International Global Navigation Satellite Systems Association
IGNSS Conference 2018

Colombo Theatres, Kensington Campus, UNSW Australia
7 – 9 February 2018

Performance assessment of multi-metric joint detection technique for anti-spoofing

Chao Sun
ACSER/UNSW/Australia; Beihang University/China
sunchao@buaa.edu.cn
Joon Wayn Cheong
ACSER/UNSW/Australia
cjwayn@unsw.edu.au
Andrew Dempster
ACSER/UNSW/Australia
a.dempster@unsw.edu.au
Laure Demicheli
ACSER/UNSW/Australia
laure.demicheli@hotmail.fr
Ediz Cetin
Macquarie University/Australia
ediz.cetin@mq.edu.au
Hongbo Zhao
Beihang University/China
bhzhb@buaa.edu.cn

ABSTRACT

Spoofing, identified as a special and efficient interference attack method, has become one of the most hazardous threats for the security and integrity of global navigation satellite system (GNSS), especially for the safety critical applications such as maritime and aviation. Signal Quality Monitoring (SQM) techniques, because of its low complexity and no need for adding extra antennas, are recently found to be a feasible countermeasure against spoofing attacks. Various SQM metrics have been developed and evaluated for this purpose. However, due to the extremely low signal to noise ratio of the GNSS signal, detection methods just using single metric suffer from high false alarm probability, which limits the practical application of SQM-based anti-spoofing techniques. This paper investigated how to combine various SQM metrics together to achieve joint detection against a sneak spoofing attack. The so called "OR" and "AND" combination strategies are proposed, and the analysis of detection probability and false alarm probability are given. The anti-spoofing ability of the joint detection method has been validated using the Texas Spoofing Test Battery (TEXBAT) dataset. The results show that multi-metric joint detection technique using "OR" combination strategy is advantageous in the detection of spoofing attacks.

KEYWORDS: Spoofing detection, signal quality monitoring (SQM), multi-metric, joint detection

1. INTRODUCTION

Global Navigation Satellite System (GNSS) has become ubiquitous in daily life, to an extent that the position delivered by GNSS systems has become embedded in an increasing number of critical systems. However, given their low received power levels, GNSS open service signals are very susceptible to interference such as spoofing and meaconing, which threatens the security and integrity of GNSS. Hence, alleviating GNSS-infrastructure vulnerability to spoofing has critical importance for the GNSS application, especially for the safety critical applications such as maritime and aviation.

Spoofing, as one of the most dangerous threats for the user receivers, is a deliberate interference that intends to manipulate the victim GNSS-receiver into generating false position or navigation solutions by broadcasting a counterfeit GNSS-like signal [1]. Unlike the military GNSS signals, the civil GNSS signals are not encrypted and their structure is precisely specified in public-available documents. Thus, any person with bad intentions and strong GNSS knowledge could generate such fake GNSS signals.

Typically, spoofing attacks can be concluded into three main categories: simplistic attack, intermediate attack and sophisticated attack. The simplistic attack employs a GNSS simulator along with a RF front-end to imitate authentic GNSS signals. This technique has lowest complexity and good effectiveness on the stand-alone commercial receivers without any countermeasures. But it can be detected easily by different anti-spoofing techniques. Intermediate attack utilizes a receiver to gain accurate knowledge of the target receiver antenna's position and velocity. Thus, this mode of attack would be implementable and formidable for most known spoofing countermeasures. The sophisticated attack uses multiple receiver-spoofers jointly to generate counterfeit signals. It is able to defeat multi-antenna receiver technique [2] but less practical because of its high complexity. As the intermediate attack poses the greatest threat, we mainly concentrate on the detection of this category in this paper.

Several studies have been launched to cope with the spoofing threats during the last decade. The first type of anti-spoofing techniques was built either based on cryptographic modulation of the civil GNSS signal [3] or on receiver antenna defence techniques [4],[5],[6]. However, massive drawbacks disable their implementation feasibility. Indeed, the cryptographic techniques would imply a changing in GPS infrastructure specification or a secured network creation, while the economic cost of adding two or more antennas to the commercial receiver is impractical for GNSS users. Recent studies and publications try to avoid such needs using methods based on the signal power monitoring [7], time of arrival (TOA) discrimination and consistency checks among different measurements [1].

Signal Quality Monitoring (SQM) techniques, originally designed for multipath detection and waveform deformation monitoring [8], are recently found to be useful to identify the deformation on the correlation function due to an intermediate spoofing attack. SQM metrics are computed from the GNSS receiver correlator outputs. Three points, Early, Prompt and Late, are picked on the complex correlation function of the signal as illustrated in Figure 2. Various SQM metrics have been developed, and some of them have been verified to be effective for spoofing detection. For example, [9] verified the Ratio test metric over a set of spoofing scenarios. Detailed performance assessment related to Ratio metric has also been done [10][11]. The early-late phase metric (ELP) was developed for multipath detection and estimation, employing the phase difference between the early and late correlator outputs

[12][13]. It has been identified to be a useful discriminator to detect the presence of spoofing. Besides, the magnitude difference metric (MD) is another plausible VSD-type spoofing detection metric. It offers symmetry like Delta metric but operates with the magnitude of noncoherent integration result instead of the correlation output of I channel.

Typically, higher probability of detection and lower probability of false alarm corresponds to a better algorithm. However, due to the very low signal to noise ratio of GNSS signal, detection methods using single metrics achieve an acceptable probability of detection, but in the meanwhile suffer from a quite high false alarm probability. which limits the practical application of the SQM-based anti-spoofing techniques. The above imperfection prompts us to consider if different metrics can be used jointly to construct a "better" metric. The joint detection technique is expected to combine the advantages of each single metric and improve the overall anti-spoofing performance to some extent.

This paper focuses on the SQM-based technique and analyses the multi-metric joint detection technique for GNSS intermediate spoofing detection. The basic principle of intermediate spoofing attacking process is explained at first, showing its effect on correlation function. Then, four different SQM metrics for spoofing detection are discussed and evaluated, respectively. At last the paper presented two metric combination strategies, "OR" mode and "AND" mode, and discussed the combinations with two, three, and four different metrics. The TEXBAT dataset was used to assess the performance of the joint detection technique and results show that the so called "OR" mode brings performance improvement compared with the single metric cases.

2. INTERMEDIATE SPOOFING ATTACK PATTERN

Prior to the introduction of the new spoofing detection method, a simple review of the intermediate spoofing attack pattern is first given in this section. During an intermediate spoofing attack, the spoofer generates a counterfeit signal for each satellite signal used in the navigation solution. For each target signal, the spoofer first performs acquisition and tracking of the authentic signal to obtain its precise navigation and timing data. With such data the spoofer is then able to generate the counterfeit signal and broadcast it to the victim GNSS receiver following a specific spoofing attack pattern [14] depicted in Figure 1.

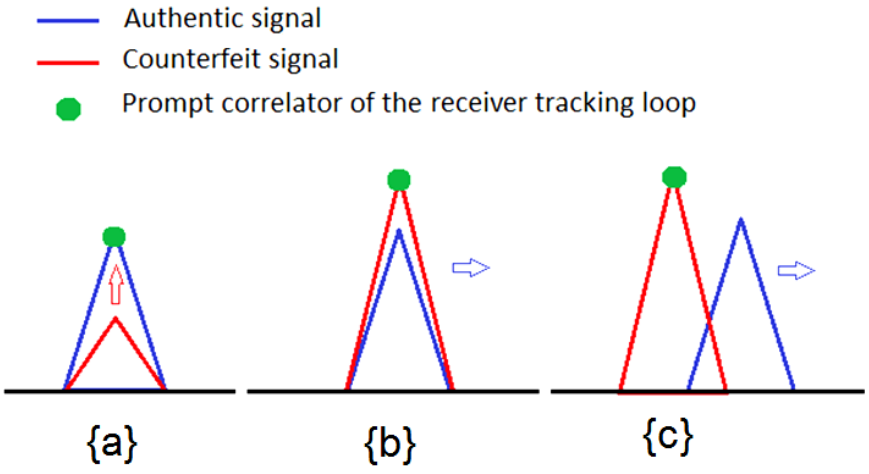

Figure 1 The intermediate spoofing attack pattern.

When the counterfeit signal is broadcasted by the spoofer, the combination of authentic and counterfeit signals reaches the antenna of the victim receiver. At the beginning of the attack, the spoofed signals are generated with the same code delay and Doppler shift as authentic signal to ensure that their correlation functions are perfectly aligned with each other. Initially the counterfeit signal power is very low, remaining below the noise floor, in order not to draw the attention of the target receiver. Then the spoofer gradually increases the power of the spoofed signal and finally exceeds the authentic signal's power level. At this point, the spoofer has taken control of the victim receiver's tracking loop. Thereafter, a lift-off occurs as illustrated in Figure 1{c}. The spoofer slowly leads the spoofed signal away from the authentic signal excluding definitively the latter from receiver's tracking results. Thus, the spoofer manipulates the receiver by making it believe it is still tracking the same authentic signal while it is tracking the counterfeit one. It is worth noting that during the entire attack, the tracking loop of the victim receiver always keeps locked, which results in the difficulty for the receiver to be aware of the danger.

During the interactions between authentic and counterfeit signal, as both the authentic and the counterfeit signal reach the victim receiver, the receiver tracks a distorted composite signal. It is likely that the receiver alternates several times between tracking the authentic correlation peak and the counterfeit one before finally choosing to track the counterfeit signal. Thus, the two signals are to some extent struggling to control the receiver's code and carrier tracking loops during a certain amount of time. Phase and power of the signal admixture will fluctuate strongly and frequently at this moment and during the period when the authentic signal is moving away from the counterfeit signal. Such fluctuation affects the complex correlation shape and thus also affects the correlator output values I_E, I_L, Q_E, Q_L, I_P, and Q_P.

3. DESCRIPTION OF DETECTION METRICS

3.1 Detection Metrics

SQM techniques were firstly used for multipath detection and their performances in this domain have been deeply assessed. However, the structures of the spoofed and multipath signal are very similar, so the SQM metrics are also extended to the area of spoofing detection. SQM metrics are computed from the GNSS receiver correlator outputs. Three points, Early, Prompt and Late, are picked on the complex correlation function of the signal as illustrated in Figure 2. The Prompt correlator corresponds to the correlation function peak for an ideal DLL tracking loop. Early and Late correlator outputs are spaced by *d* chips, respectively ahead and behind the Prompt correlator, where *d* is called the correlator spacing. The complex correlation function is computed as:

$$x(t) = I(t) + jQ(t) \tag{1}$$

where $I(t)$ is the In-Phase and $Q(t)$ is the Quadrature component of the complex correlation function. The magnitude of the complex correlation function is computed as:

$$\left|x(t)\right| = \sqrt{I(t)^2 + Q(t)^2} \tag{2}$$

Figure 2 shows the complex correlation component in the presence of spoofing signal. $I_{E,d}(t)$, $I_{P,d}(t)$ and $I_{L,d}(t)$ refers to the Early, Prompt and Late In-Phase correlator output at

time t, respectively; $Q_{E,d}(t)$, $Q_{P,d}(t)$ and $Q_{L,d}(t)$ denote the Early, Prompt and Late Quadrature correlator output at time t, respectively. We can see that both In-Phase and Quadrature correlation functions are severely distorted due to the spoofing attack which allows us to develop countermeasures by analysing these correlator outputs.

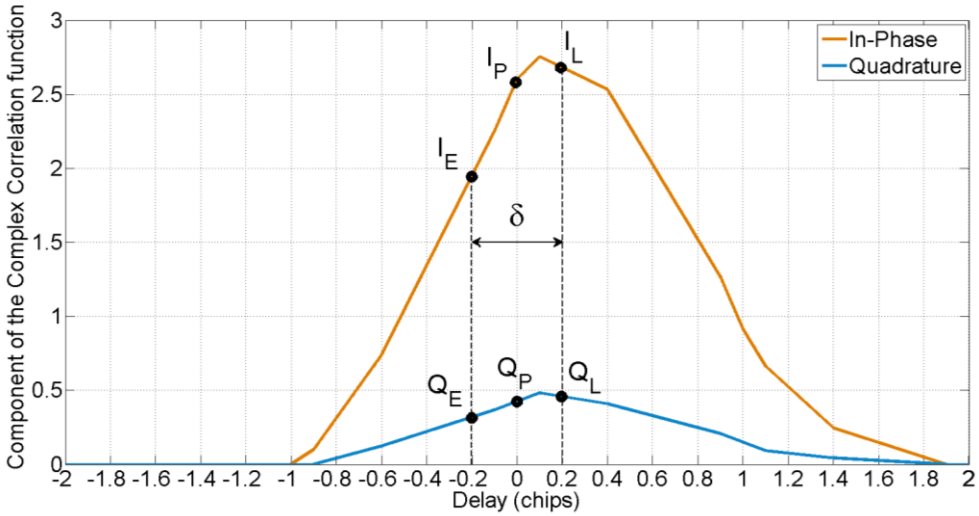

Figure 2 In-Phase and Quadrature complex correlation component at time t. *d* =0.2 chip.

Employing the multiple samples of the complex correlation function given above, different strategies have been proposed to compute metrics. In this paper, we mainly consider the following four metrics:

(1) Delta Metric:

$$\Delta_d(t) = \frac{I_{E,d}(t) - I_{L,d}(t)}{2I_P} \tag{3}$$

(2) Ratio Metric:

$$RT_d = \frac{I_{E,d}(t) + I_{L,d}(t)}{2I_P} \tag{4}$$

(3) Early Late Phase Metric [13]:

$$ELP_d(t) = tan^{-1}\left(\frac{Q_{L,d}(t)}{I_{L,d}(t)}\right) - tan^{-1}\left(\frac{Q_{E,d}(t)}{I_{E,d}(t)}\right) \tag{5}$$

(4) Magnitude Difference Metric:

$$MD_d(t) = \frac{|x_{E,d}(t)| - |x_{L,d}(t)|}{2|x_P|} \tag{6}$$

4. PERFORMANCE ANALYSIS

In this section, we first give the theoretical performance of single metric, and then two metric combination strategies, “OR” mode and “AND” mode, are introduced. Finally, we discuss the possible performance changing for multi-metric joint detection technique using the two strategies.

4.1 Single metric

The spoofing detection method is 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.

Generally, the threshold value is a function of the designated false alarm probability (*Pfa*) and the level of thermal noise. For a fixed C/N_0, the final *Pfa* and *Pd* can also be seen as functions of the threshold value. According to [16], the value of test metric M_i can be approximated as a Gaussian distributed variable in some conditions regarding a clear data (the considered signal is not affected by spoofng), i.e., $M_i \sim \left(\mu_i, \sigma_i^2\right)$. Under this hypothesis, for certain thresholds Th_u and Th_l, *Pfa* is computed as follows:

$$P_{fa} = \int_{Th_u}^{\infty} f_c\left(x\right)\mathrm{d}x + \int_{-\infty}^{Th_l} f_c\left(x\right)\mathrm{d}x = erfc\left(\frac{Th_u - \mu_i}{\sqrt{2\sigma_i^2}}\right) = erfc\left(\frac{\mu_i - Th_l}{\sqrt{2\sigma_i^2}}\right) \tag{7}$$

where $f_c\left(x\right)$ represents the probability density function of the clear signal. Then we can get the expressions of two thresholds as

$$\begin{aligned} Th_u &= \mu_i + \sqrt{2\sigma_i^2}\,erfc^{-1}\left(P_{fa}\right) \\ Th_l &= \mu_i - \sqrt{2\sigma_i^2}\,erfc^{-1}\left(P_{fa}\right) \end{aligned} \tag{8}$$

Finally, employing the threshods we obtain above, the probability of detection can be written as

$$P_d = \int_{Th_u}^{\infty} f_s\left(x\right)\mathrm{d}x + \int_{-\infty}^{Th_l} f_s\left(x\right)\mathrm{d}x \tag{9}$$

where $f_s\left(x\right)$ denotes the probability density function of a metric in the presence of a spoofing attack. Equation (7), (8) and (9) can also be found in [16]. We can see that, in order to calculate Pfa and Pd, the metric distributions for both spoofing-absent and spoofing-present circumstances have to be obtained. However, the distributions of metrics in the presence of a spoofing detection can be complicated. Besides, they also depend on the number of samples of correlator's outputs, the receiver's sampling frequency and the specific spoofing attack pattern. It is impractical to derive the analytical expression of the probability density functions. So this paper evaluates the performance using the statistical method. The distribution of each SQM metric is analyzed and computed using the dataset processed by the Matlab software. Then by varying the threshold values, we are able to obtain the P_{fa} and P_d curves versus threshold values. Furthermore, we plot the receiver operator characteristic (ROC) curves with horizontal axis of P_{fa} and vertical axis of P_d. One of benefits of such process is we can get the actual ROC curves without the knowledge of the exact mathematical expression of the probability distribution.

4.2 Multi-metric Combinations

Different from the cases of single metric, the muti-metric joint detection is more complicated.

There are various ways to construt the metric combinations. For example, we can choose two from the total four metrics to form the joint metric. Also, we can choose three or four metrics for joint detection. Besides, there are also different methods to decide wether the joint metric is finally triggered. One such strategy is that the joint metric is triggered as long as one metric exceeds its threshold. It is called "OR" mode, denoted as $\mathrm{OR}(\cdot)$ in this paper. Another possible strategy is the joint metric will be triggered only when all the metrics exceed their thresholds. This is called "AND" mode, denoted as $\mathrm{AND}(\cdot)$. The final performance would vary signicantly with different metrics and different combination modes we use.

Assuming that *n* SQM metris are jointly used for spoofing detection, for *i*-th metric, it has a threshold Th_i to determine the false alarm rate of Pfa_i and detection probability of Pd_i. As the "OR" mode and "AND" mode behave differently about how to combine metrics together, the overall false alarm probability of detetction probability are also in different mathematical forms.

(a) "OR" mode

For a set of given thresholds, Th_1, Th_2,…, Th_n, the overall probability of false alarm is given by:

$$\begin{aligned} P_{fa,or} &= 1-\left(1-P_{fa,1}\right)\cdot\left(1-P_{fa,2}\right)\cdot\ldots\cdot\left(1-P_{fa,n}\right) \\ &= 1-\prod_{i=1}^{n}\left(1-P_{fa,i}\right) \end{aligned} \tag{10}$$

Now let's compare $P_{fa,or}$ with each single false alarm probability $P_{fa,i}$. Firstly, for each $P_{fa,i}$, as the value of $P_{fa,i}$ is between 0 and 1, we can get $\left(1-P_{fa,1}\right)\cdot\left(1-P_{fa,2}\right)<1-P_{fa,1}$. And then $P_{fa,or}^{(2)}=1-\left(1-P_{fa,1}\right)\cdot\left(1-P_{fa,2}\right)>1-(1-P_{fa,1})=P_{fa,1}$. Similarly, we can also have $P_{fa,or}^{(2)}=1-\left(1-P_{fa,1}\right)\cdot\left(1-P_{fa,2}\right)>1-(1-P_{fa,2})=P_{fa,2}$. This means when we use two metrics together with a "OR" mode, the final $P_{fa,or}^{(2)}$ is larger than each single false alarm rate, $P_{fa,1}$ and $P_{fa,2}$.

Now consider the case of combination of three metrics. As $\left(1-P_{fa,1}\right)\cdot\left(1-P_{fa,2}\right)\cdot\left(1-P_{fa,3}\right)<\left(1-P_{fa,1}\right)\cdot\left(1-P_{fa,2}\right)$, we have

$$P_{fa,or}^{(3)}=1-\left(1-P_{fa,1}\right)\cdot\left(1-P_{fa,2}\right)\cdot\left(1-P_{fa,3}\right)>1-\left(1-P_{fa,1}\right)\cdot\left(1-P_{fa,2}\right)=P_{fa,or}^{(2)} \tag{11}$$

Finally, the overall false alarm probability should meet the following relationship:

$$P_{fa,or}^{(n)}>\ldots>P_{fa,or}^{(i)}>\ldots>P_{fa,or}^{(2)}>\max\{P_{fa,1},P_{fa,2},\ldots,P_{fa,i}\} \tag{12}$$

This equation shows us that the combination of multi-metric has false alarm rate higher than that of each single metric. Besides, as the number of metrics gets larger, the overall false alarm rate will further increase. Like the analysis of false alarm probability, the overall probability of detection for "OR" mode can be directly given by:

$$\begin{aligned} P_{d,or} &= 1-\left(1-P_{d,1}\right)\cdot\left(1-P_{d,2}\right)\cdot\ldots\cdot\left(1-P_{d,n}\right) \\ &= 1-\prod_{i=1}^{n}\left(1-P_{d,i}\right) \end{aligned} \tag{13}$$

So, we also have the relationship:

$$P_{d,or}^{(n)} > \ldots > P_{d,or}^{(i)} > \ldots > P_{d,or}^{(2)} > \max\{P_{d,1}, P_{d,2}, \ldots, P_{d,i}\} \tag{14}$$

Although the increase of false alarm rate is not a desirable result, it does not mean the combination of multi-metrics using "OR" mode has worse performance than detection methods just using single metric. This is because the detection probability is also getting larger when multi-metric is jointly used, which may be helpful to compensate the increase of false alarm rate and boost the final algorithm performance. Just as illustrated in Figure 3 (a), the increase of both P_{fa} and P_d may lead to the final performance loss (denoted by the red arrow) or bring in performance gain (denoted by the green arrow), which depends on the actual conditions.

(b) "AND" mode

In the case of "AND" mode, the joint metric is triggered only when all the metrics exceed their thresholds. So for a same set of thresholds, Th_1, Th_2,…, Th_n, the overall probability of false alarm can be simply written as:

$$P_{fa,\text{and}} = P_{fa,1}\cdot P_{fa,2}\cdot\ldots\cdot P_{fa,n} = \prod_{i=1}^{n} P_{fa,i} \tag{15}$$

Also, overall the probability of detection in the case of "AND" mode is given by：

$$P_{d,\text{and}} = P_{d,1}\cdot P_{d,2}\cdot\ldots\cdot P_{d,n} = \prod_{i=1}^{n} P_{d,i} \tag{16}$$

As both $P_{fa,i}$ and $P_{d,i}$ are larger than 0 but smaller than 1, it can be seen clearly that the combination of different metrics will cause reductions of both P_{fa} and P_d, namely:

$$P_{fa,\text{and}}^{(n)} < \ldots < P_{fa,\text{and}}^{(i)} < \ldots < P_{fa,\text{and}}^{(2)} < \min\{P_{fa,1}, P_{fa,2}, \ldots, P_{fa,i}\} \tag{17}$$

$$P_{d,\text{and}}^{(n)} < \ldots < P_{d,\text{and}}^{(i)} < \ldots < P_{d,\text{and}}^{(2)} < \min\{P_{d,1}, P_{d,2}, \ldots, P_{d,i}\} \tag{18}$$

As illustrated in Figure 3 (b), although the total $P_{fa,\text{and}}^{(n)}$ decreases, it is still uncertain that the "AND" combination mode brings us performance gain compared with the cases of single metric. That is because it also suffers a loss of overall P_d. Thus, thorough and quantitative test is needed for effective comparison.

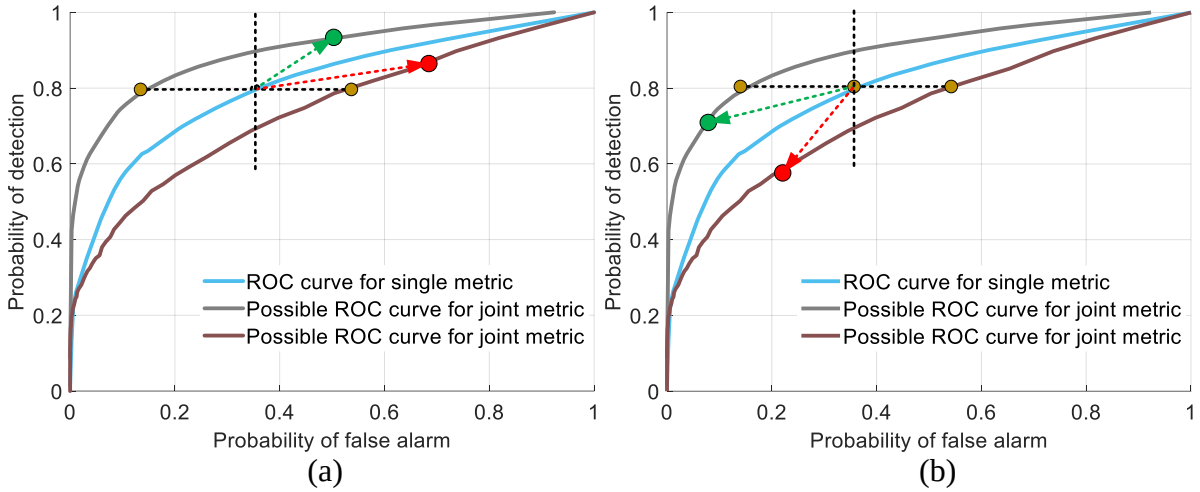

Figure 3 Possible false alarm probability and detection probability changings due to joint detection. (a) is for "OR" mode and (b) is for "AND" mode.

5. TEST ON REAL DATA

In this section, we evaluate the spoofing detection performance of the SQM-based anti-spoofing methods using either single metrics or metric combinations over real dataset. The data, named TEXBAT, is part of a test battery of real cases publicly provided by the University of Texas at Austin. The scenario used is the Static Matched-Power Time Push, which is listed as number 3 of all the available scenarios. Signals were tracked using a NordNav GPS software receiver. This scenario includes a spoofer with a low power advantage over the authentic signal (+1.3 dB) that performs a time push from seconds 150 to 300 of the total simulation time. The PRN used here is 3.

Scenario Description	Spoofing Type	Platform Mobility	Power Adv.(dB)	Frequency Lock
1: Static Switch	N/A	Static	N/A	Unlocked
2: Static Overpowered	Time	Static	10	Unlocked
3: Static Matched-Power	Time	Static	1.3	Locked
4: Static Matched-Power	Position	Static	0.4	Locked
5: Dynamic Overpowered	Time	Dynamic	9.9	Unlocked
6: Dynamic Matched-Power	Position	Dynamic	0.8	Locked

Table 1 Texas Spoofing Test Battery: Scenarios Summary [15]

5.1 Single metric

In the beginning, we make a comparison of detection performance between four single metrics. The typical profile of metrics responses to a spoofing attack is illustrated in Figure 4. For the second stage of a spoofing attack, both authentic and counterfeit signals reach the receiver and interact with each other. They lead to distortion of the correlation function of the mixed-signal and bring in noticeable risings and declines of the metric values over time from the 150th to the 300th second. Whereas for the first stage (before the 150th second) and the third stage (after the 280th second), because either the authentic signal or the counterfeit signal is stably tracked, the final metric values keep a steady behaviour. Thus, we can detect the attack during the second stage of the spoofing attack, thanks to these remarkable metrics variations.

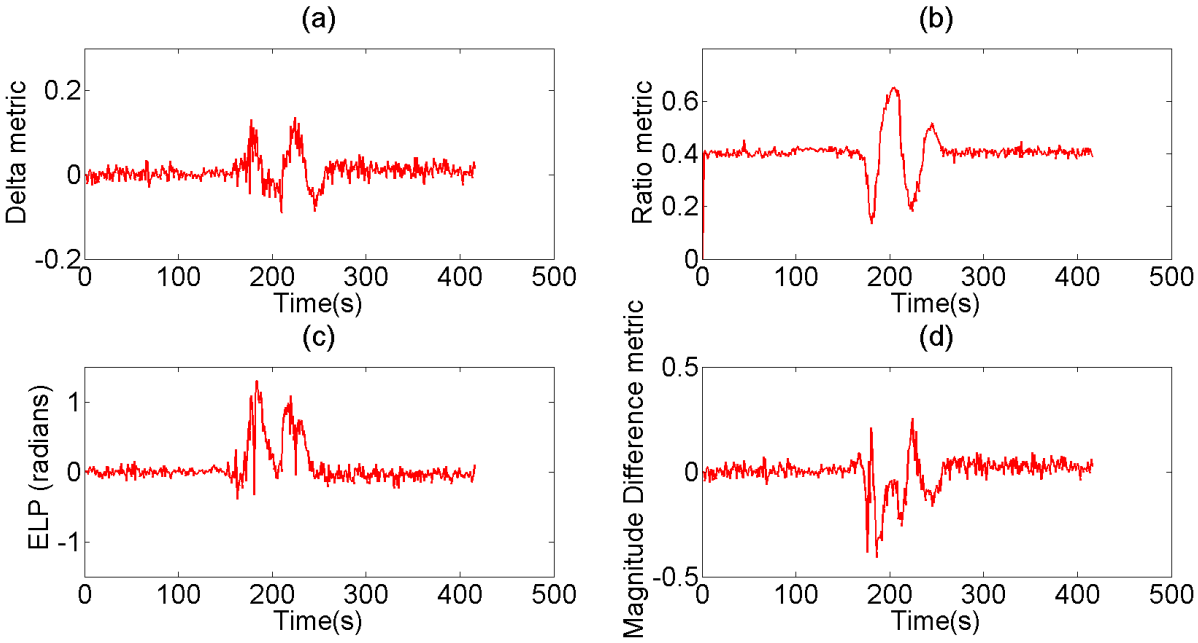

Figure 4 Four metrics responses to a Matched-Power spoofing scenario: scenario 6 from TEXBAT and computed with a 0.5 chip correlator spacing.

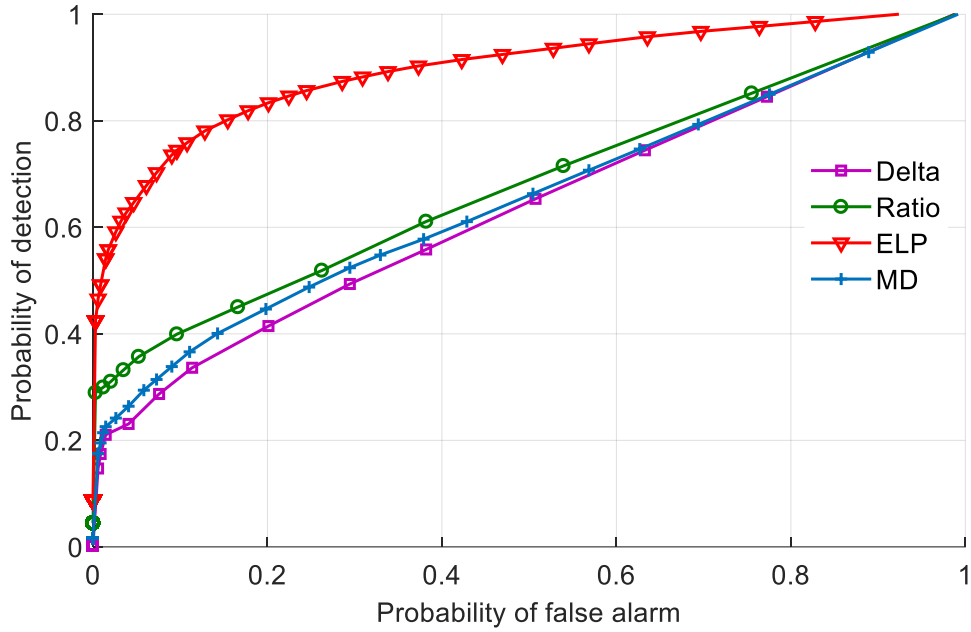

Figure 5. ROC curves employing the dataset of TEXBAT scenario 3—Static Matched-Power Time Push, with the power advantage of 1.3 dB. The correlator spacing used here is 0.4 chip.

Figure 5 shows the ROC curves of each metric using the above dataset and the threshold computation method explained in section 4. We can see that the Delta metric, Ratio metric, and MD metric have quite similar performance, whereas, the ELP metric significantly outperforms the other three metrics. This is probably because the spoofing attack can cause dramatic phase fluctuation between the Early and Late correlator outputs, which better indicates an underlying spoofing attack.

5.2 Combinations of multi-metric

In this subsection, the results of two-metric, three-metric and four-metric combinations will be presented in turn.

a) Combinations of two metrics

When two metrics are picked out from total four metrics to form one choose, there will be 6 different combinations: (Delta, Ratio), (Delta, ELP), (Delta, MD), (Ratio, ELP), (Ratio, MD), (ELP, MD). Figure 6 shows the ROC curves of various two-metric combinations in OR mode. The ROC curves using four single metrics are also presented for comparison. We can see that the combinations of two metrics always outperform each single metric. For example, all three curves related to the ELP metric perform better than the single ELP metric. Besides, OR(ELP, Ratio) has higher probability of detection than either ELP metric and Ratio metric. Compared with ELP metric, the detection probability has been improved by more than 0.05 averagely, and compared with Ratio metric, this performance improvement is even more significant. Thus, using two metrics jointly in OR mode is an efficient way to enhance the spoofing detection performance.

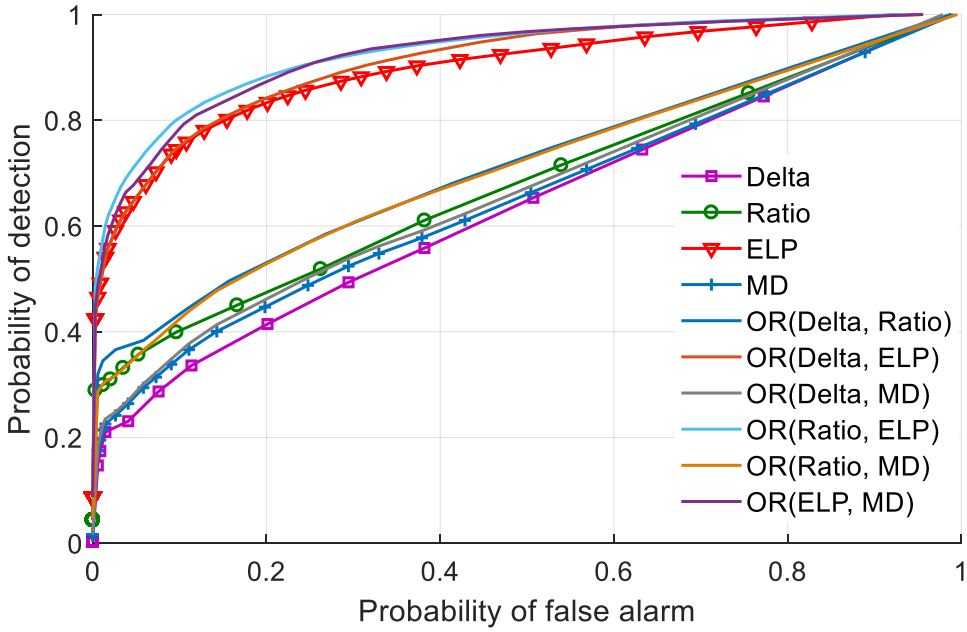

Figure 6. ROC curves for combinations of two metrics using "OR" Strategy.

Figure 7 plots the ROC curves for six two-metric combinations using AND strategy. Compared with OR mode, the AND mode does not show any performance gain. It seems to have performance between the two metrics it uses, and sometimes even worse than both two metrics.

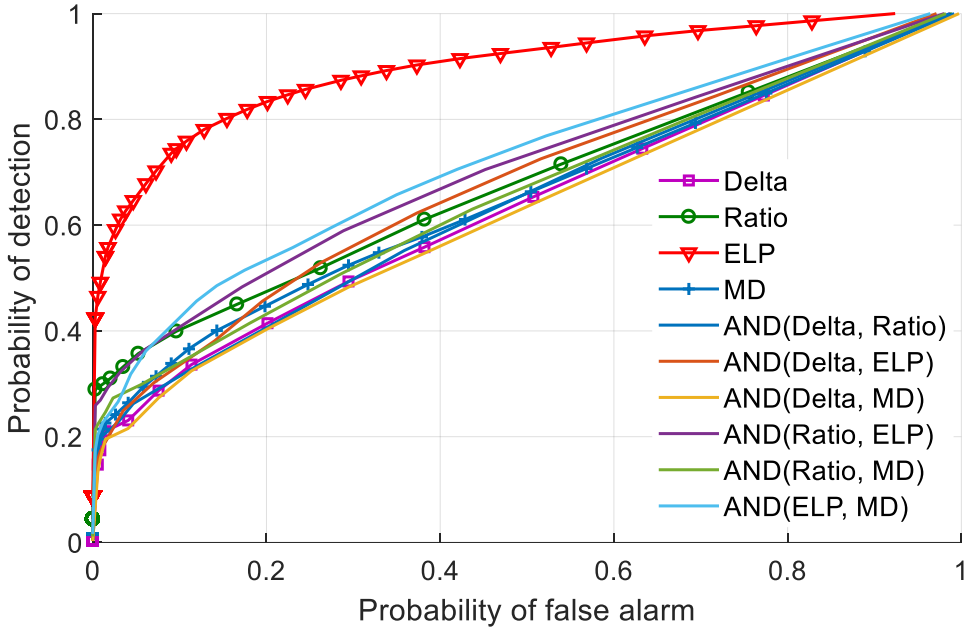

Figure 7. ROC curves for combinations of two metrics using "AND" Strategy.

b) Combinations of three metrics

Whereas for three-metric combinations, there will be four different combinations when choosing three metrics from total four metrics: (Delta, Ratio, ELP), (Delta, Ratio, MD), (Delta, ELP, MD) and (Ratio, ELP, MD). Figure 8 illustrates the ROC curves for three-metric combinations in OR mode. It can be seen that OR(Delta, Ratio, ELP), OR(Delta, ELP, MD) and OR(Ratio, ELP, MD) all have better detection probability than the single ELP metric for a given false alarm rate. But they have quite similar performance with OR(Ratio, ELP), which means the performance gain obtained from two-metric to three-metric combinations is rather limited, and even can be ignored. Besides, just as expected, the only metric combination that is not related to the ELP metric shows the worst performance among all choices.

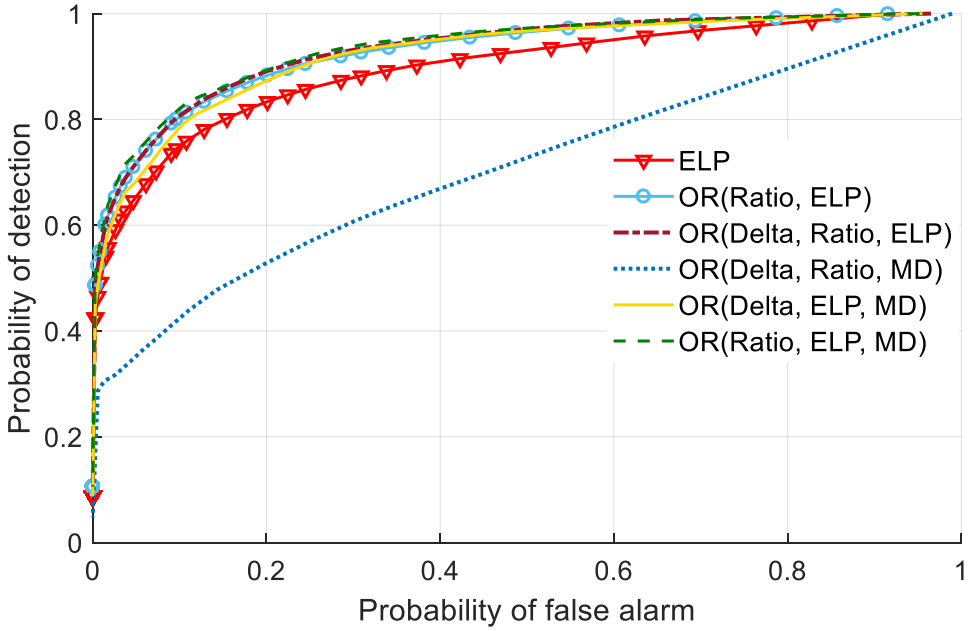

Figure 8. ROC curves for combinations of three metrics using "OR" Strategy.

Figure 9 shows the ROC curves using three-metric combinations in AND mode. The results of single ELP metric and OR(Ratio, ELP), as the best single-metric and two-metric combination, are kept for comparison. It is clear that the four AND combinations have similar performance and still shows no performance improvement compared with single ELP metric and OR(Ratio, ELP).

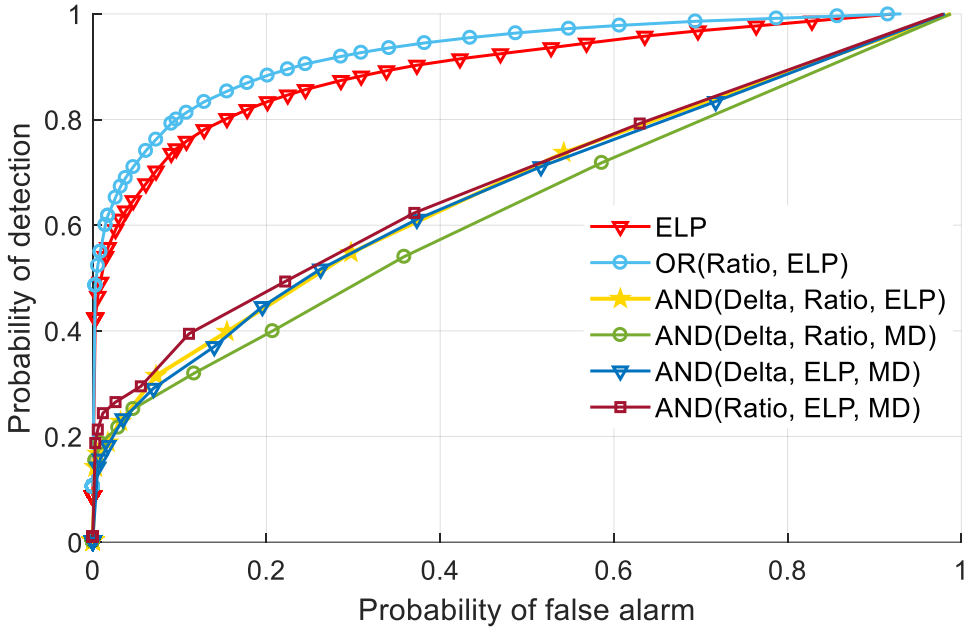

Figure 9. ROC curves for combinations of three metrics using "AND" Strategy.

c) Combinations of four metrics

In the end, we plot the ROC curves for the four-metric combination with both "OR" and "AND" strategies. From Figure 10 we can see that the OR(all four metrics) performs just a little better than OR(Ratio, ELP), and this again indicates that using more metrics together may not definitely bring significant performance gain compared with the cases only using two metrics. But the four-metric joint detection will lead to an increase of algorithm complexity, which is not desirable. Thus, a combination of two metrics achieves a balance between the detection performance and computation load. In addition, the AND(all four metrics) still has the worst performance among the choices in Figure 10, which demonstrates again the AND strategy is not an efficient way to combine different metrics into a better one and it will not be recommended in the practical applications.

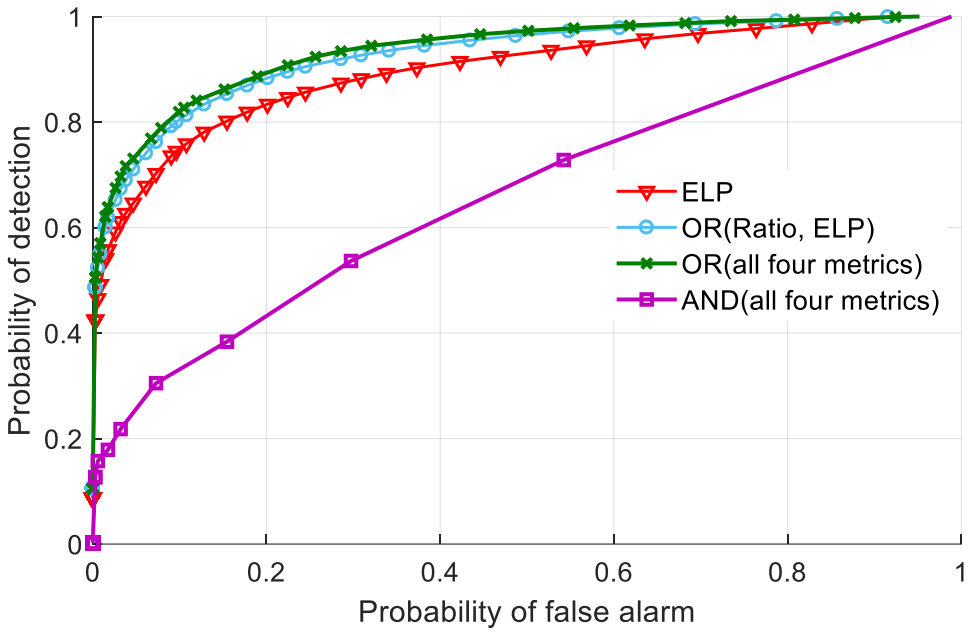

Figure 10. ROC curves for combinations of four metrics using "OR" and "AND" Strategies.

6. CONCLUSIONS

This paper has discussed the multi-metric joint detection technique for anti-spoofing, trying to combine different metrics together to perform spoofing detection rather than only using single SQM metric. Two different combination strategies have been analysed and the cases of using two metrics, three metrics and all four metrics have been discussed. The performance has been evaluated using the Texas Spoofing Test Battery (TEXBAT) dataset in the form of ROC curves. Results show that, compared with the detection methods only using single metric, the multi-metric combination technique in "OR" mode has higher ROC performance, whereas, the metric combinations in "AND" mode show no performance improvement compared with single metric, which is not recommended in the practical applications. Besides, performance gain obtained by increasing the number of metrics used for joint detection is limited, thus a combination of two metrics, achieving a balance between the detection performance and computation load, would be the best choice.

REFERENCES

[1] Jafarniajahromi A, Broumandan A, Nielsen J, et al. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques[J]. International Journal of Navigation & Observation, 2012, 2012(9).

[2] Montgomery P Y, Humphreys T E, Ledvina B M. Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense Against a Portable Civil GPS Spoofer[J]. Proceedings of the International Technical Meeting of the Institute of Navigation Itm, 2009, 1(1):124-130.

[3] Wesson, K., Rothlisberger, M., & Humphreys, T. (2012). Practical cryptographic civil GPS signal authentication. Navigation, 59(3), 177-193.

[4] Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2011). Civilian GPS spoofing detection based on dual-receiver correlation of military signals. Proceedings of the Institute of Navigation GNSS (ION GNSS 2011).

[5] Montgomery, P. Y., Humphreys, T. E., & Ledvina, B. M. (2009). A multi-antenna defense: Receiver-autonomous GPS spoofing detection. Inside GNSS, 4(2), 40-46.
[6] [Konovaltsev, A., Cuntz, M., Haettich, C., & Meurer, M. (2013). Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array. Proc. ION GNSS+ 2013, 17-20.
[7] Jahromi A J, Broumandan A, Nielsen J, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements[J]. International Journal of Satellite Communications & Networking, 2012, 30(4):181-191.
[8] Phelts RE (2001) Multicorrelator techniques for robust mitigation of threats to GPS signal quality. Doctoral dissertation, Stanford University
[9] Manfredini E G, Dovis F, Motella B. Validation of a signal quality monitoring technique over a set of spoofed scenarios[C]// Satellite Navigation Technologies and European Workshop on Gnss Signals and Signal Processing. IEEE, 2014:1-7.
[10] Yang Y, Li H, Lu M. Performance Assessment of Signal Quality Monitoring Based GNSS Spoofing Detection Techniques[J]. 2015.
[11] Jahromi A J, Broumandan A, Daneshmand S, et al. Galileo signal authenticity verification using signal quality monitoring methods[C]// International Conference on Localization and Gnss. IEEE, 2016:1-8.
[12] Mubarak O M, Dempster A G. Performance comparison of ELP and DELP for multipath detection[C]// International Technical Meeting of the Satellite Division of the Institute of Navigation. 2009:2276-2283.
[13] Mubarak O M, Dempster A G. Analysis of early late phase in single-and dual-frequency GPS receivers for multipath detection[M]. Springer-Verlag New York, Inc. 2010.
[14] Humphreys T E, Ledvina B M, Psiaki M L, et al. “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,”[C]// International Technical Meeting of the Satellite Division of the Institute of Navigation. 2008:2314-2325.
[15] Humphreys, T. E., Bhatti, J. A., Shepard, D. P., & Wesson, K. D. (2012). The Texas Spoofing Test Battery: Toward a standard for evaluating GNSS signal authentication techniques. In Proceedings of the ION GNSS Meeting.
[16] Fantino M, Molino A, Mulassano P, Nicola M, Rao M (2009) Signal quality monitoring: Correlation mask based on ratio test metrics for multipath detection. In: Proceedings of the international global navigation satellite systems society (IGNSS) symposium, Gold Coast, Australia, December, pp 1–3