IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 27, 2018, accepted September 30, 2018, date of publication October 18, 2018, date of current version November 30, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2875948

GNSS Spoofing Detection by Means of Signal Quality Monitoring (SQM) Metric Combinations

CHAO SUN[1], JOON WAYN CHEONG[2], (Member, IEEE), ANDREW G. DEMPSTER[2], (Senior Member, IEEE), HONGBO ZHAO[1], (Member, IEEE), AND WENQUAN FENG[1], (Member, IEEE)

[1]Department of Electronic and Information Engineering, Beihang University, Beijing 100191, China
[2]The Australian Centre for Space Engineering Research, School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia

Corresponding author: Hongbo Zhao (bhzhb@buaa.edu.cn)

This work was supported by the Australian Research Council Linkage Funding under Grant LP140100252. The work of C. Sun was supported in part by the China Scholarship Council under Grant 201606020020 and in part by the Academic Excellence Foundation of BUAA for Ph.D. students.

ABSTRACT Global navigation satellite system (GNSS) signal is vulnerable and easily interfered by spoofing because of its opening signal structure and weak signal power. A signal quality monitoring (SQM) technique has been shown to be viable to detect spoofing attacks on GNSS signals. However, the effectiveness of spoofing detection employing a single SQM metric alone is limited and conditional upon the features extracted of that specific SQM metric. The complementary features among various SQM metrics can be exploited to implement joint detection to overcome the deficiency of the individual SQM metric. Motivated by this idea, this paper investigates the multi-metric joint detection technique, which combines various SQM metrics into a composite SQM metric to detect spoofing attacks. This paper proposes two combination strategies, namely amplitude combination mode and probability of false alarm combination mode (PfaM). The overall performance of different metric combinations was verified using simulations and the Texas Spoofing Test Battery dataset. Results show that the PfaM detector outperforms all single SQM metric detectors under various scenarios.

INDEX TERMS Global navigation satellite system (GNSS), joint detection, spoofing detection, signal quality monitoring (SQM).

I. INTRODUCTION

Spoofing is a kind of deliberate interference which generates a set of fake Global Navigation Satellite System (GNSS) signals to displace the authentic signals in the target receiver and finally deceive it. One of the main hazards is that the target receiver can be led almost imperceptibly into false position solutions [1]. The spoofed position can be fully controlled by the spoofer, which can threaten the security of civil GNSS users. Therefore, it is vital to develop a simple yet effective countermeasure to guard against this threat.

Many studies have focused on the spoofing detection and mitigation techniques, which can be generalized into three main categories: (1) spatial processing approaches are either based on receiver antenna array processing [2]–[5] or on a single moving antenna [6]–[8]. They achieve good anti-spoofing capability but require expensive antenna hardware or the assumption of user receiver motion; (2) baseband signal processing techniques typically work within the code and carrier tracking loops to detect the counterfeit signals by means of such as signal quality monitoring (SQM) [9]–[13], C/N0 monitoring [14], [15], Doppler anomaly monitoring [16], subspace projection [17], and distribution checks of correlator outputs [18], [19], and a moving variance-based method was also newly proposed [20], [21]; (3) post-processing techniques are implemented after the GNSS pseudo-range measurements have been produced, and consistency checks can be performed in this stage among different measurements such as ephemeris data or clock offset change [22]. 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 signal [23], multi-modal detection [24], parameter estimation methods [25], [26], and dual-receiver correlation [27].

In recent years, the SQM technique has attracted significant interest in the GNSS community. Compared to many of the other detection mechanisms mentioned previously,

SQM is much favored upon for multipath and spoofing detection due to its simplicity and efficacy and it is highly autonomous, requiring no external dependencies [28]. SQM metrics are computed from three correlator outputs that are already implemented in all code tracking loops in conventional GNSS receivers, The Early, Prompt and Late accumulators dump complex values that can be used to identify distortion of the correlation function. Various SQM metrics have been developed. Phelts first introduced two SQM techniques: Delta test metric and Ratio test metric [29]. The Delta metric aims at detecting asymmetries of the correlation peak, while the Ratio test attempts specifically to detect the presence of a 'deadzone' at the top of correlation function. They were first presented for multipath detection but recently proved to be effective for anti-spoofing by monitoring the variation of the SQM metric during the interaction stage between the counterfeit and authentic signals [30]. Detailed performance assessments related to the Ratio or Delta metric have been done over a set of spoofing scenarios [10], [11]. The Double-Delta SQM metric, which can be seen as a special Delta metric, was further developed and applied to detect the GNSS signal distortion and multipath based on the difference between two pairs of tracking and monitoring early-late correlators [31]–[34]. The early-late phase (ELP) metric was also developed for multipath detection, employing the phase difference between the early and late correlator outputs [35], [36]. It has also been verified to be a useful discriminator to detect spoofing attacks.

Reference [37] presented a PD detector by combining the SQM technique with a power distortion monitor, which makes it possible to not only detect a spoofing attack but also distinguish it from multipath and jamming. A so-called Symmetric Difference (SD) metric is used to detect distortions in the correlation peak caused by anomalous GNSS signals, including spoofing signals. In [38], a PD-ML detector was proposed to improve the SD metric in [37] by exploiting data from the additional taps to perform maximum-likelihood estimation. This method significantly improves the performance of the PD technique proposed in [37], but at the expense of additional computational complexity. At least 11 taps were needed to maintain a reasonable level of theoretical detection performance.

However, each SQM metric mentioned above has its own flaws. The Delta, Ratio and SD metrics employ the correlation outputs of the In-phase channel for detection. So, when the authentic-counterfeit composite signal fluctuates between the In-phase and Quadrature channels due to the varying relative carrier phase between the authentic signal and the counterfeit signal, the overall detection performance may deteriorate. Especially when the relative carrier phase between the authentic signal and the spoofing signal is near 0.5π or 1.5π, the Delta, Ratio and SD SQM metrics would produce near zero values. Conversely, the ELP metric achieves the maximum value at 0.5π or 1.5π but almost approaches zero when this relative carrier phase is around an integer multiple of π [36].

It is also worth noting that the experience with the spoofing testbed presented in [39] demonstrates that it is difficult to launch a carrier-phase aligned spoofing attack. If the spoofer attempts to achieve this alignment to within 1/6 of a carrier cycle, it needs the precise knowledge of the position of the target receiver antenna to about the 3 cm level for the Global Position System (GPS) L1 frequency. As the direction of movement and velocity of the target receiver are largely unknown to the spoofer, it is almost impossible to guarantee that the counterfeit signals can be perfectly carrier-phase aligned with the corresponding authentic ones. So in most cases, this relative carrier phase has to be varying constantly and randomly. Under such circumstances, using only one of Delta, Ratio or ELP metrics alone would not be optimal as they are all very sensitive to the variation of relative carrier phase as described above.

Motivated by the need for a more reliable SQM-based metric for spoofing detection, this work investigates the multi-metric joint detection technique. It is intuitive to find that the ELP and Delta or Ratio metrics are mutually complementary, which allows us to combine different SQM metrics together to make use of their respective advantages and make up for their deficiencies. Two types of combination strategy, the Amplitude combination mode (AmpM) and the Probability of false alarm (Pfa) combination mode (PfaM), are put forward and fully discussed. A generalized expression of an SQM metric is first proposed, followed by a comprehensive statistical analysis to obtain threshold values for detection and optimal scaling for the combination. Finally, the overall performance of different metric combinations is numerically verified using both simulation analysis and a real dataset called the Texas Spoofing Test Battery (TEXBAT) dataset from University of Texas [40]. It will be shown later that the PfaM combination will outperform AmpM, as well as other single metric cases.

II. SIGNAL MODEL AND SQM METRICS

Under the spoofing-free circumstances, we consider the following complex baseband model for the authentic GNSS signal after down-conversion

$$S(t) = A \cdot D(t) \cdot C(t) \cdot \exp(j\theta_a) \tag{1}$$

where $D(t)$ denotes the ± 1-valued navigation data, $C(t)$ is the pseudorandom code, and A and θ_a denote the amplitude and carrier phase of the authentic signal, respectively. Without loss of generality, we assume $D(t) = 1$, then the post-correlation model is given by

$$\begin{cases} I_d = A \cdot R(dT_c) \cdot \cos\theta_a + \eta_d^I \\ Q_d = A \cdot R(dT_c) \cdot \sin\theta_a + \eta_d^Q \end{cases} \tag{2}$$

where I_d and Q_d stand for the In-phase and Quadrature correlator outputs, respectively. T_c is the chip duration, dT_c denotes the spacing of the early (for $d < 0$) or late (for $d > 0$) correlator from the prompt correlator ($d = 0$), and d is a unitless quantity. $R(\cdot)$ is the normalized autocorrelation

function of an ideal BPSK modulation signal defined as

$$R\left(dT_c\right) = \begin{cases} 1 - \left|dT_c\right| / T_c & \left|dT_c\right| \le T_c \\ 0 & \left|dT_c\right| > T_c \end{cases} \tag{3}$$

η_d^I and η_d^Q are the Gaussian thermal noise of each channel. It is obvious that I_d and Q_d both follow a normal distribution. Assuming the residual Doppler shift error is negligible and the noise samples, η_d^I and η_d^Q, are uncorrelated. The theoretical statistics of I_d and Q_d in the absence of spoofing are as follows [12], [41]

$$\begin{cases} \mu_I = A \cdot R\left(dT_c\right) \cdot \cos\theta_a, \quad \mu_Q = A \cdot R\left(dT_c\right) \cdot \sin\theta_a \\ \sigma_I^2 = \sigma_Q^2 = \sigma_0^2 = \dfrac{1}{2T_{int}\left(C/N_0\right)}, \quad \sigma_{IQ} = 0 \end{cases} \tag{4}$$

where $\mu_I, \sigma_I^2, \mu_Q, \sigma_Q^2$ represent the mean value and variance of the In-phase and Quadrature correlator outputs, respectively, and the covariance of I-Q correlators, σ_{IQ}, is assumed to be zero. σ_0^2 is the base variance of the post-correlation noise. T_{int} denotes the coherent integration period to compute the correlation outputs. C/N_0 is the carrier to noise ratio of the received signal.

When there are spoofing attacks, the correlation peak will be distorted or asymmetric. The SQM metric then deviates from its mean value significantly which alerts us to any underway spoofing attacks. Eq. (2) can be written as

$$\begin{cases} I_d = A \cdot R\left(dT_c\right) \cdot \cos\theta_a + A \cdot \alpha \cdot R\left(dT_c - \Delta\tau\right) \\ \qquad \cdot \cos\left(\theta_a + \Delta\phi\right) + \eta_d^I \\ Q_d = A \cdot R\left(dT_c\right) \cdot \sin\theta_a + A \cdot \alpha \cdot R\left(dT_c - \Delta\tau\right) \\ \qquad \cdot \sin\left(\theta_a + \Delta\phi\right) + \eta_d^Q \end{cases} \tag{5}$$

where, the spoofing signal is characterized by the relative amplitude α, the relative code delay $\Delta\tau$ and the relative carrier phase $\Delta\phi$ with respect to the authentic signal.

A. REVIEW OF SQM METRICS

In this work, we consider three major SQM metrics: Delta, Ratio and ELP. As the SD metric in [37] and [38] is approximately equivalent to the Delta metric, for brevity, we just give the analysis of Delta metric here.

- Delta Metric

$$m_{delta} = \frac{I_{-d} - I_{+d}}{I_P} \tag{6}$$

- Ratio Metric

$$m_{ratio} = \frac{I_{-d} + I_{+d}}{I_P} \tag{7}$$

- Early Late Phase Metric

$$m_{elp} = \tan^{-1}\left(\frac{Q_{-d}}{I_{-d}}\right) - \tan^{-1}\left(\frac{Q_{+d}}{I_{+d}}\right) \tag{8}$$

where variables $I_{-\mathrm{d}}, I_{+\mathrm{d}}, Q_{-\mathrm{d}}$ and $Q_{+\mathrm{d}}$ are defined by (2) in the absence of spoofing attacks and (5) in the presence of a spoofing attack, and I_P denotes the In-phase prompt correlator with $d = 0$.

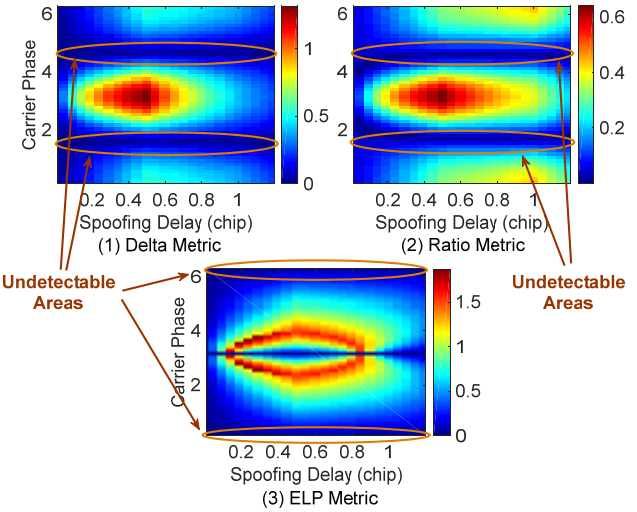


FIGURE 1. Absolute theoretical value of each SQM metric for changing code delay at various carrier phase offsets between the authentic signal and the spoofing signal attenuated by 0.8. The correlator spacing *d* is 0.5 chip.

Fig. 1 illustrates the absolute value of each SQM metric by varying relative code delay $\Delta\tau$ and the relative carrier phase $\Delta\phi$ between the authentic and counterfeit signals. Note that this diagram is also valid for line-of-sight and multipath signals. The relative amplitude α is maintained at 0.5. We can see that the expected value of each SQM metric is not uniformly distributed over the whole area. The relative carrier phase and delay have significant effect on the absolute value of the SQM metrics. The magnitude of the SQM metrics reflects the likelihood of the presence of a signal anomaly - which in this case is an indication of a spoofer.

It can be observed that the ELP metric and the other two metrics are complementary, where a region of high magnitude of one metric is a region of low magnitude for the other metric in Fig. 1. More specifically, while Delta and Ratio metrics yields a high magnitude where the relative carrier phase $\Delta\phi$ is around an integer multiple of π, the ELP metric yields a low value, and vice versa. This is because the ELP metric employs both In-phase and Quadrature components, rather than only the In-phase component (as the Delta and Ratio metrics do). During a spoofing attack, $\Delta\phi$ will vary constantly, which causes dramatical energy shifts between the In-phase component and the Quadrature component. The ELP metric reflects this variation in the Quadrature channel which makes it different from the other two SQM. Thus, the complementary feature between the ELP metric and the other SQM metrics implies that the ELP metric could be exploited together with the other SQM metrics to make the joint detection more reliable and applicable for various relative carrier phases.

B. GENERIC REPRESENTATION OF SQM METRICS

In order to set thresholds in the case of a pre-defined false alarm probability, a complete knowledge of the statistical characteristics of SQM metrics is necessary. However,

the combination of different SQM metrics in different combination ways makes it more complicated to obtain the accurate statistics. To ease analysis, this section first develops a generic representation of the SQM metrics in the absence of spoofing attacks, followed by a statistical analysis of it. It can be proved that Delta, Ratio, Double-Delta, and ELP metrics are all instances of this generic model, essentially. Then, based on the generic representation, we can not only characterize the probability distribution of different SQM metrics uniformly, but also construct various metric combinations and set the corresponding detection thresholds conveniently.

The generic representation is given by

$$m_{general} = k_1 \frac{x_1}{y_1} + k_2 \frac{x_2}{y_2} + \ldots + k_N \frac{x_N}{y_N} = \sum_{n=1}^{N} k_n \cdot r_n \quad (9)$$

with

$$r_n = \frac{x_n}{y_n}, \quad n = 1, 2, \ldots, N \quad (10)$$

The generic representation for an arbitrary SQM metric can be seen as the sum of different ratios r_n, where r_n is determined by the definition of the specific SQM metric, x_n and y_n are two Gaussian distributed variables, and N is the total number of such ratios. N is 1 for Delta metric and Ratio metric, as well as the Double-Delta metric and 2 for the ELP metric which will be further discussed in the following subsection. Variable k_n is the coefficient of r_n. The typical value is 1 or -1 for each single metric, but it could be any value for metric combinations.

Take the Delta metric as an example. According to its expression given by (6), we can set $x_1 = I_{-d} - I_{+d}$, $y_1 = I_p$, $k_1 = 1$, and $N = 1$, then the Delta metric is expressed in the form of (9), namely $m_{delta} = k_1 x_1 / y_1$. Similarly, we can also rewrite the Ratio metric as $m_{ratio} = k_1 x_1 / y_1$ with $x_1 = I_{-d} + I_{+d}$, $y_1 = I_p$, $k_1 = 1$, and $N = 1$.

As mentioned above, the SQM metrics considered in this paper can be seen as the ratios of two Gaussian distributed variables. However, each ratio does not follow a normal distribution theoretically. For example, the mean value of r_n does not exist, since it becomes infinite when y_n approaches zero. This makes the work of characterizing the statistics of SQM metrics complicated. Thus, reasonable approximations should be considered to simplify the analysis and at the same time ensure that the estimation error is acceptable. Considering many real physical phenomena follow a normal distribution, it is possible that under some conditions r_n can be approximated as a normal distributed variable. It is possible to locally approximate r_n by a Taylor series and then calculate the mean value and variance. Once it can be proved that each ratio approximately follows a normal distribution, assuming r_n with $n = 1, 2, \ldots, N$ are jointly Gaussian random variables, the constructed SQM metrics will also follow a normal distribution. Hence, next we need to consider the Taylor expansion of r_n centered on the mean value of x_n and y_n, that is μ_x and μ_y, respectively.

TABLE 1. Theoretical statistics of SQM metrics.

Delta Metric	$m_{delta} = \frac{I_{-d} - I_{+d}}{I_P}$	$N = 1$	$x_1 = I_{-d} - I_{+d}$, $y_1 = I_p$, $k_1 = 1$
	$\mu_{delta} = 0$, $\sigma^2_{delta} = 2\sigma_0^2$, $\delta_{delta} = 2$		
Ratio Metric	$m_{ratio} = \frac{I_{-d} + I_{+d}}{I_P}$	$N = 1$	$x_1 = I_{-d} + I_{+d}$, $y_1 = I_p$, $k_1 = 1$
	$\mu_{ratio} = 1$, $\sigma^2_{ratio} = \sigma_0^2$, $\delta_{ratio} = 1$		
ELP Metric	$m_{elp} = \tan^{-1}\left(\frac{Q_{-d}}{I_{-d}}\right) - \tan^{-1}\left(\frac{Q_{+d}}{I_{+d}}\right)$	$N = 1$	$x_1 = Q_{-d}$, $y_1 = I_{-d}$, $k_1 = 1$, $x_2 = Q_d$, $y_2 = I_d$, $k_2 = -1$
	$\mu_{elp} = 0$, $\sigma^2_{elp} = 8\sigma_0^2$, $\delta_{elp} = 8$		

The detailed proof of the following is presented in Appendix A. Thus, we have the mean value and variance of $k_n r_n$ as follows

$$\begin{cases} \mu_r = E[k_n r_n] \cong k_n \dfrac{\mu_x}{\mu_y} \\ \sigma_r^2 = k_n^2 \left(\dfrac{1}{\mu_y^2}\sigma_x^2 + \dfrac{\mu_x^2}{\mu_y^4}\sigma_y^2 - 2\dfrac{\mu_x}{\mu_y^3}\sigma_{x,y} \right) \end{cases} \quad (11)$$

Considering σ_x^2, σ_y^2, and $\sigma_{x,y}$ are all the functions of σ_0^2 (see Appendix A), for various SQM metrics, the nominal variance can be uniformly expressed by [12], [41]

$$\sigma_r^2 = \delta \cdot k_n^2 \cdot \sigma_0^2 = \frac{\delta \cdot k_n^2}{2\,(C/N_0)\,T_{int}} \quad (12)$$

where δ depends on the definition of the SQM metric and the correlator spacing. In the following section, we will focus on the calculation of δ for each SQM metric.

C. THEORETICAL DISTRIBUTION

Assuming the correlator spacing $d = 0.5$ chip, we can obtain the variance of Delta and Ratio metrics in the absence of spoofing attacks as $\sigma^2_{delta} = 2\sigma_0^2$ and $\sigma^2_{ratio} = \sigma_0^2$. A comprehensive derivation for the statistical first moments of Delta and Ratio metrics has been presented in Appendix B.

The ELP metric is defined as the difference of phase angle between Early and Late correlator outputs in radians. Considering the arctangent functions in the expression, it seems not straightforward to obtain its accurate probability distribution. However, it can still be expressed in the form of the generic representation we proposed above. The ELP metric should be first approximated employing Maclaurin series expansion. The comprehensive derivation for the ELP metric can be found in Appendix C.

Finally, a summary of definition and theoretical statistics of SQM metrics with $d = 0.5$ chip is given in Table 1. These statistics are used to calculate the thresholds used for

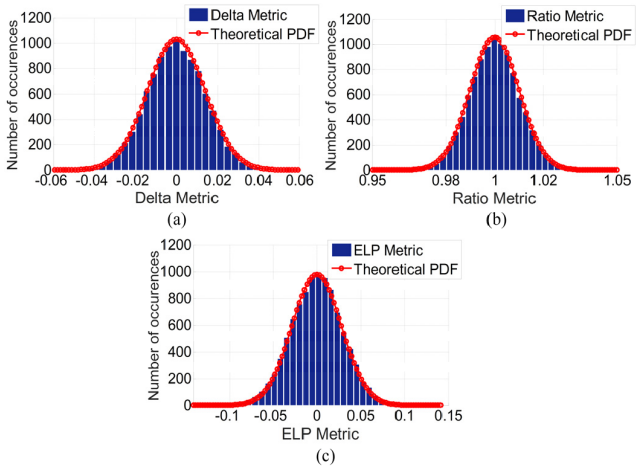


FIGURE 2. Histograms and theoretical PDF curves for (a) Delta metric, (b) Ratio metric and (c) ELP metric.

the proposed Pfa metric combination mode and amplitude combination mode described in the next section.

Fig. 2 illustrates the comparison between the derived theoretical probability density function (PDF) curves and the histograms in the absence of spoofing. The histograms are obtained by running 10^4 times simulation trials. For ease of comparison, the PDF curve has been aligned with the peak of the histogram in each subfigure. We can see that the theoretical PDF curves of three SQM metrics are all well matched with the simulation results, which demonstrates that the estimated statistics in Table 1 are reliable.

It is also worth noting that although the ELP metric seems noisier than the other two SQM metrics as the variance of the ELP metric is the largest, it does not mean the ELP performs worst. A larger variance in the absence of spoofing leads to a higher threshold, but the overall performance also depends on the distribution of the SQM metrics in the presence of various potential types of spoofing attacks which is quite complicated to characterize. Thus, the anti-spoofing performance of each metric should be further verified by simulations or tests with real data.

D. SPOOFING DETECTION METHOD

Spoofing detection is generally implemented by comparing the value of the SQM metric with a threshold. Thus, a spoofing-present decision is made if the threshold value is exceeded, and a spoofing-absent decision is made otherwise.

As analyzed previously, the value of SQM metric can be approximated as a Gaussian distributed variable. Therefore, for certain upper and lower thresholds Th_u and Th_l, P_{fa} is computed as follows

$$P_{fa} = \int_{Th_u}^{\infty} f_c(x)\,\mathrm{d}x + \int_{-\infty}^{Th_l} f_c(x)\,\mathrm{d}x = erfc\left(\frac{Th_u - \mu_i}{\sqrt{2\sigma_i^2}}\right) = erfc\left(\frac{\mu_i - Th_l}{\sqrt{2\sigma_i^2}}\right) \quad (13)$$

where $f_c(x)$ represents the probability density function of a certain SQM metric in the absence of a spoofing attack, and $erfc(\cdot)$ is the complementary error function. $f_c(x)$ is obtained based on the theoretical distribution of each SQM metric in Table 1. Then we can obtain the expressions of two thresholds as

$$Th_u = \mu_i + \sqrt{2\sigma_i^2}erfc^{-1}(P_{fa})$$
$$Th_l = \mu_i - \sqrt{2\sigma_i^2}erfc^{-1}(P_{fa}) \quad (14)$$

The threshold values are determined by a pre-defined P_{fa} and the statistics of each metric or metric combination. Considering the mean value and variance are different for various SQM metrics or metric combinations, the threshold values are definitely different.

III. METRIC COMBINATION

As mentioned previously, each SQM metric looks at the correlation function distortion from a specific point of view. It is unreliable to implement spoofing detection only depending on the result of each SQM metric at any given time. Using multiple metrics together could be intuitively efficient to improve the robustness of spoofing detection. When various SQM metrics are jointly used in a certain manner, different metric combinations can be constructed.

There could be different ways to construct the metric combinations. First, different numbers of SQM metrics can be jointly used, such as two or more metrics. Herein, we just consider the two-metric combination cases. As the ELP metric uses the information of phase difference between the Early and Late correlator outputs which differentiates it from the other two metrics, it has the potential to provide evidence of any spoofing attack underway from a new angle. Thus, the two-metric combinations, one of which is the ELP metric, deserve more attention. Another factor needing to be considered is the participation of each SQM metric used in the metric combinations. The contribution of each SQM metric could be adjustable, and the ''optimal'' case needs to be determined by some further analysis. Finally, and most importantly, different combination strategies should be considered and compared. In this work, we explore two combination strategies: amplitude combination mode (AmpM) and Pfa combination mode (PfaM). In the following sections, we focus on the discussion about these two combination strategies and their anti-spoofing performance.

A. AMPLITUDE COMBINATION MODE

Different from the cases of single metrics, multi-metric joint detection is more complicated. The amplitude combination mode is denoted as AmpM $(\cdot)$ in this paper, and its expression is given by

$$m_{12} = \beta \cdot m_1 + (1-\beta) \cdot m_2 \quad (15)$$

where m_1 and m_2 are any two SQM metrics, and m_{12} is the metric combination of m_1 and m_2 using amplitude combination mode. The metric combinations are constructed in

the form of the linear combination of various SQM metrics. In order to include the contribution of quadrature components, we mainly focus on the combinations constituted by two SQM metrics, one of which is the ELP metric.

The Delta and Ratio metrics can be seen as linear combinations of different early and late correlator outputs normalized by the prompt value, so they are naturally unitless, whereas if the ELP metric is defined by (8), it will be in units of radians, which makes AmpM given by (15) somewhat unreasonable and unaccountable. However, according to the generic representations presented in section II.B and (C4), the ELP metric can also be approximated as the sum of two ratios. As each ratio is unitless, the ELP metric can also be unitless. So for the sake of convenience, the approximate form of the ELP metric is employed in the construction of metric combinations. It should be noted that the prerequisite of such approximation is that the correlator output of the Quadrature channel is very close to 0. But in the presence of spoofing, there will be energy transferring between the In-phase and Quadrature branches, and this approximation may be false. At this point, the ELP metric should be computed in radians using its initial definition expression (8). As the range of values for the arctangent function is between -0.5π and 0.5π, the value of the ELP metric will be within the range from $-\pi$ to π.

In order to perform a statistical analysis on the amplitude combination strategy, (15) also needs to be expressed in the form of the generic representation. Taking the amplitude combination of ELP and Delta metrics as an example, the joint metric is given by

$$\begin{aligned} m_{elp+delta} &= \beta \cdot \left(\frac{Q_{-d}}{I_{-d}} - \frac{Q_{+d}}{I_{+d}} \right) + (1-\beta) \cdot \left(\frac{I_{-d} - I_{+d}}{I_P} \right) \\ &= \beta k_1 r_1 + \beta k_2 r_2 + (1-\beta) k_3 r_3 \end{aligned} \tag{16}$$

where r_1, r_2, and r_3 are ratios between various correlator outputs which have been shown to be normally distributed in the previous parts. As the covariance between any two correlators is typically nonzero, the correlator outputs are not independent of each other. But it is reasonable that the ratios can be seen as mutually independent. This is because these ratios have different denominators which are also normally distributed variables. The value of ratios would be further randomized and thus the covariance between any two correlators could be very close to zero. So according to the properties of the normal distribution, we can easily have the following conclusion that the mean value of a metric combination equals the sum of mean values of all ratios in (16), and the overall variance also equals the sum of variances of each ratio.

Now set $\beta = 0.5$, and we have the mean value of $m_{elp+delta}$ is 0 and the variance of $m_{elp+delta}$ is $0.5^2 \times 8\sigma_0^2 + 0.5^2 \times 2\sigma_0^2 = 2.5\sigma_0^2$. Therefore, $m_{elp+delta} \sim N\left(0, 2.5\sigma_0^2\right)$. In the same way, for the metric combination of ELP and Ratio, we have the mean value of $m_{elp+ratio}$ is 0.5 and the variance is $0.5^2 \times 8\sigma_0^2 + 0.5^2 \times \sigma_0^2 = 2.25\sigma_0^2$, so $m_{elp+ratio} \sim N\left(0, 2.25\sigma_0^2\right)$. The definition and theoretical statistics of the amplitude combination mode with $d = 0.5$ chip and $\beta = 0.5$ are summarized in Table 2.

TABLE 2. Statistics of the amplitude combination mode.

AmpM (ELP,Delta)	$\beta \cdot \left(\tan^{-1}\left(\frac{Q_{-d}}{I_{-d}}\right) - \tan^{-1}\left(\frac{Q_{+d}}{I_{+d}}\right) \right) + (1-\beta) \cdot \frac{I_{-d} - I_{+d}}{I_P}$
	$\mu_{\mathrm{AmpM(elp,delta)}} = 0$, $\sigma^2_{\mathrm{AmpM(elp,delta)}} = 2.5\,\sigma_0^2$
AmpM (ELP,Ratio)	$\beta \cdot \left(\tan^{-1}\left(\frac{Q_{-d}}{I_{-d}}\right) - \tan^{-1}\left(\frac{Q_{+d}}{I_{+d}}\right) \right) + (1-\beta) \cdot \frac{I_{-d} + I_{+d}}{I_P}$
	$\mu_{\mathrm{AmpM(elp,ratio)}} = 0.5$, $\sigma^2_{\mathrm{AmpM(elp,ratio)}} = 2.25\,\sigma_0^2$

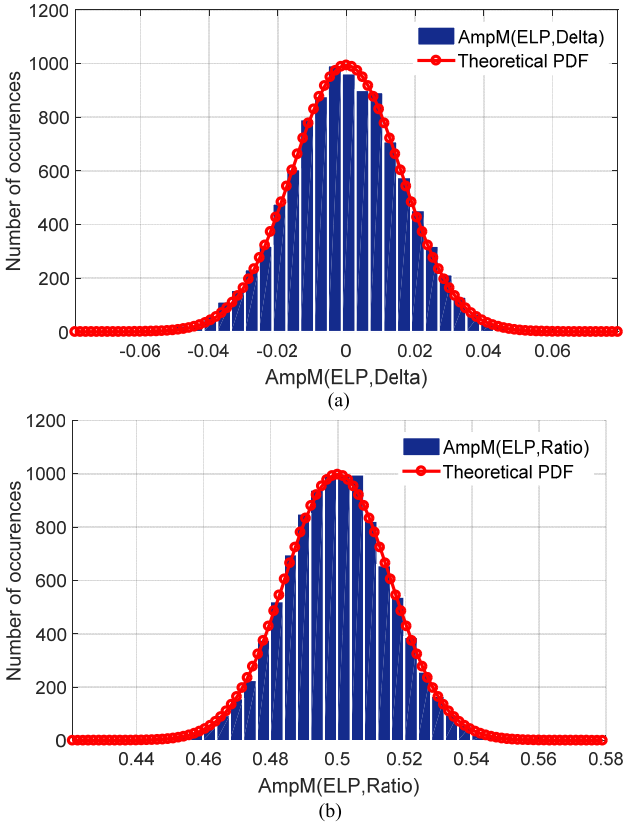


FIGURE 3. Histogram and theoretical PDF curve for amplitude combination combinations of (a) ELP and Delta metrics (b) ELP and Ratio metrics. β is set to 0.5.

Fig. 3 plots the theoretical PDF curves of metric combinations, AmpM(ELP, Delta), and AmpM(ELP, Ratio), together with the histograms calculated from 10^4 simulation runs. We can see that the theoretical curves are consistent with the histograms. Thus, the theoretical distribution of the SQM metric combinations in AmpM mode is considered to be validated. It will be used to set detection thresholds for the metric combinations in the practical applications.

B. PFA COMBINATION MODE

The previous discussed AmpM is a kind of tightly-coupled combination strategy. Compared to AmpM, the Pfa

combination mode is loosely-coupled. Different SQM metrics work independently, but the final decision is made based on the detection results of different SQM metrics. So, the Pfa combination strategy is defined as the spoofing-presence decision is made as long as one metric exceeds its threshold. It is denoted as PfaM $(\cdot)$ in this paper.

For the sake of simplification, we just assume two SQM metrics are jointly used for spoofing detection. Let $P_{fa,i}$ ($i = 1$ or 2) denote the probabilities of false alarm of the two SQM metrics; they could be independent of each other. The detection threshold for each SQM metric can be calculated based on the detection method described in section II.D. Finally, the overall probability of false alarm for the metric combination is computed by

$$\begin{aligned} P_{fa} &= 1 - \left(1 - P_{fa,1}\right) \cdot \left(1 - P_{fa,2}\right) \\ &= P_{fa,1} + P_{fa,2} - P_{fa,1} \cdot P_{fa,2} \end{aligned} \tag{17}$$

In the typical case where $P_{fa,i}$ is chosen to be close to zero, such as 1% or even smaller values, the last term in (17) can be ignored, thus the overall P_{fa} can be simply rewritten as the sum of $P_{fa,1}$ and $P_{fa,2}$

$$P_{fa} \approx P_{fa,1} + P_{fa,2} \tag{18}$$

So, if we want to construct a metric combination with overall P_{fa} equal to a given value, i.e. $P_{fa} = P_{fa,given}$, $P_{fa,given}$ should be allocated in proportion to $P_{fa,1}$ and $P_{fa,2}$. Here we define a factor λ to characterize this allocation

$$\begin{cases} P_{fa,1} = \lambda \cdot P_{fa,\text{given}} \\ P_{fa,2} = (1 - \lambda) \cdot P_{fa,\text{given}} \end{cases} \tag{19}$$

We can see that, similar to β in the definition formula of the amplitude combination strategy (eq. (15)), λ can also be seen as a weighting factor to adjust the participation of each SQM metric. The difference is that, β is used to adjust the metric amplitude that each metric contributes, but λ adjusts the false alarm probability that each metric contributes. This is why we call this combination strategy the Pfa combination mode.

C. EVALUATION CRITERION

So far, we have discussed two combination strategies and how to calculate theoretical threshold values for a specific P_{fa}. For the sake of comparison, we need a performance metric to characterize the anti-spoofing performance of SQM metrics and their combination strategies. Considering the relative carrier phase and code delay between the counterfeit signal and its authentic counterpart are varying during a spoofing attack, a good spoofing detection method is expected to be less sensitive to this variation and uniformly sensitive to a large range of carrier phases and code delays. So here we define two measurements, detectable area and overall detection ratio, as follows:

- Detectable Area

For a given P_{fa}, if the probability of detection (P_d) in the case of a certain relative code delay and relative carrier phase exceeds a minimum acceptable detection probability, it is then considered to be a detectable point. All the detectable points constitute the detectable area. The minimum acceptable detection probability can also be seen as a threshold for its P_d.

- Overall Detection Ratio

The overall detection ratio, defined as (20), is a criterion to characterize the robustness of the SQM metric over all relative carrier phases and code phases. It is a ratio between the detectable area and the total area. The total area is a fixed rectangle area whose width represents various code delay of spoofing signal relative to the authentic signal and height represents the relative carrier phase. Thus, a larger detectable area corresponds to a larger overall detection ratio and the SQM metric with larger overall detection ratio will be regarded as a better metric as it is more robust to the time-varying code delay and carrier phase.

$$\text{Overall Detection Ratio} = \frac{\text{Detectable Area}}{\text{Total Area}} \tag{20}$$

IV. SIMULATION RESULTS

Simulation results for different metric combinations in terms of detectable area and overall detection ratio are provided in this section. In the following simulations, a spoofing signal with amplitude attenuation of 0.7 was added to the authentic signal. P_{fa} is set to 0.01 and the minimum acceptable detection probability is set to 0.8. The thresholds for spoofing detection are calculated based on (14), and the tracking loop integration time is 1 ms.

The C/N_0 used here is 53 dB-Hz, which is consistent with that of the TEXBAT dataset used in the next section. This is a reasonably strong signal environment where the user receiver is able to reliably track the signals from authentic GNSS satellites prior to the spoofing attacks, which is a prerequisite of the SQM-based spoofer detector. A weak signal condition implies poor C/N_0 of the received signal. Left uncompensated, it will result in larger variance of the correlator outputs and a decline of detection probability. To counter weak signal conditions, the tracking loop integration time needs to be extended.

A. SENSITIVITY OF SQM TO RELATIVE CODE PHASE AND RELATIVE CARRIER PHASE

This subsection tries to show the effect of relative code phase and relative carrier phase on the SQM metrics. Subfigures on the left side of Fig. 4 show the detection probability for each SQM metric by varying the code delay and carrier phase of the counterfeit signal relative to the authentic signal. When a minimum acceptable detection probability is applied, we have the detectable areas of each SQM metric as shown in the subfigures on the right side of Fig. 4. The detectable area is highlighted in yellow. It can be seen that the detectable areas of the Delta metric and Ratio metric are very similar, owing to the similar information they use to perform spoofing detection, whereas the ELP metric has a complementary

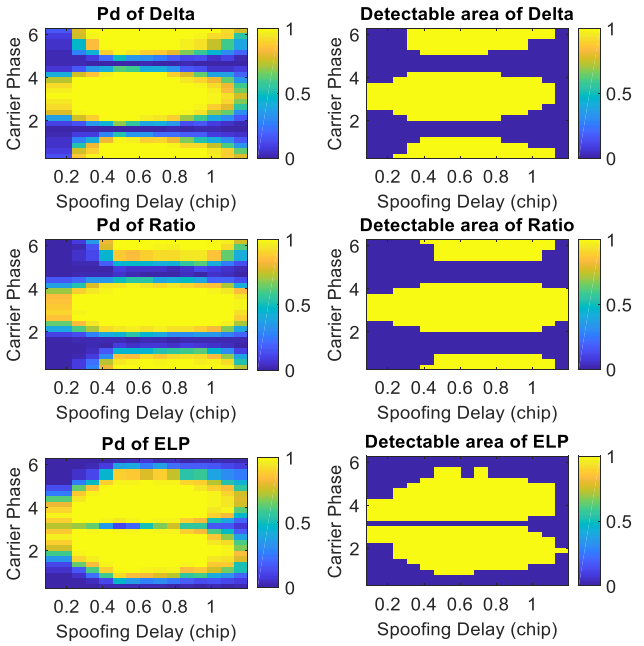


FIGURE 4. Detection probability and detectable area for individual SQM metrics.

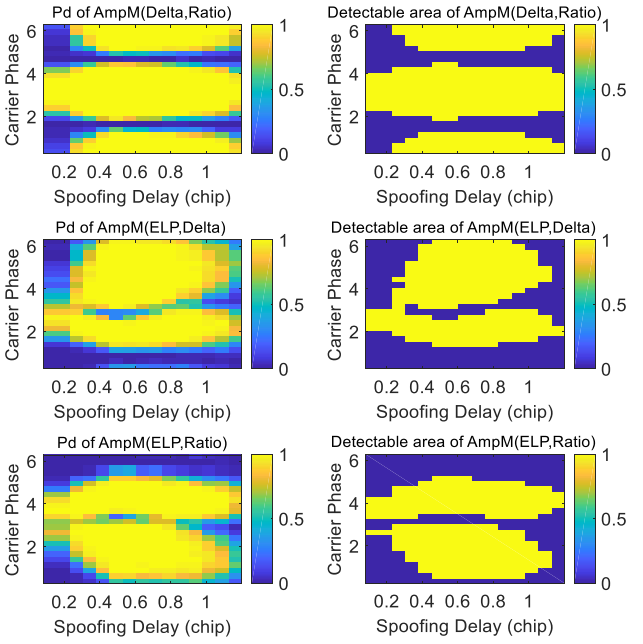


FIGURE 5. Detection probability and detectable area for amplitude combination mode (AmpM).

shape to the other two SQM metrics. The complementarity makes it possible to improve the performance of anti-spoofing by using metrics jointly.

Fig. 5 illustrates the detection probability and the corresponding detectable area for amplitude combination mode. The weighting factor β is set to 0.5. Compared with the results of the Delta metric and Ratio metric in Fig. 4, AmpM(Delta, Ratio) has a very similar shape of detectable area, whereas AmpM(ELP, Delta) and AmpM(ELP, Ratio) show irregular detectable areas which are different from that of AmpM(Delta, Ratio). However, we can see the amplitude combination mode only changes the shape of detectable area, but it doesn't significantly enlarge the detectable area (see also Table 3). Thus, it seems that this combination achieves very limited performance gain.

Fig. 6 shows the detection probability and detectable area for the Pfa combination mode. The weighting factor λ is set to 0.5. It is obvious that PfaM(ELP, Delta) and PfaM(ELP, Ratio) significantly improve the probability of detection for a specific carrier phase and code delay. The final detection area shows a combined shape of the detectable areas of the ELP metric and Delta metric (or Ratio metric). Thus, the Pfa combination mode can be an effective strategy to construct the SQM metric combinations and eventually improve the robustness of spoofing detection. In addition, the Pfa combination of Delta and Ratio metrics has minimal effect on the overall detection ratio, which demonstrates that the combination of Delta and Ratio metrics could not significantly boost the overall performance no matter what combination strategy is adopted.

For comparison purposes, the overall detection ratio has been calculated based on the simulation results from Fig. 4 to Fig. 6 to be shown in Table 3. It is calculated using the definition formula of (20). We can see the overall detection ratios for each single metric are all around 0.5, which means there is no real difference among various SQM metrics in terms of the spoofing detection performance. However for the amplitude combination mode, the detection ratios just slightly increase compared with single SQM metrics. But Pfa combination provides a marginal improvement of almost 20% in terms of its overall detection ratio. Especially PfaM(ELP, Ratio) outperforms all the other cases with an overall detection ratio of 0.7746.

TABLE 3. Overall detection ratios for different SQM metrics and metric combinations.

Single metric	Delta	Ratio	ELP
Detection Ratio	0.4972	0.5178	0.5000
Combination Modes	**Delta+Ratio**	**ELP+Delta**	**ELP+Ratio**
Mode 1: Amplitude combination	0.5772	0.5111	0.5139
Mode 2: Pfa combination	0.6044	0.7653	0.7746

B. EFFECT OF β AND λ

Another consideration is the selection of weighting factors β and λ for the amplitude and Pfa combination mode, respectively. It is necessary to evaluate the effect of β and λ on the overall performance. Simulations have been performed by varying β and λ, and all else being the same as the previous subsection. The overall detection ratio curves for various metric combinations with are shown in Fig. 7. For AmpM

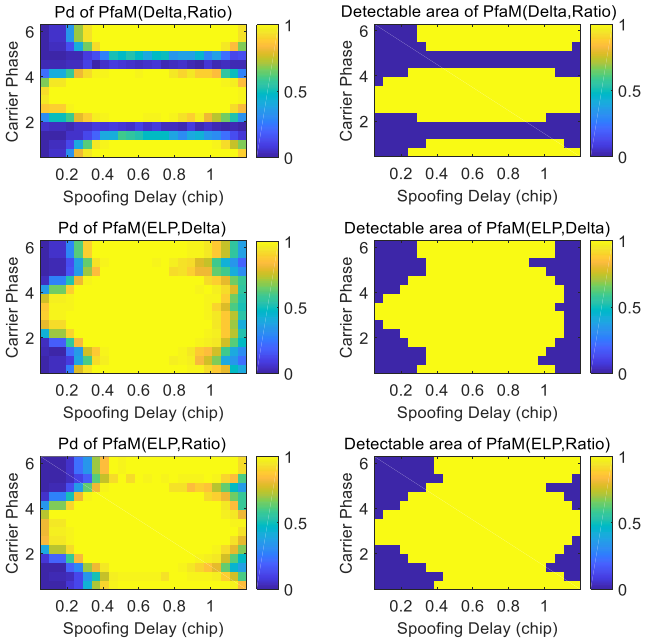


FIGURE 6. Detection probability and detectable area for combination Pfa combination mode.

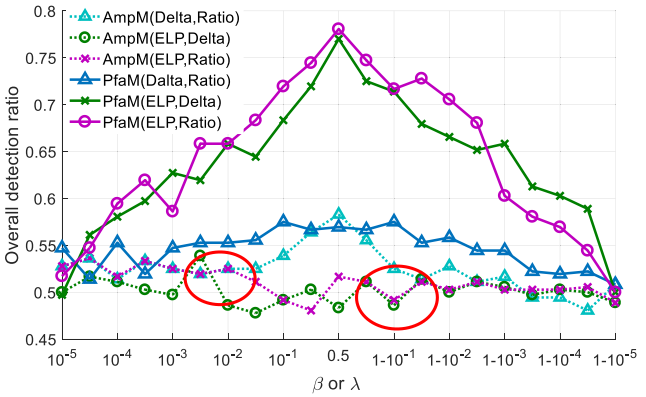


FIGURE 7. Overall detection ratio VS. weighting factor β for amplitude combination mode and weighting factor λ for Pfa combination mode. Two red circles indicate the curves of AmpM begin to separate or overlap.

and PfaM, the horizontal axis represents β and λ, respectively. We can see that for PfaM(ELP, Delta) and PfaM(ELP, Ratio), the overall detection ratio increases stably from about 0.5 to larger than 0.75 reaching the maximum, as λ varies from 10^{-5} to 0.5. Then it drops back to 0.5, as λ increases from 0.5 to 1-10^{-5}. Thus, 0.5 can be the best value of λ to achieve the largest detection ratio, whereas the combination of Delta and Ratio metric still shows no significant performance gain compared to its individual metrics.

However, for the amplitude combination strategy, all three dotted curves fluctuant around 0.5, except for AmpM(Delta, Ratio) which improves slightly at $\beta = 0.5$. Also, when β is smaller than 10^{-2}, we can see the curves of AmpM(Delta, Ratio) and AmpM(ELP, Ratio) overlap. This is because the choice of β has given dominance to the Ratio metric. Similarly, the curves of AmpM(ELP, Delta) and AmpM(ELP, Ratio) are also very close to each other when β is larger than 0.9, as dominance has been given to the ELP metric.

V. TESTS WITH THE TEXBAT DATASET

In this section, we evaluate the spoofing detection performance using individual metrics and metric combinations with real data. The dataset, named TEXBAT, is part of a test battery of real cases publicly provided by the University of Texas at Austin [40]. Considering the limitations of space, we will focus our performance evaluation using Scenario 2 and compare it with Scenario 3. The two scenarios differ in terms of the ways to align the carrier phase, which has been fully discussed in [21]. From Scenario 2 and 3, we can observe significant variation in detection performance between a crude frequency unlocked spoofer (i.e. Scenario 2) and a frequency locked spoofer (i.e. Scenario 3). The signals were processed using a modified version of the MATLAB GPS software receiver [42] at a correlator output rate of 1000 samples per second. As mentioned above, the performance of the Delta and Ratio metrics is quite close. Thus, for brevity, we will only consider the Ratio metric, ELP metric, PfaM, and AmpM metric combinations in the following tests.

A. SCENARIO 2

Scenario 2 of the TEXBAT dataset includes a spoofer with a high-power advantage over the authentic signal (+10 dB). The total signal length is about 350 s. A frequency-unlocked spoofing attack is launched from the 150 s to 250 s, and the relative code phase between the authentic signal and spoofing signal begins at 0 chips and ends at 2 chips. After the interaction stage, the tracking loop of target receiver eventually locks on the counterfeit signal.

To examine carefully the changes of detection performance during the whole spoofing attack, the detection rate of single metrics, and various metric combinations with AmpM and PfaM are illustrated in Fig. 8. The definition of detection rate here is essentially identical with the overall detection ratio in section IV, which is given by

$$\text{detection rate} = \frac{Num\left\{(m(n) > \mathrm{T}_h) \text{ or } (m(n) < \mathrm{T}_l)\right\}}{N}, \quad n = 1, 2, \ldots .N \qquad (21)$$

It is defined as a ratio between the number of SQM measurements that exceed the thresholds and the total number of measurements N over a detection window. So N is a function of detection window and the integral time of tracking loop.

To illustrate its time domain transients, a short detection window of 10 seconds is chosen for the results in Fig. 8, so a set of detection rates is computed within every 10-second long dataset. Constant false alarm rate (CFAR) processing is employed and the predetermined false alarm rate used in this test is 0.01, which is used to calculate the theoretical thresholds for spoofing detection. The weighting factors of

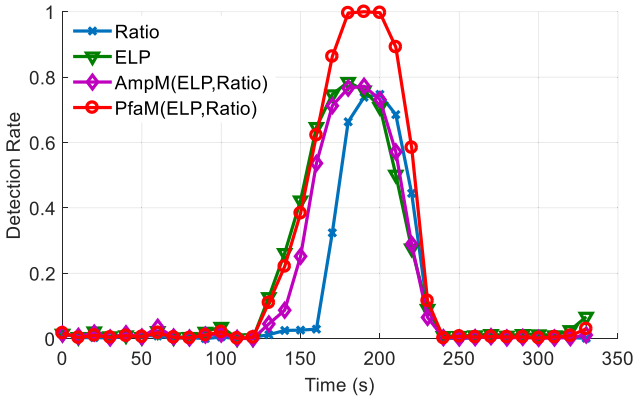


FIGURE 8. Changings of detection rate for single metrics and various metric combinations over Scenario 2 of the TEXBAT dataset.

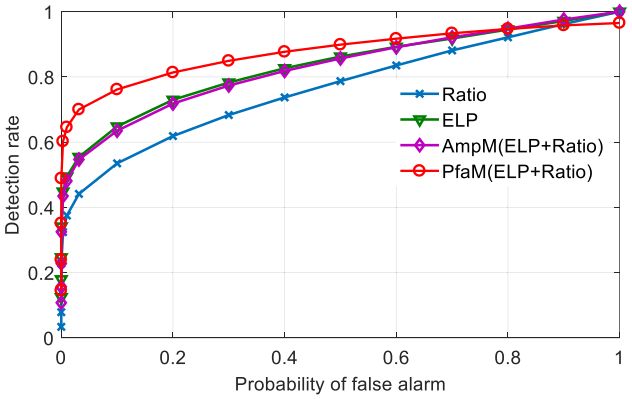


FIGURE 9. ROC curves for individual SQM metrics and various metric combinations over Scenario 2 of the TEXBAT dataset.

two combination strategies, λ and β, are all set to 0.5 in the following tests.

We can see from Fig. 8 that for the first 120 seconds, the detection rate curves are all slightly larger than 0. That's because in this stage, the spoofing attack has not been launched. The metric response of this stage is identical to the pure authentic signal circumstance, so the detection rate at this moment is almost equal to the pre-set false alarm rate of 0.01. After that, all curves start increasing. We can see PfaM(ELP,Ratio) outperforms the other methods for the whole period of the interaction stage from 150 s to 250 s. Particularly, the instantaneous detection rate of PfaM(ELP,Ratio) approximates 100% during the interval between 160 and 200 s. After 250 s where the interaction stage has ended, the relative code phase exceeds 1 chip, which precludes any SQM methods from detecting any spoofer-authentic signal interaction.

It is also interesting to mention that the detection rate curve of the Ratio metric noticeably lags behind other three curves. This is probably because the sum of the Early and Late correlator outputs does not change so dramatically in the early stage of a spoofing attack when the spoofing signal has a code delay similar to the authentic signal. This conclusion is also supported by Fig. 4, from which we can see the detectable area of the Ratio metric shifts slightly to the right compared with that of the Delta or ELP metric. Thus, the Ratio metric has a relatively slower reaction. In addition, although a β of 0.5 is used here, the AmpM(ELP, Ratio) performs similarly to the ELP metric but differently from the Ratio metric. This is because the variance of the ELP metric σ^2_{elp} is approximately 8 times σ^2_{ratio} (see Table 1), so the ELP metric affects more in AmpM(ELP, Ratio) than the Ratio metric even the two SQM metrics are combined in the same proportion.

Fig. 9 shows the Receiver Operating Characteristic (ROC) curves of detection techniques for single metrics and various metric combinations. The detection window is 100 seconds, from 150 s to 250 s. This period is corresponding to the interaction stage between the authentic signal and spoofing signal. We can see that for a given false alarm rate of 0.1, the detection rate of PfaM(ELP, Ratio) exceeds 0.75. However, AmpM(ELP, Ratio) is even slightly worse than the individual ELP metric. So, the Pfa combination mode outperforms the amplitude combination mode, as well as each individual SQM metrics.

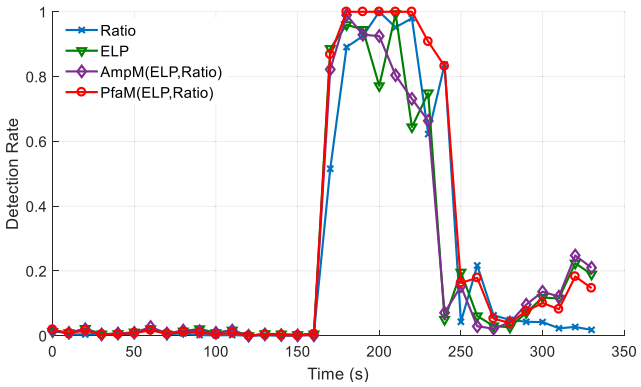


FIGURE 10. Changings of detection rate for single metrics and various metric combinations over Scenario 3 of the TEXBAT dataset.

B. SCENARIO 3

This scenario considers a spoofer with a low power advantage over the authentic signal (+1.3 dB) that performs a frequency-locked time push from seconds 150 to 300 of the total simulation time. The PRN used here is 3.

Fig. 10 shows the transients of the detection rate of single SQM metrics as well as various metric combinations under Scenario 3 of the TEXBAT dataset. The detection window used to compute each detection rate is 10 s, which is identical to Fig. 8. During the interaction stage (defined from 150 s to 250 s), the PfaM(ELP, Ratio) method visibly outperforms all other methods. On the other hand, the detection rate curves of the AmpM(ELP,Ratio) method shows no improvement against other individual SQM metrics.

Similar conclusions can also be reached from Fig. 11, which gives ROC curves of different SQM metrics over the interval from 150 s to 250 s. Also, we can see that the ELP metric outperforms the Ratio metric in Fig. 9 but not in Fig. 11. This is because for a frequency unlocked case

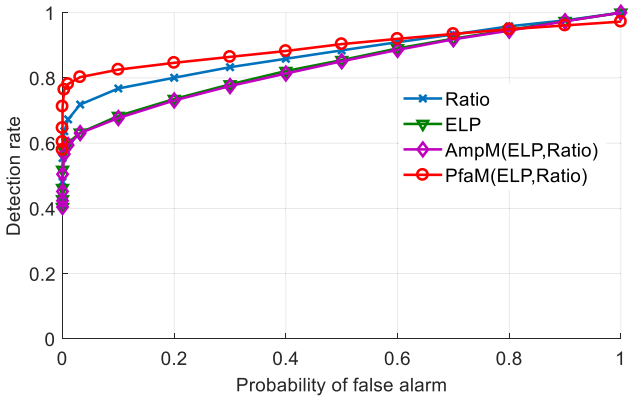


FIGURE 11. ROC curves for basic SQM metrics and various metric combinations over Scenario 3 of the TEXBAT dataset.

(Scenario 2 of the TEXBAT), the relative carrier phase between the authentic and counterfeit signals is not constant but time-varying. As a result, the energy of the counterfeit signal frequently transfers between the I and Q channels, which is captured by the ELP metric. However, for a frequency locked case (Scenario 3 of the TEXBAT), this effect is not obvious and thus the Ratio metric shows better performance.

It should also be noted that the performance evaluation presented above does not consider the environmental effects, such as multipath. Similar to a spoofing attack, multipath can also result in the distortion of correlation peak, which will cause false alarm to an SQM-based spoofing detector and deteriorate its performance. This is a challenge to all the SQM-based anti-spoofing techniques but beyond the scope of this article. It can be perceived that additional techniques should be jointly used with the SQM method, such as power monitoring [37], [38], Doppler domain detection [16], and multiple satellites consistency checks [43] to reliably distinguish spoofing attacks from multipath. Future research will focus on how to distinguish spoofing from multipath to improve the feasibility of the anti-spoofing method under complex multipath environment. Alternatively, this paper can also be used as the foundation of a detector that jointly detects multipath and spoofing attacks.

VI. CONCLUSION

This paper has proposed a multi-metric joint detection technique for spoofing detection, by attempting to combine various SQM metrics to perform spoofing detection rather than choosing one of many SQM metrics. Two different combination strategies have been proposed and analyzed. The performance has been evaluated using the TEXBAT dataset. Results show that for a given false alarm rate of 0.1, the detection rate exceeds 0.75 for PfaM(ELP, Ratio), but less than 0.65 for AmpM(ELP, Ratio), the individual ELP metric, and the Ratio metric. The proposed multi-metric combination technique in PfaM combination improves the robustness of spoofing detection and shows significant ROC performance improvement when compared against any individual SQM metric.

APPENDIX A
THE DERIVATION OF STATISTICS FOR THE GENERIC SQM MODEL

For $f\,(\mathrm{x},\mathrm{y}) = \mathrm{x}/\mathrm{y}$, the Taylor series expansion of $f\,(\mathrm{x},\mathrm{y})$ centered on the mean value of x and y is given by

$$f\,(\mathrm{x},\mathrm{y}) \cong g_0 + g_x \cdot (x-\mu_x) + g_y \cdot \left(y-\mu_y\right) \tag{A1}$$

with

$$\begin{cases} g_0 = f\left(\mu_x,\mu_y\right) = \dfrac{\mu_x}{\mu_y} \\ g_x = f'_x\left(\mu_x,\mu_y\right) = \left.\dfrac{\partial f}{\partial x}\right|_{x=\mu_x, y=\mu_y} = \dfrac{1}{\mu_y} \\ g_y = f'_y\left(\mu_x,\mu_y\right) = \left.\dfrac{\partial f}{\partial y}\right|_{x=\mu_x, y=\mu_y} = -\dfrac{\mu_x}{\mu_y^2} \end{cases} \tag{A2}$$

where μ_x and μ_y are the mean value of x and y, respectively. The mean value of $f\,(\mathrm{x},\mathrm{y})$ can be computed by

$$\begin{aligned} E\left[f\,(\mathrm{x},\mathrm{y})\right] &\cong E\left[g_0\right] + g_x \cdot E\left(x-\mu_x\right) + g_y \cdot E\left(y-\mu_y\right) \\ &= E\left[g_0\right] = g_0 = \frac{\mu_x}{\mu_y} \end{aligned} \tag{A3}$$

where $E\,(\cdot)$ represents the operation of statistical expectation. We can also get the mean square value of $f\,(\mathrm{x},\mathrm{y})$, which can be expressed as

$$\begin{aligned} &E\left[f\,(\mathrm{x},\mathrm{y})^2\right] \\ &\quad\cong E\left[g_0^2\right] + g_x^2 \cdot E\left[(x-\mu_x)^2\right] + g_y^2 \cdot E\left[\left(y-\mu_y\right)^2\right] \\ &\qquad + 2g_0 \cdot g_x \cdot E\left(x-\mu_x\right) + 2g_0 \cdot g_y \cdot E\left(y-\mu_y\right) \\ &\qquad + 2g_x \cdot g_y \cdot E\left[\left(x-\mu_x\right)\left(y-\mu_y\right)\right] \end{aligned} \tag{A4}$$

Then after some mathematical manipulations, the above equation can be rewritten as

$$E\left[f\,(\mathrm{x},\mathrm{y})^2\right] \cong g_0^2 + g_x^2 \cdot \sigma_x^2 + g_y^2 \cdot \sigma_y^2 + 2g_x \cdot g_y \cdot \sigma_{xy} \tag{A5}$$

The variance of $f\,(\mathrm{x},\mathrm{y})$ can be written as

$$\begin{aligned} \sigma^2_{f(\mathrm{x},\mathrm{y})} &= E\left[f\,(\mathrm{x},\mathrm{y})^2\right] - E\left[f\,(\mathrm{x},\mathrm{y})\right]^2 \\ &= g_x^2 \cdot \sigma_x^2 + g_y^2 \cdot \sigma_y^2 + 2g_x \cdot g_y \cdot \sigma_{xy} \end{aligned} \tag{A6}$$

So, the variance of $f\,(\mathrm{x},\mathrm{y})$ can be further written as

$$\sigma^2_{f(\mathrm{x},\mathrm{y})} = \frac{1}{\mu_y^2}\sigma_x^2 + \frac{\mu_x^2}{\mu_y^4}\sigma_y^2 - 2\frac{\mu_x}{\mu_y^3}\sigma_{\mathrm{x},\mathrm{y}} \tag{A7}$$

APPENDIX B
STATISTICS OF DELTA AND RATIO METRICS

According to the generic representation of SQM metrics (eq.(9)), for Ratio metric, we have

$$\begin{cases} x = I_{-d} + I_{+d} \\ y = I_P \end{cases} \tag{B1}$$

Assuming I_{+d} and I_{-d} are independent of each other, we can easily obtain

$$\begin{cases} \mu_x = 2R\,(dT_c) \\ \mu_y = R(0) \end{cases} \tag{B2}$$

So, we have $\mu_{ratio} = \mu_x/\mu_y = 2R(dT_c)/R(0)$. The covariance of x and y, σ_{xy}, can be computed by

$$\begin{aligned}\sigma_{xy} &= \sigma_{yx} = Cov\left[\mathrm{x}, \mathrm{y}\right] \\ &= E\left\{(I_{-d} + I_{+d} - E\left[I_{-d} + I_{+d}\right]) \cdot \left(I_p - E\left[I_p\right]\right)\right\} \\ &= E\left\{(I_{-d} - E\left[I_{-d}\right]) \cdot I_p\right\} + E\left\{(I_{+d} - E\left[I_{+d}\right]) \cdot I_p\right\} \\ &= \sigma_{I_{-d}I_p} + \sigma_{I_{+d}I_p} = 2\sigma_0^2 R(dT_c)\end{aligned} \tag{B3}$$

The variance of y, σ_y^2, can be directly given as $\sigma_y^2 = \sigma_0^2$ and σ_x^2 is calculated as follows

$$\begin{aligned}\sigma_x^2 &= Var\left[I_{-d} + I_{+d}\right] \\ &= Var\left[I_{-d}\right] + Var\left[I_{+d}\right] + 2Cov\left[I_{-d}, I_{+d}\right] \\ &= 2\sigma_0^2 + 2\sigma_0^2 R(2dT_c)\end{aligned} \tag{B4}$$

Thus, based on (A7) and (B2) to (B4), the variance of the Ratio metric is computed as

$$\begin{aligned}\sigma_{ratio}^2 = &\frac{1}{R(0)^2}\left(2\sigma_0^2 + 2\sigma_0^2 R(2dT_c)\right) \\ &+ \frac{4R(dT_c)^2}{R(0)^4}\sigma_0^2 - \frac{4R(dT_c)}{R(0)^3} \cdot 2\sigma_0^2 R(dT_c)\end{aligned} \tag{B5}$$

If we assume $d = 0.5$ chip, it can be easily obtained that $\sigma_{ratio}^2 = \sigma_0^2$ and $\delta_{ratio} = 1$.

In the same way, the Delta metric can also be rewritten in the form of (9) with

$$\begin{cases} x = I_{-d} - I_{+d} \quad y = I_P \\ \mu_x = 0 \quad \mu_y = R(0) \\ \sigma_x^2 = 2\sigma_0^2\left(R(0) - R(2dT_c)\right) \quad \sigma_y^2 = \sigma_0^2 \\ \sigma_{xy} = Cov\left(I_{-d} - I_{+d}, I_P\right) \\ \qquad = Cov\left(I_{-d}, I_P\right) - Cov\left(I_d, I_P\right) = 0 \end{cases} \tag{B6}$$

Then we can obtain the statistics of the Delta metric as follows

$$\begin{cases} \mu_{delta} = \dfrac{\mu_x}{\mu_y} = 0 \\ \sigma_{delta}^2 = \dfrac{1}{R(0)^2} \cdot \sigma_x^2 + \dfrac{0}{R(0)^4}\sigma_y^2 - 2\dfrac{0}{R(0)^3} \cdot \sigma_{xy} \\ \qquad = \dfrac{2\sigma_0^2\left(R(0) - R(2dT_c)\right)}{R(0)^2} \end{cases} \tag{B7}$$

If we set $d = 0.5$ chip, we will have $\sigma_{delta}^2 = 2\sigma_0^2$ and $\delta_{ratio} = 2$.

APPENDIX C
STATISTICS OF THE ELP METRIC

It is known that the arctangent function has the following Maclaurin series expansion

$$\arctan x = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} x^{2n+1} = x - \frac{x^3}{3} + \frac{x^5}{5} - \cdots \quad \text{for } |x| \le 1 \tag{C1}$$

So, the phase angle of a correlator with correlator spacing d can be expanded as

$$\tan^{-1}\left(\frac{Q_d}{I_d}\right) = \frac{Q_d}{I_d} - \frac{1}{3}\left(\frac{Q_d}{I_d}\right)^3 + \frac{1}{5}\left(\frac{Q_d}{I_d}\right)^5 - \cdots \tag{C2}$$

When the tracking loop is locked, and the received signal is stabilized in PLL mode, there are no tracking code and phase offsets. The signal energy mainly concentrates on the In-phase branch and Q_d/I_d is very close to 0. In the circumstances, the terms in (C2), except for the first term, will be very small that they can be ignored for simplification of analysis. Thus, the phase angle can be approximately written as

$$\begin{cases} \theta_{early} = \tan^{-1}\left(\dfrac{Q_{-d}}{I_{-d}}\right) \approx \dfrac{Q_{-d}}{I_{-d}} \\ \theta_{late} = \tan^{-1}\left(\dfrac{Q_{+d}}{I_{+d}}\right) \approx \dfrac{Q_{+d}}{I_{+d}} \end{cases} \tag{C3}$$

Finally, the ELP metric approximately can be written as

$$m_{elp} \approx \hat{m}_{elp} = \frac{Q_{-d}}{I_{-d}} - \frac{Q_{+d}}{I_{+d}} = \frac{x_1}{y_1} - \frac{x_2}{y_2} = r_1 - r_2 \tag{C4}$$

So, ELP metric is also expressed in the form of (9), where

$$\begin{cases} x_1 = Q_{-d}, \quad y_1 = I_{-d}, \; x_2 = Q_{+d}, \; y_2 = I_{+d} \\ \mu_{x1} = \mu_{x2} = A \cdot R(dT_c) \cdot \sin\theta_a = 0 \\ \mu_{y1} = \mu_{y2} = A \cdot R(dT_c) \cdot \cos\theta_a = A \cdot R(dT_c) \\ \sigma_{x1}^2 = \sigma_{y1}^2 = \sigma_{x2}^2 = \sigma_{y2}^2 = \sigma_0^2 \\ \sigma_{x1y1} = \sigma_{x2y2} = Cov\left(Q_{-d}, I_{-d}\right) = Cov\left(Q_{+d}, I_{+d}\right) = 0 \\ k_1 = 1, \quad k_2 = -1 \end{cases} \tag{C5}$$

As both r_1 and r_2 can be characterized by a normal distribution, the difference value $r_1 - r_2$ will also follow a normal distribution with mean value $\mu_{elp} = E\left[r_1\right] - E\left[r_2\right]$ and variance $\sigma_{elp}^2 = Var\left[r_1\right] + Var\left[r_2\right]$. Next, we need to obtain the mean value and the variance of r_1 and r_2.

For r_1, the mean value $E\left[r_1\right]$ equals to $\mu_{x1}/\mu_{y1} = 0$. According to (A7), the variance $Var\left[r_1\right]$ is computed by

$$\begin{aligned} Var\left[r_1\right] &= \frac{1}{R(dT_c)^2 \cdot \cos^2\theta_a}\sigma_0^2 + \frac{R(dT_c)^2 \cdot \sin^2\theta_a}{R(dT_c)^4 \cdot \cos^4\theta_a}\sigma_0^2 \\ &\quad - 2\frac{R(dT_c) \cdot \sin\theta_a}{R(dT_c)^3 \cdot \cos^3\theta_a} R\left(d_{x1y1}T_c\right)\sigma_0^2 \\ &= \frac{1}{R(dT_c)^2 \cdot \cos^4\theta_a}\sigma_0^2 \\ &\quad - 2\frac{\sin\theta_a\cos\theta_a}{R(dT_c)^2 \cdot \cos^4\theta_a} R\left(d_{x1y1}T_c\right)\sigma_0^2 \\ &= \frac{1 - 2\sin\theta_a\cos\theta_a R\left(d_{x1y1}T_c\right)}{R(dT_c)^2 \cdot \cos^4\theta_a}\sigma_0^2 \end{aligned} \tag{C6}$$

When we substitute $\theta_a \approx 0$ and $d = 0.5$ into (C6), we have

$$Var\left[r_1\right] = \frac{1}{A^2 \cdot R(dT_c)^2 \cdot \cos^2\theta_a}\sigma_0^2 = 4\sigma_0^2 \tag{C7}$$

Similarly, the statistics of r_2 can be directly given by

$$\begin{cases} E\left[r_1\right] = 0 \\ Var\left[r_1\right] = 4\sigma_0^2 \end{cases} \tag{C8}$$

Finally, we obtain the overall statistics of the ELP metric as follows

$$\begin{cases} \mu_{elp} = 0 \\ \sigma_{elp}^2 = 4\sigma_0^2 + 4\sigma_0^2 = \delta_{elp} \cdot \sigma_0^2 = 8\sigma_0^2 \end{cases} \tag{C9}$$

REFERENCES

[1] 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, Art. no. 127072, May 2012, doi: 10.1155/2012/127072.

[2] 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.

[3] 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.

[4] 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, 2015.

[5] 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.

[6] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in *Proc. 26th Int. Techn. Meeting Satell. Div. Inst. Navigat.*, Nashville, TN, USA, Sep. 2013, pp. 2949–2991.

[7] J. Nielsen, A. Broumandan, and G. Lachapelle, "GNSS spoofing detection for single antenna handheld receivers," *J. Navigat.*, vol. 58, no. 4, pp. 335–344, 2011.

[8] F. Wang, H. Li, and M. Lu, "GNSS spoofing countermeasure with a single rotating antenna," *IEEE Access*, vol. 5, pp. 8039–8047, 2017.

[9] 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.

[10] Y. Yang, H. Li, and M. Lu, "Performance assessment of signal quality monitoring based GNSS spoofing detection techniques," in *Proc. CSNC*, Xi'an, China, 2015, pp. 783–793.

[11] 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, 2014, doi: 10.1109/NAVITEC.2014.7045136.

[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*, Barcelona, Spain, 2016, pp. 1–8.

[13] J. Huang, L. L. Presti, B. Motella, and M. Pini, "GNSS spoofing detection: Theoretical analysis and performance of the ratio test metric in open sky," *ICT Express*, vol. 2, no. 1, pp. 37–40, 2016.

[14] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements," *Int. J. Satell. Commun. Netw.*, vol. 30, no. 4, pp. 181–191, 2012.

[15] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/N_0 estimates," in *Proc. ION GNSS*, Nashville, TN, USA, 2012, pp. 2878–2884.

[16] 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.

[17] 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.

[18] 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.

[19] 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, 2017.

[20] 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.

[21] C. Sun *et al.*, "Moving variance-based signal quality monitoring method for spoofing detection," *GPS Solutions*, vol. 22, p. 83, Jul. 2018.

[22] A. Jovanovic, C. Botteron, and P.-A. Fariné, "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.

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

[24] 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.

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

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

[27] 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.

[28] C. Sun, J. W. Cheong, A. 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, pp. 1–15.

[29] 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.

[30] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal quality monitoring applied to spoofing detection," in *Proc. 24th Int. Techn. Meeting Satell. Div. Inst. Navigat.*, Portland, OR, USA, Sep. 2011, pp. 1888–1896.

[31] A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Performance evaluation of signal quality monitoring techniques for GNSS multipath detection and mitigation," presented at the Int. Tech. Symp. Navigat. Timing, 2017.

[32] M. Irsigler, G. W. Hein, and B. Eissfeller, "Multipath performance analysis for future GNSS signals," in *Proc. ION NTM*, San Diego, CA, USA, Jan. 2004, pp. 225–238.

[33] J. Wu and A. G. Dempster, "'BOC-Gated-PRN' a multipath mitigation technique for BOC(n,n) waveforms," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 2, pp. 1136–1153, Apr. 2011.

[34] R. E. Phelts, T. Walter, and P. Enge, "Toward real-time SQM for WAAS: Improved detection techniques," in *Proc. ION GPS/GNSS*, Portland, OR, USA, Sep. 2003, pp. 2739–2749.

[35] O. M. Mubarak and A. G. Dempster, "Performance comparison of ELP and DELP for multipath detection," in *Proc. 22nd Int. Techn. Meeting Satell. Div. Inst. Navigat.*, Savannah, GA, USA, Sep. 2009, pp. 2276–2283.

[36] 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, 2010.

[37] 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.

[38] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS signal authentication," *IEEE Trans. Aerosp. Electron. Syst.*, to be published.

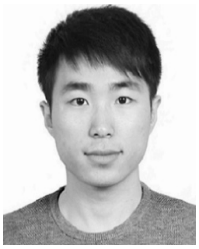
[39] T. E. Humphreys, D. Shepard, and J. A. Bhatti, "A testbed for developing and evaluating GNSS signal authentication techniques," in *Proc. Int. Symp. Certification GNSS Syst. Services (CERGAL)*, Dresden, Germany, 2014, pp. 1–15. [Online]. Available: http://rnl.ae.utexas.edu/images/stories/files/papers/tb.pdf

[40] 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. ION GNSS*, Nashville, TN, USA, 2012, pp. 3569–3583.

[41] A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Characterization of signal quality monitoring techniques for multipath detection in GNSS applications," *Sensors*, vol. 17, no. 7, p. 1579, 2017.

[42] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach* (Applied and Numerical Harmonic Analysis). Boston, MA, USA: Birkhäuser, 2007.

[43] E. G. Manfredini, B. Motella, and F. Dovis, "Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests," in *Proc. ION GNSS*, Tampa, FL, USA, 2015, pp. 3100–3106.



CHAO SUN was born in 1990. He received the B.S. degree in electronic and information engineering from Beihang University in 2013, where he is currently pursuing the Ph.D. degree with the Department of Electronic and Information Engineering.

Since 2017, he has been a Visiting Ph.D. Student with The Australian Centre for Space Engineering Research, University of New South Wales, Sydney, NSW, Australia. His research focuses on GNSS multipath mitigation, GNSS spoofing, and anti-spoofing techniques.

JOON WAYN CHEONG received the Ph.D. degree from the University of New South Wales (UNSW), where he cracked the Locata pseudolite positioning system's code and derived high-sensitivity GPS signal acquisition algorithms. He is currently a Research Associate with the School of Electrical Engineering, UNSW, where he is 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 GNSS field include weak signal acquisition, GNSS/pseudolite integrated signal processing, and GNSS interference and spoofing.

ANDREW G. DEMPSTER (M'92–SM'03) 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 in efficient circuits for signal processing arithmetic from the University of Cambridge, Cambridge, U.K., in 1995.

He was a System Engineer and the 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 received the Ph.D. degree in communication and information system from Beihang University, Beijing, China, in 2012. He is currently an Assistant Research Fellow 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.

WENQUAN FENG received the Ph.D. degree in communication and information system from Beihang University, Beijing, China. He has been teaching as the Dean of studies at Beihang University since 2011, where 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.