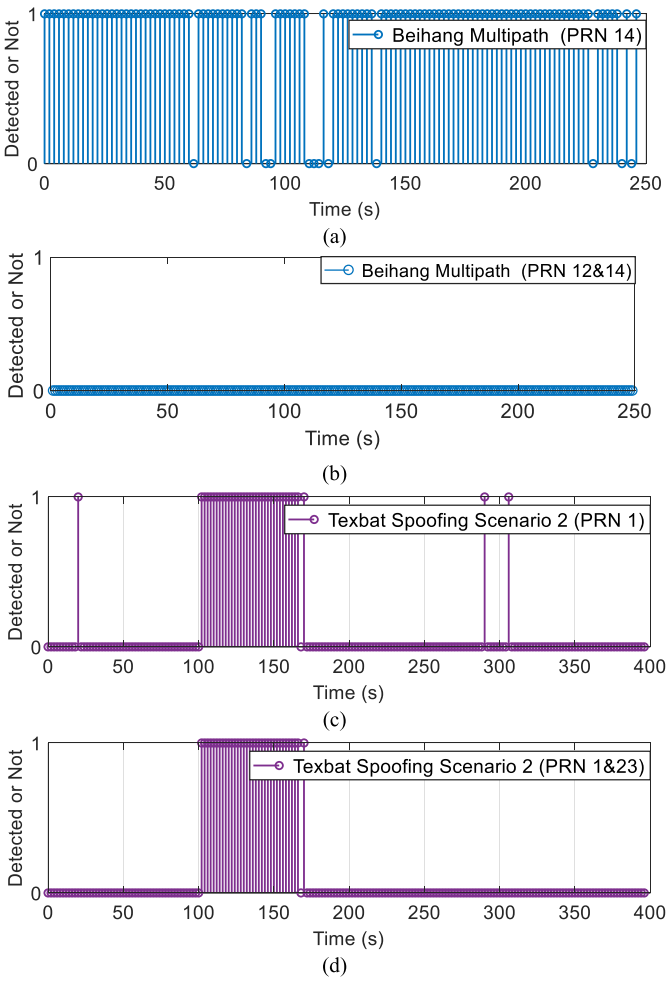

Fig. 18. Changes of detection results over time under the Beihang multipath scenario (a) without cross-check, (b) with cross-check and the frequency-unlocked spoofing scenario, (c) without cross-check, and (d) with cross-check.

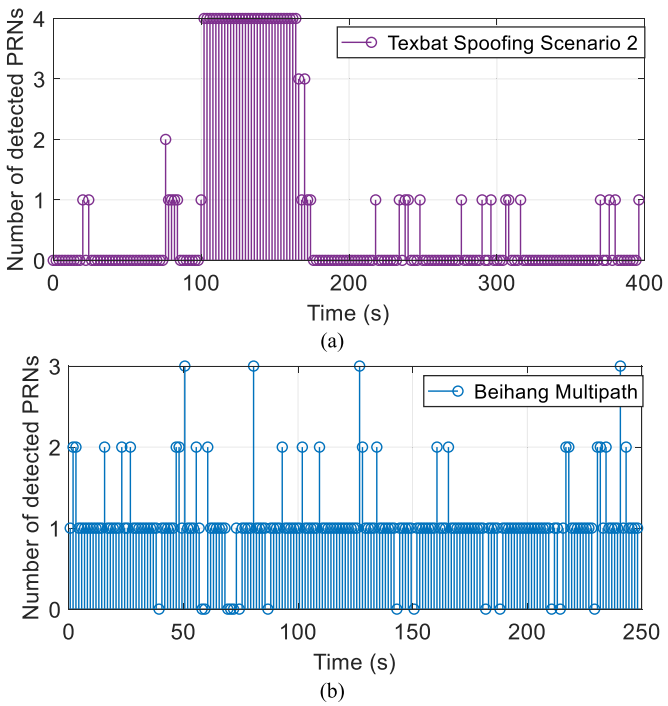

Fig. 19. Number of triggered satellites versus time for (a) spoofing-only scenario (TEXBAT Scenario 2) and (b) multipath-only scenario (Beihang multipath scenario).

TABLE III
CLASSIFICATION ACCURACY FOR TWO SPOOFING SCENARIOS AND MULTIPATH SCENARIO

Data Type \ Decision		Spoofing -presence	Multipath -presence	Clear signal
Spoofing: TEXBAT S2	PRNs 3, 6, 13, 23	**93.33%**	6.67%	0%
Spoofing: TEXBAT S3	PRNs 13, 19, 10, 16	**81.57%**	18.43%	0%
Multipath	PRNs 14, 12, 10, 32	**0%**	92.46%	7.54%
Clear Signal	TEXBAT 2 + TEXBAT 3 + Multipath	**0%**	4.12%	95.88%

It demonstrates that the cross-check still maintains the high spoofing detection capability with the assumption that all visible satellites will be spoofed indiscriminately in a spoofing attack. Therefore, the cross-check between satellites can be an effective means for the proposed Q-channel SQM-based spoofing detector to mitigate the false alarm caused by multipath.

In the second experiment, all four satellites involved in positioning calculation are used for cross-check. When more than two satellites are used for joint detection, the misclassification probability of multipath as spoofing is further reduced using this cross-check operation.

Fig. 19 counts the total number of triggered Q-channel metrics for TEXBAT Scenario 2 and the Beihang multipath scenario. We can see from Fig. 19(a) that all four satellites are detected during the period from 100 to 170 s, where, in fact, there is a spoofing attack. In some epochs, only one, two, or three satellites are triggered, which we classify as multipath. For the epochs where zero satellites are triggered, they will be classified as a clear signal. For the multipath-only scenario shown in Fig. 19(b), all had less than four triggered satellites; hence, no epochs were wrongly classified as spoofing.

The classification accuracy evaluated over all epochs of Fig. 19 is summarized in Table III. The evaluation duration for two spoofing scenarios is from 100 to 170 s. The correlator spacing to measure the Q-channel metric is 0.4 chips, and the averaging time is set to 2 s uniformly. The number of satellites in-view N is 4. Take spoofing scenario TEXBAT S2 as an example, the Q-channel SQM metrics corresponding to GNSS signals with PRN numbers 3, 6, 13, and 23 are employed jointly for cross-check.

It is worth noting that we set P_{fa} for each Q-channel metric in this test to 10^{-2}. For the spoofing-present decision, the theoretical joint false alarm probability caused by noise is $(10^{-2})^N = 10^{-8}$ according to (17). For the multipath-present decision, the joint false alarm probability due to noise is $1 - (1 - 10^{-2})^N - (10^{-2})^N \approx 0.0394$. Both quantities are acceptable. If we raise the spoofing detection P_{fa} from 10^{-8} to 10^{-3}, the resulting multipath-present decision will have an unacceptably high Pfa of 54.2%. Hence, there is a

tradeoff in choosing the thresholds for the proposed intersatellite cross-check mechanism.

It can be seen from Table III that, for TEXBAT spoofing Scenario 2, 93.33% spoofing epochs are correctly classified as spoofing, and 6.67% spoofing epochs are misclassified as multipath. For TEXBAT spoofing Scenario 3, the classification accuracy drops slightly. As the spoofing attack generally lasts for 100 s or more, tens of detections (averaging time = 2 s) can be performed during this period. Thus, the classification accuracy here for a single detection is high enough for real applications. Under the multipath scenario, no multipath signal is wrongly classified as spoofing, which means that the proposed cross-check mechanism significantly reduces misclassification. The misclassification rate in Table III corroborates our theoretical calculations. In addition, the clear signals of TEXBAT Scenarios 2 and 3 and Beihang multipath data are also tested in the last experiment in Table III. The overall misclassification rate for spoofing is zero, and the misclassification rate for multipath is 4.12%. They are acceptable and consistent with the preset P_{fa}, 10^{-8}, and 3.94%, respectively.

V. Conclusion

This article proposes a new SQM metric by employing and measuring the abnormal energy in the Q-channel of the tracking loop. We verified its performance in detecting spoofing and multipath on the widely accepted TEXBAT spoofing dataset and a multipath data collected in Beihang University, respectively. Results show that conventional I-channel SQM metrics have worse detection performance due to the time-varying relative carrier phase between the authentic and the counterfeit signals (or reflected signals). The proposed SQM metric overcomes this defect showing statistically higher detection rates. When the averaging time is set to 4 s, the probability of detection under the TEXBAT Scenario 2 is larger than 95% with P_{fa} of 10^{-2}. This method is also a computationally inexpensive antispoofing technique. It is highly practical as it requires minimal modification to the baseband correlators and firmware to conventional GNSS receivers.

In addition, an intersatellite cross-check scheme was proposed to reduce the false alarm rate caused by multipath to spoofing detection. The experiments presented in Section IV-C are examples to demonstrate the effectiveness of intersatellite cross-check. Under the multipath scenario, no multipath signal is wrongly classified as spoofing when averaging time = 2 s, and four satellites are used for cross-check.

References

[1] S. Toscani, C. Muscas, and P. A. Pegoraro, "Design and performance prediction of space vector-based PMU algorithms," *IEEE Trans. Instrum. Meas.*, vol. 66, no. 3, pp. 394–404, Mar. 2017.

[2] Y. Wang and J. P. Hespanha, "Distributed estimation of power system oscillation modes under attacks on GPS clocks," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 7, pp. 1626–1637, Jul. 2018.

[3] E. Schmidt, D. Akopian, and D. J. Pack, "Development of a real-time software-defined GPS receiver in a labVIEW-based instrumentation environment," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 9, pp. 2082–2096, Sep. 2018.

[4] P. Xie and M. G. Petovello, "Measuring GNSS multipath distributions in urban canyon environments," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 2, pp. 366–377, Feb. 2015.

[5] E. Schmidt, Z. Ruble, D. Akopian, and D. J. Pack, "Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 8, pp. 2768–2784, Aug. 2019.

[6] 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.

[7] S. Honkala *et al.*, "Performance of EGNSS-based timing in various threat conditions," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 5, pp. 2287–2299, May 2020.

[8] K. Ali, E. G. Manfredini, and F. Dovis, "Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics," in *Proc. IEEE/ION PLANS*, Monterey, CA, USA, May 2014, pp. 1240–1247.

[9] 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 Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process.*, Noordwijk, The Netherlands, Dec. 2011, pp. 1–6.

[10] E. G. Manfredini, F. Dovis, and B. Motella, "Validation of a signal quality monitoring technique over a set of spoofed scenarios," in *Proc. NAVITEC*, Noordwijk, The Netherlands, Dec. 2014, pp. 1–7, doi: 10.1109/NAVITEC.2014.7045136.

[11] K. Wesson, D. Shepard, J. Bhatti, and T. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proc. ION GNSS*, Portland, OR, USA, Sep. 2011, pp. 2646–2656.

[12] 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.

[13] Y. Yang, H. Li, and M. Lu, "Performance assessment of signal quality monitoring based GNSS spoofing detection techniques," in *Proc. CSNC*. Berlin, Germany: Springer, 2015, pp. 783–793.

[14] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. Presti, "Signal quality monitoring applied to spoofing detection," in *Proc. ION GNSS*, Portland, OR, USA, Sep. 2011, pp. 1888–1896.

[15] 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.

[16] 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.

[17] 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.

[18] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, L. Demicheli, and W. Feng, "A new signal quality monitoring method for anti-spoofing," in *Proc. China Satell. Navigat. Conf.* Singapore: Springer, 2018, pp. 221–231.

[19] C. Sun *et al.*, "Moving variance-based signal quality monitoring method for spoofing detection," *GPS Solutions*, vol. 22, no. 3, pp. 1–13, Jul. 2018.

[20] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements," *Int. J. Satell. Commun. Netw.*, vol. 30, no. 4, pp. 181–191, Jul. 2012.

[21] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/N0 estimates," in *Proc. ION GNSS*, Nashville, TN, USA, 2012, pp. 2878–2884.

[22] A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Two-dimensional signal quality monitoring for spoofing detection," in *Proc. ESA/ESTEC NAVITEC*, Noordwijk, The Netherlands, 2016, pp. 14–16.

[23] S. Han, L. Chen, W. Meng, and C. Li, "Improve the security of GNSS receivers through spoofing mitigation," *IEEE Access*, vol. 5, pp. 21057–21069, 2017.

[24] A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver," in *Proc. ION ITM*, Newport Beach, CA, USA, 2012, pp. 790–800.

[25] M. T. Gamba, M. D. Truong, B. Motella, E. Falletti, and T. H. Ta, "Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets," *GPS Solutions*, vol. 21, no. 2, pp. 577–589, Apr. 2017.

[26] A. Jovanovic, C. Botteron, and P. A. Farine, "Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers," in *Proc. IEEE/ION PLANS*, Monterey, CA, USA, May 2014, pp. 1258–1271.

[27] E. Domínguez *et al.*, "Multi-antenna techniques for NLOS and spoofing detection using vehicular real signal captures in urban and road environments," in *Proc. ION GNSS*, Tampa, FL, USA, Sep. 2015, pp. 2966–2982.

[28] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, "Autonomous spoofing detection and mitigation in a GNSS receiver with an adaptive antenna array," in *Proc. ION GNSS*, Nashville, TN, USA, 2013, pp. 2937–2948.

[29] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 45–57, Feb. 2015.

[30] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for GNSS receiver," *IEEE Sensors J.*, vol. 18, no. 7, pp. 2952–2958, Apr. 2018.

[31] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2250–2267, Oct. 2013.

[32] S. Lu, Y. Gong, H. Luo, F. Zhao, Z. Li, and J. Jiang, "Heterogeneous multi-task learning for multiple pseudo-measurement estimation to bridge GPS outages," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–16, 2021.

[33] M. Z. Mostafa, H. A. Khater, M. R. Rizk, and A. M. Bahasan, "A novel GPS/ RAVO/MEMS-INS smartphone-sensor-integrated method to enhance USV navigation systems during GPS outages," *Meas. Sci. Technol.*, vol. 30, no. 9, p. 95103, 2019.

[34] G. He, X. Yuan, Y. Zhuang, and H. Hu, "An integrated GNSS/LiDAR-SLAM pose estimation framework for large-scale map building in partially GNSS-denied environments," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–9, 2021.

[35] K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[36] J. Li, J. Zhang, S. Chang, and M. Zhou, "Performance evaluation of multimodal detection method for GNSS intermediate spoofing," *IEEE Access*, vol. 4, pp. 9459–9468, 2016.

[37] M. R. Mosavi, Z. Nasrpooya, and M. Moazedi, "Advanced anti-spoofing methods in tracking loop," *J. Navigat.*, vol. 69, no. 4, pp. 883–904, Jul. 2016.

[38] F. Wang, H. Li, and M. Lu, "GNSS spoofing detection and mitigation based on maximum likelihood estimation," *Sensors*, vol. 17, no. 7, p. 1532, Jun. 2017.

[39] C. Sun, J. W. Cheong, A. G. Dempster, L. Demicheli, E. Cetin, and H. Zhao, "Performance assessment of multi-metric joint detection technique for anti-spoofing," presented at the IGNSS, Sydney, NSW, Australia, Feb. 2018.

[40] R. E. Phelts, "Multicorrelator techniques for robust mitigation of threats to GPS signal quality," Ph.D. dissertation, Dept. Mech. Eng., Stanford Univ., Stanford, CA, USA, 2001.

[41] B. Xu, Q. Jia, and L.-T. Hsu, "Vector tracking loop-based GNSS NLOS detection and correction: Algorithm design and performance analysis," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 7, pp. 4604–4619, Jul. 2020.

[42] G. Chen, M. Gan, C. L. P. Chen, and L. Chen, "A two-stage estimation algorithm based on variable projection method for GPS positioning," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 11, pp. 2518–2525, Nov. 2018.

[43] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GNSS signal authentication techniques," in *Proc. ION GNSS*, Nashville, TN, USA, 2012, pp. 3569–3583.

[44] 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. ITM ION*, Savannah, GA, USA, Sep. 2008, pp. 2314–2325.

[45] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, and W. Feng, "Recovering authentic global position system L1 signals under spoofing using dual receiver direct positioning," *J. Navigat.*, vol. 74, no. 4, pp. 782–800, Jul. 2021.

[46] A. Broumandan, A. Jafarnia-Jahromi, G. Lachapelle, and R. T. Ioannides, "An approach to discriminate GNSS spoofing from multipath fading," in *Proc. NAVITEC*, Dec. 2016, pp. 1–7.

[47] R. G. Gallager, *Principles of Digital Communication*. Hoboken, NJ, USA: Wiley, 2010.

[48] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications*. Norwood, MA, USA: Artech House, 2005.

[49] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, "A software-defined GPS and Galileo receiver: A single-frequency approach," in *Applied and Numerical Harmonic Analysis*. Boston, MA, USA: Birkhäuser, 2007.

Chao Sun received the B.S. degree in electronic and information engineering and the Ph.D. degree in communication and information systems from Beihang University, Beijing, China, in July 2013 and June 2019, respectively.

From 2017 to 2018, he was a Visiting Ph.D. Student with the Australian Centre for Space Engineering Research, University of New South Wales, Sydney, NSW, Australia. He currently holds a post-doctoral position at the Department of Electronic and Information Engineering, Beihang University. His research focuses on global navigation satellite system (GNSS) spoofing detection and interference mitigation techniques.

Joon Wayn Cheong (Member, IEEE) received the Ph.D. degree from the University of New South Wales (UNSW), Sydney, NSW, Australia, in 2012.

He cracked the Locata pseudolite positioning system's code and derived high-sensitivity GPS signal acquisition algorithms at UNSW. He is currently a Research Associate with the School of Electrical Engineering, UNSW, where he is currently developing the firmware for the space-qualified Namuru family of GPS/Galileo integrated receivers under the Garada and QB50 project. His other research interests in the global navigation satellite system (GNSS) field include weak signal acquisition, GNSS/pseudolite integrated signal processing, and GNSS interference and spoofing.

Andrew G. Dempster (Senior Member, IEEE) received the B.Eng. and M.Eng.Sc. degrees from the University of New South Wales (UNSW), Sydney, NSW, Australia, in 1984 and 1992, respectively, and the Ph.D. degree from the University of Cambridge, Cambridge, U.K., in 1995, all in efficient circuits for signal processing arithmetic.

He was a system engineer and a project manager for the first global positioning system receiver developed in Australia in the late 1980s and has been involved in satellite navigation ever since. He is currently the Director of the Australian Centre for Space Engineering Research, UNSW. He has published in the areas of arithmetic circuits, signal processing, biomedical image processing, satellite navigation, and space systems. His current research interests include satellite navigation receiver design and signal processing, and space systems.

Hongbo Zhao (Member, IEEE) received the Ph.D. degree in communication and information systems from Beihang University, Beijing, China, in 2012.

He is currently an Associate Professor with the Department of Electronic and Information Engineering, Beihang University. His current research interests include satellite navigation, satellite communication, and the associated signal processing techniques.

Lu Bai received the B.E. degree in electronic and information engineering from Beihang University, Beijing, China, in 2014, where she is currently pursuing the Ph.D. degree.

Her research focuses on global navigation satellite system (GNSS) antispoofing and GNSS-5G hybrid positing methods.

Wenquan Feng (Member, IEEE) received the Ph.D. degree in communication and information systems from Beihang University, Beijing, China, in 2010.

He has been teaching as the Dean of studies at Beihang University since 2011. He is currently a Professor with the Department of Electronic and Information Engineering, Beihang University. His current research interests include satellite navigation, satellite communication, and complex system fault diagnosis.