IET Radar, Sonar & Navigation

Research Article

IET Journals
The Institution of Engineering and Technology

Signal quality monitoring-based spoofing detection method for Global Navigation Satellite System vector tracking structure

ISSN 1751-8784
Received on 12th January 2020
Revised 16th February 2020
Accepted on 21st February 2020
E-First on 17th April 2020
doi: 10.1049/iet-rsn.2020.0021
www.ietdl.org

Xinran Zhang[1], Hong Li[1] ✉, Chun Yang[2], Mingquan Lu[1]

[1]*Department of Electronic Engineering, Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, People's Republic of China*

[2]*Institute of Electronic Engineering, China Academy of Engineering Physics, Mianyang 621000, People's Republic of China*

✉ *E-mail: lihongee@tsinghua.edu.cn*

Abstract: The vector tracking structure is receiving growing attention due to its better tracking performance than the traditional scalar tracking structure. For the scalar tracking structure, signal quality monitoring (SQM) methods can effectively detect spoofing attacks based on the influence of correlation peaks overlap on the coherent integration results. However, the methods are invalid when the overlap is inexistent. While for the vector tracking structure, the authors find that because of the combined tracking of all received signals, the coherent integration results are affected by spoofing attacks regardless of whether the overlap exists. It implies that SQM techniques have a wider application range for the vector tracking structure. To this end, an SQM-based spoofing detection method for the vector tracking structure is proposed in this study. Analysis and simulation results demonstrate that the proposed method is useful even in the spoofing scenarios where the correlation peaks do not overlap. And it can detect spoofing attacks on both pseudo-code and carrier Doppler by using the existing observations in the tracking process, which is highly practical for the vector tracking structure.

1 Introduction

Global Navigation Satellite System (GNSS) is the most widely used navigation and positioning infrastructure, and its security is increasingly valued. It is well accepted that due to the low power and publicly known structure of civil signals, GNSS is susceptible to jamming and spoofing [1, 2]. Jamming is to reduce the carrier-to-noise ratios of received GNSS signals by transmitting high-power signals, while spoofing is to deviate the positioning result by replacing authentic signals with counterfeited ones [3]. The counterfeited signals are similar in power and structure to the authentic ones. Spoofing may be more harmful than jamming because victim receivers generally cannot distinguish spoofing and authentic signals, which would lead to severe consequences. It also promotes the research of spoofing countermeasure techniques [4, 5].

Signal quality monitoring (SQM) techniques, initially developed for multipath detection [6, 7], have been used to detect spoofing attacks in recent years. Most SQM spoofing detection methods concentrate on the pseudo-code domain. When a spoofing signal competes with an authentic signal for taking control of a tracking loop, their pseudo-code phases are gradually approaching. Then, the pseudo-code phases will slowly separate after the tracking loop locks the spoofing signal. In this process, the correlation peaks of the authentic and spoofing signals that correspond to the same satellite will overlap, which can affect the coherent integration results that are the outputs of the early correlator, prompt correlator, and late correlator. According to this effect, the optional SQM metrics are various, such as the delta metric, the ratio metric, and the magnitude difference metric [8]. It is viable to detect spoofing attacks by observing and thresholding these metrics [9]. The particular performance assessment has been presented in [10, 11]. Besides, considering that it is possible to influence the coherent integration results in the carrier Doppler domain, a carrier Doppler SQM method is proposed to strengthen the performance and reliability of the spoofing detection [12]. This method can detect spoofing attacks on carrier Doppler by adding two correlators with slower and faster Doppler shifts, respectively, and using the difference between the slower and faster correlator outputs as a metric.

For most GNSS receivers with the traditional scalar tracking structure, SQM methods can effectively detect spoofing attacks based on the influence of correlation peaks overlap on the coherent integration results [3]. However, the scope of application is limited. SQM methods are invalid for the spoofing scenarios where the correlation peaks do not overlap.

On the other hand, the vector tracking structure is receiving growing attention due to its better tracking performance than the scalar tracking structure in low carrier-to-noise ratio environments or high dynamics [13–16] and its capability in anti-jamming [17, 18]. The vector tracking structure is based on the consistency among received signals. The consistency is reflected in that the pseudo-code phases and carrier Doppler shifts estimated from the positioning result are approximately equal to the corresponding values of the received signals [19, 20]. While when there are spoofing signals, the positioning result is incorrect [21]. Then, the pseudo-code phases and carrier Doppler shifts estimated from the incorrect positioning result are probable to deviate from the received signals' values, which mean that the consistency is destroyed. For the vector tracking structure, these deviations, as part of the input of tracking loops, eventually make locally generated signals and received signals inconsistent in the pseudo-code phase and carrier phase. Subsequently, the inconsistency can affect the coherent integration results. In short, spoofing attacks may destroy the consistency among received signals, thereby influencing vector tracking loops [22], causing the pseudo-code phase differences and carrier phase differences between received signals and locally generated signals to deviate from zero, and ultimately affecting the coherent integration results of the vector tracking structure. We underscore that this effect on the coherent integral results is due to the inconsistency among received signals, regardless of whether the correlation peaks overlap.

That is to say, not only the overlap of the correlation peaks but also the inconsistency among received signals due to spoofing attacks will affect the coherent integration results of the vector tracking structure. It implies that for the vector tracking structure, SQM techniques have a wider application range. To this end, an SQM-based spoofing detection method for the vector tracking structure is proposed in this paper. In general, the pseudo-code phase differences and carrier phase differences between received

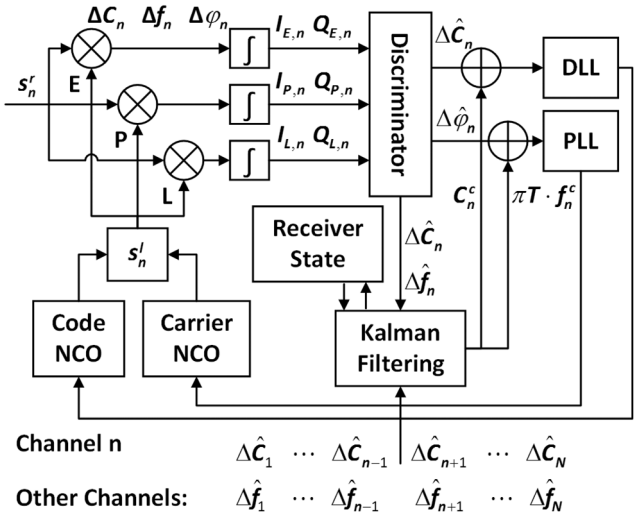

Fig. 1 *Vector tracking structure*

signals and locally generated signals are approximately equal to zero when there is no spoofing attack, but deviate from zero under spoofing attacks. Based on this, the proposed method uses the pseudo-code phase differences and carrier phase differences estimated by the coherent integration results to detect spoofing attacks.

Since the overlap of the correlation peaks has a similar effect on the coherent integration results of the vector tracking structure as that of the scalar tracking structure, to simplify the analysis, the spoofing scenarios we focus on in this paper are the cases where the correlation peaks do not overlap. We perform a detailed analysis and a series of simulations on the proposed method. Analysis and simulation results demonstrate that the proposed method is still useful for the vector tracking structure when the correlation peaks do not overlap. And it can detect spoofing attacks on both pseudo-code and carrier Doppler by using the existing observations in the tracking process, which is highly practical for the vector tracking structure.

This paper is organised as follows. In Section 2 the vector tracking structure is briefly introduced, and the pseudo-code phase differences and carrier phase differences between received signals and locally generated signals under spoofing attacks are analysed. In Section 3 the SQM-based spoofing detection method for the vector tracking structure is introduced, and its detection performance is discussed in detail. The simulation results are presented in Section 4. Conclusions are drawn in Section 5.

2 Analysis of vector tracking structure under spoofing attacks

In this section, we briefly introduce the vector tracking structure and discuss the influence of spoofing attacks on vector tracking loops. Besides, the pseudo-code phase differences and carrier phase differences between received signals and locally generated signals under spoofing attacks are emphatically analysed.

2.1 Vector tracking structure

The vector tracking structure is shown in Fig. 1. The pseudo-code phase, carrier Doppler shift, and carrier phase of the nth received signal s_n^r are C_n^r, f_n^r, and φ_n^r, respectively. For the nth locally generated signal s_n^l, the corresponding parameters are C_n^l, f_n^l, and φ_n^l. Then, the pseudo-code phase difference ΔC_n, carrier Doppler shift difference Δf_n, and carrier phase difference $\Delta\varphi_n$ between the nth received signal and locally generated signal can be expressed as

$$\begin{cases} \Delta C_n = C_n^r - C_n^l \\ \Delta f_n = f_n^r - f_n^l \\ \Delta\varphi_n = \varphi_n^r - \varphi_n^l \end{cases} \tag{1}$$

$I_{\mathrm{E},n}$, $Q_{\mathrm{E},n}$, $I_{\mathrm{P},n}$, $Q_{\mathrm{P},n}$, $I_{\mathrm{L},n}$, and $Q_{\mathrm{L},n}$ are the coherent integration results, where I represents the in-phase branch, Q represents the Quadrature branch, and the subscripts E, P, and L represent the early, prompt, and late correlators, respectively. The discriminator uses the coherent integration results to estimate ΔC_n, Δf_n, and $\Delta\varphi_n$.

Since it is inevitable that there is noise in received signals, the coherent integration results are inaccurate. So that the estimated pseudo-code phase difference $\Delta\hat{C}_n$, estimated carrier Doppler shift difference $\Delta\hat{f}_n$, and estimated carrier phase difference $\Delta\hat{\varphi}_n$, which are obtained by the coherent integration results, are not exactly equal to ΔC_n, Δf_n, and $\Delta\varphi_n$, respectively. The corresponding estimation errors εC_n, εf_n, and $\varepsilon\varphi_n$ can be shown as

$$\begin{cases} \varepsilon C_n = \Delta\hat{C}_n - \Delta C_n \\ \varepsilon f_n = \Delta\hat{f}_n - \Delta f_n \\ \varepsilon\varphi_n = \Delta\hat{\varphi}_n - \Delta\varphi_n \end{cases} \tag{2}$$

Kalman filtering in the vector tracking structure updates the receiver state $\boldsymbol{s}$ through the measured pseudo-code phases $(C_1, \ldots, C_N)$ and measured carrier Doppler shifts $(f_1, \ldots, f_N)$ of all received signals, where N represents the number of received signals. $\boldsymbol{s}$ consists of the position (x_u, y_u, z_u), velocity (x_u^v, y_u^v, z_u^v), clock bias τ_u, and frequency offset f_u

$$\boldsymbol{s} = \begin{bmatrix} x_u & x_u^v & y_u & y_u^v & z_u & z_u^v & \tau_u & f_u \end{bmatrix}^{\mathrm{T}} \tag{3}$$

The measured pseudo-code phase C_n can be expressed as the sum of the pseudo-code phase of the nth locally generated signal C_n^l and the estimated pseudo-code phase difference $\Delta\hat{C}_n$. According to (1) and (2), it also equals to the pseudo-code phase of the nth received signal C_n^r plus the estimation error εC_n

$$C_n = C_n^l + \Delta\hat{C}_n = C_n^r + \varepsilon C_n \tag{4}$$

Besides, it is similar for the measured carrier Doppler shift f_n

$$f_n = f_n^l + \Delta\hat{f}_n = f_n^r + \varepsilon f_n \tag{5}$$

We define the pseudo-code phase correction C_n^{c} by subtracting the measured pseudo-code phase C_n from the pseudo-code phase estimated from the updated receiver state $\tilde{\boldsymbol{s}}$. The carrier Doppler shift correction f_n^{c} is similar. As shown in (6), $\boldsymbol{h}(\cdot)$ represents the relationship between the receiver state and the pseudo-code phases and carrier Doppler shifts

$$\begin{aligned} &\begin{bmatrix} C_1^{\mathrm{c}} & \cdots & C_N^{\mathrm{c}} & f_1^{\mathrm{c}} & \cdots & f_N^{\mathrm{c}} \end{bmatrix}^{\mathrm{T}} \\ &= \boldsymbol{h}(\tilde{\boldsymbol{s}}) - \begin{bmatrix} C_1 & \cdots & C_N & f_1 & \cdots & f_N \end{bmatrix}^{\mathrm{T}} \end{aligned} \tag{6}$$

Different from the traditional scalar tracking structure that the estimated pseudo-code phase difference $\Delta\hat{C}_n$ and estimated carrier phase difference $\Delta\hat{\varphi}_n$ are directly used as the input of delay lock loop (DLL) and phase lock loop (PLL), respectively, which eventually entering the tracking loops of the vector tracking structure are the combinations of the estimation results ($\Delta\hat{C}_n$ and $\Delta\hat{\varphi}_n$) and the corrections (C_n^{c} and f_n^{c})

$$\begin{cases} C_{\mathrm{DLL},n} = \Delta\hat{C}_n + C_n^{\mathrm{c}} \\ \varphi_{\mathrm{PLL},n} = \Delta\hat{\varphi}_n + \pi T \cdot f_n^{\mathrm{c}} \end{cases} \tag{7}$$

where $C_{\mathrm{DLL},n}$ denotes the input of DLL, $\varphi_{\mathrm{PLL},n}$ denotes the input of PLL, T is the coherent integration time that is set to 1 ms in subsequent simulations.

Since the pseudo-code phase correction C_n^{c} and carrier Doppler shift correction f_n^{c} are in connection with the receiver state, for the vector tracking structure, all tracking loops connected by the receiver state are no longer independent. Therefore, it does not take much imagination to understand that spoofing attacks, which influence the receiver state, will also influence vector tracking loops. The influence of spoofing attacks on vector tracking loops will be discussed in the next part.

2.2 Influence of spoofing attacks on vector tracking loops

Assume that the spoofing pseudo-code phase and spoofing carrier Doppler shift of the nth received signal are C_n^{s} and f_n^{s}, respectively. Both C_n^{s} and f_n^{s} are equal to zero meaning the nth received signal is authentic. Otherwise, it is counterfeited. Then, according to (6), and combining (4) and (5), the pseudo-code phase correction C_n^{c} and carrier Doppler shift correction f_n^{c} under spoofing attacks could be deduced as

$$\begin{aligned} &\begin{bmatrix} C_1^{\mathrm{c}} & \cdots & C_N^{\mathrm{c}} & f_1^{\mathrm{c}} & \cdots & f_N^{\mathrm{c}} \end{bmatrix}^{\mathrm{T}} \\ &\simeq \left(\boldsymbol{H}\left(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\mathrm{T}} - \boldsymbol{I}\right) \\ &\quad \times \begin{bmatrix} C_1^{\mathrm{s}} + \varepsilon C_1 & \cdots & C_N^{\mathrm{s}} + \varepsilon C_N & f_1^{\mathrm{s}} + \varepsilon f_1 & \cdots & f_N^{\mathrm{s}} + \varepsilon f_N \end{bmatrix}^{\mathrm{T}} \end{aligned} \tag{8}$$

where $\boldsymbol{H}$ represents the measurement matrix that is the derivative of the function $\boldsymbol{h}(\cdot)$ on the actual receiver state $\bar{\boldsymbol{s}}$

$$\boldsymbol{H} = \frac{\partial \boldsymbol{h}(\boldsymbol{s})}{\partial \boldsymbol{s}}\bigg|\boldsymbol{s} = \bar{\boldsymbol{s}} \tag{9}$$

The measurement matrix $\boldsymbol{H}$ is determined by the satellite geometry distribution.

Considering that the effect of C_n^{s} on $(f_1^{\mathrm{c}}, \ldots, f_N^{\mathrm{c}})$ and the effect of f_n^{s} on $(C_1^{\mathrm{c}}, \ldots, C_N^{\mathrm{c}})$ are usually small and negligible, (8) could be replaced by (10)

$$\begin{aligned} &\begin{bmatrix} C_1^{\mathrm{c}} \\ \vdots \\ C_N^{\mathrm{c}} \end{bmatrix} \simeq \left(\boldsymbol{G}_1\left(\boldsymbol{G}_1^{\mathrm{T}}\boldsymbol{G}_1\right)^{-1}\boldsymbol{G}_1^{\mathrm{T}} - \boldsymbol{I}\right)\begin{bmatrix} C_1^{\mathrm{s}} + \varepsilon C_1 \\ \vdots \\ C_N^{\mathrm{s}} + \varepsilon C_N \end{bmatrix} \\ &\begin{bmatrix} f_1^{\mathrm{c}} \\ \vdots \\ f_N^{\mathrm{c}} \end{bmatrix} \simeq \left(\boldsymbol{G}_2\left(\boldsymbol{G}_2^{\mathrm{T}}\boldsymbol{G}_2\right)^{-1}\boldsymbol{G}_2^{\mathrm{T}} - \boldsymbol{I}\right)\begin{bmatrix} f_1^{\mathrm{s}} + \varepsilon f_1 \\ \vdots \\ f_N^{\mathrm{s}} + \varepsilon f_N \end{bmatrix} \\ &\boldsymbol{G}_1 = \boldsymbol{H}([\quad 1 \quad \cdots \quad N], \quad [1 \quad 3 \quad 5 \quad 7]) \\ &\boldsymbol{G}_2 = \boldsymbol{H}([N+1 \quad \cdots \quad 2N], \quad [2 \quad 4 \quad 6 \quad 8]) \end{aligned} \tag{10}$$

where the matrix $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$ are both composed of the elements in the measurement matrix $\boldsymbol{H}$.

As shown in (10), when there is no spoofing signal, both $(C_1^{\mathrm{s}}, \ldots, C_N^{\mathrm{s}})$ and $(f_1^{\mathrm{s}}, \ldots, f_N^{\mathrm{s}})$ are equal to zero. The estimation errors $(\varepsilon C_1, \ldots, \varepsilon C_N)$ and $(\varepsilon f_1, \ldots, \varepsilon f_N)$ are usually zero mean in this case. Then, the corrections $(C_1^{\mathrm{c}}, \ldots, C_N^{\mathrm{c}})$ and $(f_1^{\mathrm{c}}, \ldots, f_N^{\mathrm{c}})$ are approximately zero mean. While when there are spoofing attacks, it is not difficult to deduce that these corrections are likely to deviate from zero. Essentially this is due to the consistency among received signals being destroyed by spoofing attacks. It should be pointed out that although there are special spoofing attacks that can maintain the consistency among received signals and do not cause the corrections to deviate from zero, the formula (10) is also tenable. Hence, the subsequent analysis will not separate the special spoofing attacks.

For the vector tracking structure under spoofing attacks, the non-zero mean pseudo-code phase correction C_n^{c} and carrier Doppler shift correction f_n^{c} entering tracking loops will affect the code NCO (numerically controlled oscillator) and the carrier NCO. The effects on the NCOs will ultimately affect the pseudo-code phase C_n^l, carrier Doppler shift f_n^l, and carrier phase φ_n^l of the nth locally generated signal. When the vector tracking structure is stable, the inputs of tracking loops should be approximately zero mean. Then, (11) could be deduced according to (7)

$$\begin{cases} \mathrm{E}\left(\Delta\hat{C}_n\right) \simeq -\mathrm{E}(C_n^{\mathrm{c}}) \\ \mathrm{E}(\Delta\hat{\varphi}_n) \simeq -\pi T \cdot \mathrm{E}(f_n^{\mathrm{c}}) \end{cases} \tag{11}$$

Combining (11) with (10), we can conclude that the estimated pseudo-code phase difference $\Delta\hat{C}_n$ and estimated carrier phase difference $\Delta\hat{\varphi}_n$ are likely to be non-zero mean when there are spoofing attacks. It means that the pseudo-code phase difference ΔC_n and carrier phase difference $\Delta\varphi_n$ are also non-zero mean. In addition, the carrier Doppler shift difference Δf_n should be zero mean to maintain $\Delta\varphi_n$ stable.

The above analysis is for the spoofing scenarios without overlapping correlation peaks. To sum up, for the vector tracking structure in such a spoofing scenario, the pseudo-code phases and carrier phases of locally generated signals are inconsistent with received signals, but the carrier Doppler shifts are consistent. Considering that all these parameters of locally generated signals are consistent with received signals for the scalar tracking structure in the same case, the feature is brought by the vector tracking structure.

Assume that the correlator spacing is one chip, the coherent integration results $I_{\mathrm{E},n}$, $Q_{\mathrm{E},n}$, $I_{\mathrm{P},n}$, $Q_{\mathrm{P},n}$, $I_{\mathrm{L},n}$, and $Q_{\mathrm{L},n}$ can be expressed as (12), where f_{s} is the sampling frequency, A_n is the signal amplitude, $n_{I_{\mathrm{E},n}}$, $n_{Q_{\mathrm{E},n}}$, $n_{I_{\mathrm{P},n}}$, $n_{Q_{\mathrm{P},n}}$, $n_{I_{\mathrm{L},n}}$, and $n_{Q_{\mathrm{E},n}}$ are the errors due to the noise in received signals. In general, we regard it as Gaussian white noise and assume its variance is σ^2 to simplify analysis. Then, these errors are subject to the same Gaussian distribution of zero mean, as shown in (13)

$$\begin{cases} I_{\mathrm{E},n} = \dfrac{f_{\mathrm{s}}T}{2}A_n(0.5 + \Delta C_n)\cos(\Delta\varphi_n) + n_{I_{\mathrm{E},n}} \\ Q_{\mathrm{E},n} = \dfrac{f_{\mathrm{s}}T}{2}A_n(0.5 + \Delta C_n)\sin(\Delta\varphi_n) + n_{Q_{\mathrm{E},n}} \\ I_{\mathrm{P},n} = \dfrac{f_{\mathrm{s}}T}{2}A_n(1 - |\Delta C_n|)\cos(\Delta\varphi_n) + n_{I_{\mathrm{P},n}} \\ Q_{\mathrm{P},n} = \dfrac{f_{\mathrm{s}}T}{2}A_n(1 - |\Delta C_n|)\sin(\Delta\varphi_n) + n_{Q_{\mathrm{P},n}} \\ I_{\mathrm{L},n} = \dfrac{f_{\mathrm{s}}T}{2}A_n(0.5 - \Delta C_n)\cos(\Delta\varphi_n) + n_{I_{\mathrm{L},n}} \\ Q_{\mathrm{L},n} = \dfrac{f_{\mathrm{s}}T}{2}A_n(0.5 - \Delta C_n)\sin(\Delta\varphi_n) + n_{Q_{\mathrm{L},n}} \end{cases} \tag{12}$$

$$n_{I_{E,n}}, n_{Q_{E,n}}, n_{I_{P,n}}, n_{Q_{P,n}}, n_{I_{L,n}}, n_{Q_{L,n}} \sim N\left(0, \quad \frac{f_s T}{2}\sigma^2\right) \tag{13}$$

In summary, spoofing attacks are likely to destroy the consistency among received signals, which causes the pseudo-code phase corrections $(C_1^{\mathrm{c}}, \ldots, C_N^{\mathrm{c}})$ and carrier Doppler shift corrections $(f_1^{\mathrm{c}}, \ldots, f_N^{\mathrm{c}})$ to deviate from zero. For the vector tracking structure, these corrections enter tracking loops, ultimately resulting in the pseudo-code phase differences $(\Delta C_1, \ldots, \Delta C_N)$ and carrier phase differences $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$ between received signals and locally generated signals that are non-zero mean. From (12), it is evident that ΔC_n and $\Delta\varphi_n$ influence the coherent integration results. In short, spoofing attacks can influence the coherent integration

results of the vector tracking structure through affecting ΔC_n and $\Delta\varphi_n$. This influence does not require the overlapping correlation peaks. Therefore, for the vector tracking structure, not only the overlap of the correlation peaks but also the inconsistency among received signals due to spoofing attacks will affect the coherent integration results. It means that SQM techniques could be used for the vector tracking structure to detect spoofing attacks regardless of whether the correlation peaks overlap. It is the most significant difference between the application of SQM techniques to the scalar tracking structure and the vector tracking structure.

2.3 Analysis of pseudo-code phase difference and carrier phase difference

In this section, we will further analyse the pseudo-code phase difference ΔC_n and carrier phase difference $\Delta\varphi_n$ of the vector tracking structure under spoofing attacks. It is indispensable for studying the performance of the proposed SQM-based spoofing detection method in the next section.

The selected estimation methods for ΔC_n and $\Delta\varphi_n$ in this paper are shown in (14) [23]

$$\begin{cases} \Delta\hat{C}_n = \dfrac{1}{2}\dfrac{\sqrt{I_{\mathrm{E},n}^2+Q_{\mathrm{E},n}^2}-\sqrt{I_{\mathrm{L},n}^2+Q_{\mathrm{L},n}^2}}{\sqrt{I_{\mathrm{E},n}^2+Q_{\mathrm{E},n}^2}+\sqrt{I_{\mathrm{L},n}^2+Q_{\mathrm{L},n}^2}} \\ \Delta\hat{\varphi}_n = \tan^{-1}\left(\dfrac{Q_{\mathrm{P},n}}{I_{\mathrm{P},n}}\right) \end{cases} \tag{14}$$

According to the tracking threshold of DLL and PLL [23], when the pseudo-code phase difference ΔC_n exceeds $[-0.5, 0.5]$ chip, or the carrier phase difference $\Delta\varphi_n$ exceeds $[-0.25\pi, 0.25\pi]$ radian, tracking loops will be unable to lock the nth received signal. In this case, the loss of lock provides the information about the existence of spoofing attacks. It means that we can be aware of spoofing attacks without additional spoofing detection methods. Hence the proposed SQM-based spoofing detection method only considers the pseudo-code phase difference and carrier phase difference within the ranges.

Here, we use $w_{n,1}$ and $w_{n,2}$ to represent $\sqrt{I_{\mathrm{L},n}^2+Q_{\mathrm{L},n}^2}/\sqrt{I_{\mathrm{E},n}^2+Q_{\mathrm{E},n}^2}$ and $Q_{\mathrm{P},n}/I_{\mathrm{P},n}$, respectively. For the nth received signal, the carrier-to-noise ratio can be expressed as

$$(C/N_0)_n = (A_n)^2 f_s/4\sigma^2 \tag{15}$$

Then, the probability density functions of $w_{n,1}$ and $w_{n,2}$ could be deduced as (16) and (17) [24]

$$\begin{aligned} p_{n,1}(w_{n,1}) = {} & \frac{2w_{n,1}}{\left(w_{n,1}^2+1\right)^2}\times\exp\left(-\frac{a_{n,11}^2w_{n,1}^2+a_{n,12}^2}{2\left(w_{n,1}^2+1\right)}\right) \\ & \times\left(\left(1+\frac{a_{n,11}^2+a_{n,12}^2w_{n,1}^2}{2\left(w_{n,1}^2+1\right)}\right)\times I_0\left(\frac{a_{n,11}a_{n,12}w_{n,1}}{w_{n,1}^2+1}\right)\right. \\ & \left.+\left(\frac{a_{n,11}a_{n,12}w_{n,1}}{w_{n,1}^2+1}\right)\times I_1\left(\frac{a_{n,11}a_{n,12}w_{n,1}}{w_{n,1}^2+1}\right)\right) \\ & \begin{cases} a_{n,11} = \sqrt{2T(C/N_0)_n}(0.5+\Delta C_n) \\ a_{n,12} = \sqrt{2T(C/N_0)_n}(0.5-\Delta C_n) \end{cases} \end{aligned} \tag{16}$$

$$\begin{aligned} p_{n,2}(w_{n,2}) = {} & \frac{1}{\pi\left(w_{n,2}^2+1\right)}\times\exp\left(-\frac{a_{n,21}^2+a_{n,22}^2}{2}\right) \\ & +\frac{a_{n,21}+a_{n,22}w_{n,2}}{\sqrt{2\pi}\left(w_{n,2}^2+1\right)^{3/2}}\times\exp\left(-\frac{\left(a_{n,22}-a_{n,21}w_{n,2}\right)^2}{2\left(w_{n,2}^2+1\right)}\right) \\ & \times\left(1-Q\left(\frac{a_{n,21}+a_{n,22}w_{n,2}}{\sqrt{w_{n,2}^2+1}}\right)\right) \\ & \begin{cases} a_{n,21} = \sqrt{2T(C/N_0)_n}(1-|\Delta C_n|)\cos(\Delta\varphi_n) \\ a_{n,22} = \sqrt{2T(C/N_0)_n}(1-|\Delta C_n|)\sin(\Delta\varphi_n) \end{cases} \end{aligned} \tag{17}$$

According to (14), (16), and (17), we can calculate the mean of $\Delta\hat{C}_n$ and $\Delta\hat{\varphi}_n$

$$\begin{cases} \mathrm{E}\left(\Delta\hat{C}_n\right) = \int\left(\dfrac{1}{2}\dfrac{1-w_{n,1}}{1+w_{n,1}}p_{n,1}(w_{n,1})\right)\mathrm{d}w_{n,1} \\ = \gamma_1(\Delta C_n, (C/N_0)_n) \\ \mathrm{E}\left(\Delta\hat{\varphi}_n\right) = \int\left(\tan^{-1}(w_{n,2})p_{n,2}(w_{n,2})\right)\mathrm{d}w_{n,2} \\ = \gamma_2(\Delta C_n, \Delta\varphi_n, (C/N_0)_n) \end{cases} \tag{18}$$

Here we use $\gamma_1(\cdot)$ and $\gamma_2(\cdot)$ to denote the relationships.

Combining (10), (11), and (18), and considering that the mean of εC_n and εf_n in (10) satisfies (19)

$$\begin{cases} \mathrm{E}(\varepsilon C_n) = \mathrm{E}\left(\Delta\hat{C}_n\right) - \Delta C_n \\ \mathrm{E}(\varepsilon f_n) = 0 \end{cases} \tag{19}$$

we can associate the spoofing pseudo-code phases $(C_1^{\mathrm{s}}, \ldots, C_N^{\mathrm{s}})$, the spoofing carrier Doppler shifts $(f_1^{\mathrm{s}}, \ldots, f_N^{\mathrm{s}})$, the pseudo-code phase differences $(\Delta C_1, \ldots, \Delta C_N)$, and the carrier phase differences $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$. The relationships of them can be deduced as follows:

$$\begin{aligned} & \begin{bmatrix} \Delta C_1 \\ \cdots \\ \Delta C_N \end{bmatrix} + \boldsymbol{G}_1\left(\boldsymbol{G}_1^{\mathrm{T}}\boldsymbol{G}_1\right)^{-1}\boldsymbol{G}_1^{\mathrm{T}}\begin{bmatrix} \gamma_1(\Delta C_1, (C/N_0)_1) - \Delta C_1 \\ \cdots \\ \gamma_1(\Delta C_N, (C/N_0)_N) - \Delta C_N \end{bmatrix} \\ & \simeq \left(\boldsymbol{I} - \boldsymbol{G}_1\left(\boldsymbol{G}_1^{\mathrm{T}}\boldsymbol{G}_1\right)^{-1}\boldsymbol{G}_1^{\mathrm{T}}\right)\begin{bmatrix} C_1^s \\ \cdots \\ C_N^s \end{bmatrix} \end{aligned} \tag{20}$$

$$\begin{aligned} & \begin{bmatrix} \gamma_2(\Delta C_1, \Delta\varphi_1, (C/N_0)_1) \\ \vdots \\ \gamma_2(\Delta C_N, \Delta\varphi_N, (C/N_0)_N) \end{bmatrix} \\ & \simeq \pi T\cdot\left(\boldsymbol{I} - \boldsymbol{G}_2\left(\boldsymbol{G}_2^{\mathrm{T}}\boldsymbol{G}_2\right)^{-1}\boldsymbol{G}_2^{\mathrm{T}}\right)\begin{bmatrix} f_1^{\mathrm{s}} \\ \vdots \\ f_N^{\mathrm{s}} \end{bmatrix} \end{aligned} \tag{21}$$

From (20) and (21), it is not difficult to find that the spoofing pseudo-code phases $(C_1^{\mathrm{s}}, \ldots, C_N^{\mathrm{s}})$ can affect the pseudo-code phase differences $(\Delta C_1, \ldots, \Delta C_N)$ and the spoofing carrier Doppler shifts $(f_1^{\mathrm{s}}, \ldots, f_N^{\mathrm{s}})$ can affect the carrier phase differences $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$. When there is no spoofing attack that both $(C_1^{\mathrm{s}}, \ldots, C_N^{\mathrm{s}})$ and $(f_1^{\mathrm{s}}, \ldots, f_N^{\mathrm{s}})$ are zeros, $(\Delta C_1, \ldots, \Delta C_N)$ and $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$ are approximately equal to zero. In contrast, when there are spoofing attacks, $(\Delta C_1, \ldots, \Delta C_N)$ and $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$ may deviate from zero. Combining (20) and (21), the spoofing pseudo-code phases $(C_1^{\mathrm{s}}, \ldots, C_N^{\mathrm{s}})$ can also affect the carrier phase differences $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$ through affecting the pseudo-code phase differences $(\Delta C_1, \ldots, \Delta C_N)$. Nevertheless, the effect is relatively small and negligible. Besides, the carrier-to-noise ratios and the satellite geometry distribution that determines the measurement matrix $\boldsymbol{H}$ are the main influential factors. Here, we demonstrate the relationships in (20) and (21) through a numerical simulation. Considering the case of only one spoofing signal that the signal with pseudo-random noise (PRN) 2 is spoofed, we set the spoofing pseudo-code phase is 0.5 chip and the spoofing carrier Doppler shift is 250 Hz, and assume that all received signals have the same carrier-to-noise ratio. The satellite geometry distribution and the simulation results are depicted in Figs. 2–4.

From Figs. 3 and 4, it is evident that the spoofing pseudo-code phase and spoofing carrier Doppler shift of one signal have effects on the pseudo-code phase differences and carrier phase differences of all signals. The degree of influence on each signal is different,

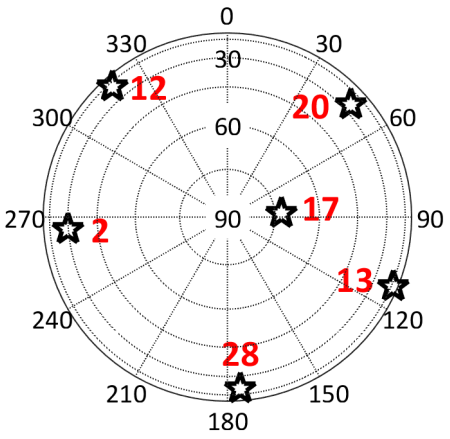

Fig. 2 *Satellite geometry distribution*

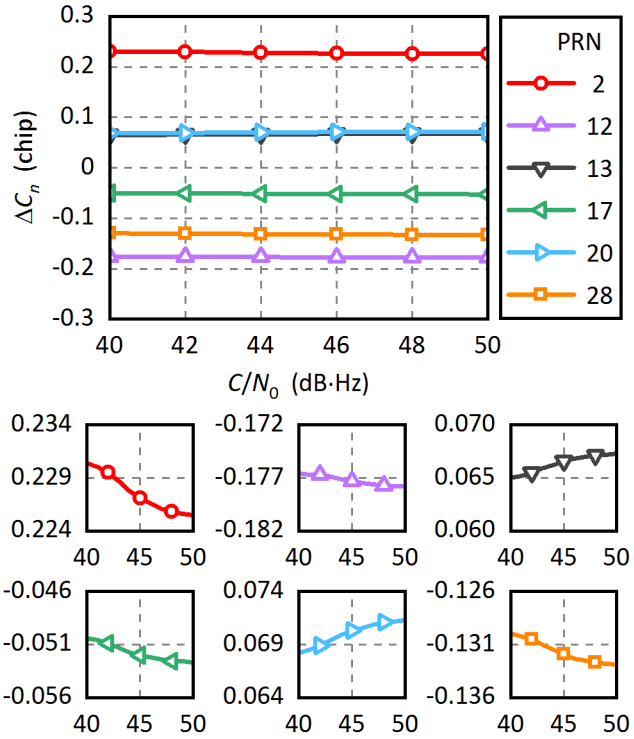

Fig. 3 *Pseudo-code phase differences under various carrier-to-noise ratios*

which is relevant to the satellite geometry distribution that determines the measurement matrix $\boldsymbol{H}$. Additionally, the carrier-to-noise ratio is also an influential factor though its effect is not significant. Generally, lower the carrier-to-noise ratio, larger the absolute value of the carrier phase difference. Although the pseudo-code phase difference is also affected by the carrier-to-noise ratio, it does not match this relationship. The otherness is because the mean of the estimated pseudo-code phase difference error εC_n is non-zero, while the mean of the estimated carrier Doppler shift difference error εf_n is zero, which has been shown in (19).

3 Signal quality monitoring-based spoofing detection method for vector tracking structure

In the previous section, we have analysed the influence of spoofing attacks on vector tracking loops and derived the pseudo-code phase differences $(\Delta C_1, \ldots, \Delta C_N)$ and carrier phase differences $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$ under spoofing attacks. Spoofing attacks are likely to destroy the consistency among received signals. For the vector tracking structure, the inconsistency of received signals can cause the pseudo-code phases and carrier phases of locally generated signals to be inconsistent with received signals. This could affect

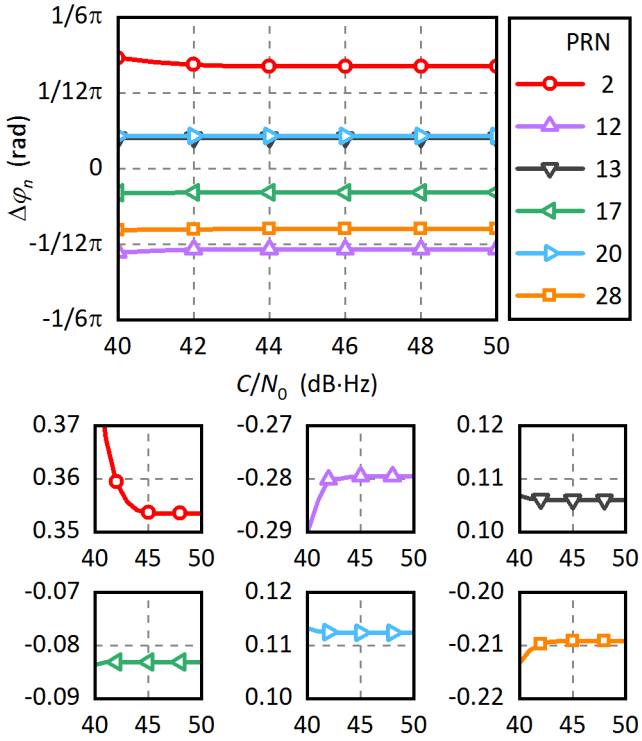

Fig. 4 *Carrier phase differences under various carrier-to-noise ratios*

the coherent integration results. In this section, we first present the influence of spoofing attacks on the coherent integration results through a simulation. Then, an SQM-based spoofing detection method for the vector tracking structure is introduced and analysed.

3.1 Influence of spoofing attacks on coherent integration results

The simulation results are presented in Fig. 5. As depicted in Fig. 5, the upper two panels are the coherent integration results without spoofing attack, and the lower two panels are the ones under spoofing attacks. The correlation peaks do not overlap in this simulation. The receiver adopts the scalar tracking structure in the first 0.2 s and then switches to the vector tracking structure. For the scalar tracking structure, the coherent integration results in the non-spoofing attack environment and the spoofing attack environment have no noticeable difference. While for the vector tracking structure, the coherent integration results in the two environments are significantly different.

Combining the simulation results and formula (14), it is not hard to speculate that for the vector tracking structure, both the estimated pseudo-code phase difference $\Delta\hat{C}_n$ and the estimated carrier phase difference $\Delta\hat{\varphi}_n$ could be used for detecting spoofing attacks. According to the analysis in the previous section, the spoofing attacks on the pseudo-code and the carrier Doppler could be detected by thresholding $\Delta\hat{C}_n$ and $\Delta\hat{\varphi}_n$, respectively. The proposed SQM-based spoofing detection method is in line with this idea.

3.2 Method introduction

For the spoofing scenarios with overlapping correlation peaks, the current SQM methods [6–12] for the scalar tracking structure could still be used for the vector tracking structure. According to the analysis in Section 2.2, for the vector tracking structure in the spoofing scenarios where the correlation peaks do not overlap, the pseudo-code phases and carrier phases of locally generated signals are inconsistent with received signals, but the carrier Doppler shifts are consistent. Therefore, in this case, most of the pseudo-code SQM methods are still useful. However, the carrier Doppler SQM method [12] that uses the difference between the slower and faster Doppler shift correlator outputs as a metric is invalid.

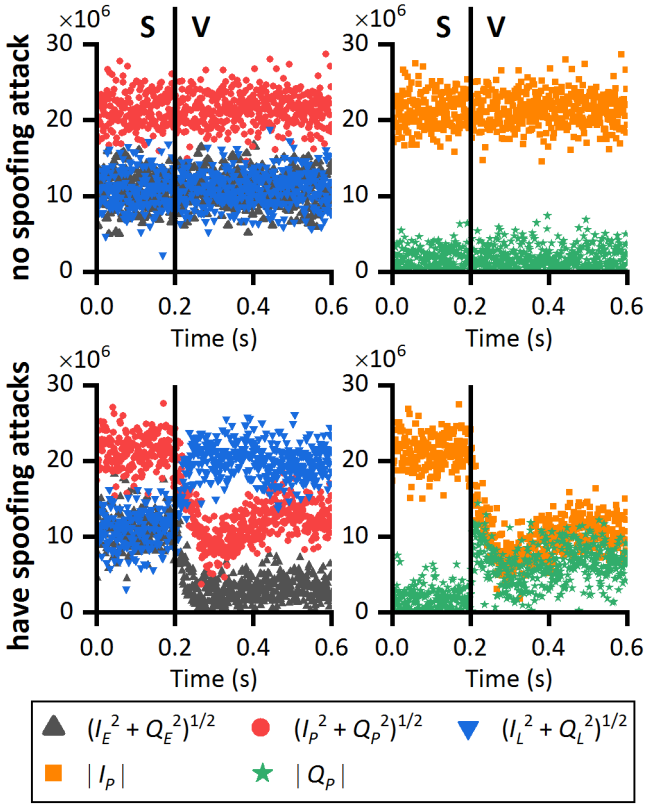

Fig. 5 *Coherent integration results of the scalar tracking structure and vector tracking structure in two environments*

To sum up, for the vector tracking structure, the current SQM methods can detect spoofing attacks on pseudo-code, but cannot detect spoofing attacks on carrier Doppler for the spoofing scenarios where the correlation peaks do not overlap. To this end, we propose a new SQM-based spoofing detection method. The proposed method can detect spoofing attacks on both pseudo-code and carrier Doppler through the pseudo-code phase differences and carrier phase differences estimated by the coherent integration results. It is more suitable for the vector tracking structure because the receiver hardware architecture does not need to be modified for spoofing detection. The specific process of the proposed method will be introduced next.

The numerical simulation in the Section 2 has shown that even if there is only one spoofing signal, the pseudo-code phase differences $(\Delta C_1, \ldots, \Delta C_N)$ and carrier phase differences $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$ for all signals deviate from zero. And these values are various because the influence extent of spoofing attacks on each signal is different. The most intuitive method is to directly detect all pseudo-code phase differences and carrier phase differences estimated by the coherent integration results. Nevertheless, this method is computationally intensive.

To simplify computation, the proposed SQM-based spoofing detection method includes two steps. The first is to find out the signal with the largest parameter ξ_n defined as (22). Here, $\Delta\hat{C}_n^{(K)}$ and $\Delta\hat{\varphi}_n^{(K)}$ are the Kth estimations of ΔC_n and $\Delta\varphi_n$, respectively. Their definitions are shown in (23). K is the number of the consecutive coherent integration times. β_C and β_φ represent the weight of ΔC_n and $\Delta\varphi_n$. For the estimation methods of ΔC_n and $\Delta\varphi_n$ in this paper, their pull-in ranges are $[-0.5, 0.5]$ chip and $[-0.25\pi, 0.25\pi]$ radian [23]. Hence, we could set β_C and β_φ to 0.5 chip and 0.25π radian, respectively. When selecting other estimation methods, β_C and β_φ could also be adjusted according to the corresponding pull-in ranges

$$\xi_n = \frac{1}{2}\left(\left|\frac{\Delta\hat{C}_n^{(K)}}{\beta_C}\right| + \left|\frac{\Delta\hat{\varphi}_n^{(K)}}{\beta_\varphi}\right|\right) \tag{22}$$

$$\begin{aligned}
&\Delta\hat{C}_n^{(K)} = \frac{1}{2}\frac{\sqrt{\left(I_{\mathrm{E},n}^{(K)}\right)^2 + \left(Q_{\mathrm{E},n}^{(K)}\right)^2} - \sqrt{\left(I_{\mathrm{L},n}^{(K)}\right)^2 + \left(Q_{\mathrm{L},n}^{(K)}\right)^2}}{\sqrt{\left(I_{\mathrm{E},n}^{(K)}\right)^2 + \left(Q_{\mathrm{E},n}^{(K)}\right)^2} + \sqrt{\left(I_{\mathrm{L},n}^{(K)}\right)^2 + \left(Q_{\mathrm{L},n}^{(K)}\right)^2}} \\
&\Delta\hat{\varphi}_n^{(K)} = \tan^{-1}\left(\frac{Q_{\mathrm{P},n}^{(K)}}{I_{\mathrm{P},n}^{(K)}}\right) \\
&\begin{cases}
I_{(\mathrm{E,P,L}),n}^{(K)} = \dfrac{1}{K}\displaystyle\sum_{k=1}^{K} I_{(\mathrm{E,P,L}),n,k} \times \mathrm{sign}(I_{\mathrm{P},n,k}) \\
Q_{(\mathrm{E,P,L}),n}^{(K)} = \dfrac{1}{K}\displaystyle\sum_{k=1}^{K} Q_{(\mathrm{E,P,L}),n,k} \times \mathrm{sign}(I_{\mathrm{P},n,k})
\end{cases}
\end{aligned} \tag{23}$$

After the parameters $(\xi_1, \ldots, \xi_N)$ corresponding to all signals are calculated and the largest one ξ_m is found, the second step is to perform a binary hypothesis test on the mth signal to detect whether the spoofing attacks exist. The SQM metric $[\eta_1 \quad \eta_2]^{\mathrm{T}}$ is defined as (24). Combining the previous analysis, it can be seen that η_1 is mainly affected by spoofing attacks on pseudo-code and η_2 is mainly affected by spoofing attacks on carrier Doppler

$$\begin{cases}
\eta_1 = \left|\Delta\hat{C}_m^{(K)}\right| \\
\eta_2 = \left|\Delta\hat{\varphi}_m^{(K)}\right|
\end{cases} \tag{24}$$

Considering the effect of noise, the binary hypothesis test could be expressed as

$$\begin{cases}
H_0\text{: } \eta_1 \le T_1 \text{ and } \eta_2 \le T_2 \\
H_1\text{: } \eta_1 > T_1 \text{ or } \eta_2 > T_2
\end{cases} \tag{25}$$

H_0 indicates the hypothesis that both the pseudo-code phase difference ΔC_m and the carrier phase difference $\Delta\varphi_m$ are approximately equal to zero. H_1 indicates that at least one of ΔC_m and $\Delta\varphi_m$ is deviated from zero. T_1 and T_2 are the pseudo-code phase difference threshold and carrier phase difference threshold, respectively. When the test result is H_0, we believe that there is no spoofing signal in received signals. Conversely, a test result of H_1 means the existence of the spoofing attacks on pseudo-code or carrier Doppler.

The above is the whole process of the proposed SQM-based method for spoofing detection. In practical applications, we can appropriately reduce the frequency of the first step. It would not affect our detection results very much and can cut down the amount of computation.

Here we explain the reason that the binary hypothesis test is performed on the mth signal. When all received signals are authentic, the pseudo-code phase differences $(\Delta C_1, \ldots, \Delta C_N)$ and carrier phase differences $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$ are approximately equal to zero, as are their estimations $\left(\Delta\hat{C}_1^{(K)}, \ldots, \Delta\hat{C}_N^{(K)}\right)$ and $\left(\Delta\hat{\varphi}_1^{(K)}, \ldots, \Delta\hat{\varphi}_N^{(K)}\right)$. Under this circumstance, no matter which signal is selected, even for the mth signal with the largest parameter ξ_m, the SQM metrics η_1 and η_2 are close to zero. While when there are spoofing attacks, $\left(\Delta\hat{C}_1^{(K)}, \ldots, \Delta\hat{C}_N^{(K)}\right)$ and $\left(\Delta\hat{\varphi}_1^{(K)}, \ldots, \Delta\hat{\varphi}_N^{(K)}\right)$ may deviate from zero. These parameters $(\xi_1, \ldots, \xi_N)$ are usually different and greater than zero. The size of the parameter can roughly reflect the degree to which the signal is affected by spoofing attacks. Generally speaking, the probability of detecting spoofing attacks will be higher when the binary hypothesis test is performed on the signal that is more affected by spoofing attacks. In conclusion, it is reasonable to detect whether there are spoofing attacks based on the mth signal.

On the other hand, these parameters are affected by noise. According to (12)–(14) and (23), we can derive that the variance of $I_{\mathrm{E},n}^{(K)}$, $Q_{\mathrm{E},n}^{(K)}$, $I_{\mathrm{P},n}^{(K)}$, $Q_{\mathrm{P},n}^{(K)}$, $I_{\mathrm{L},n}^{(K)}$, and $Q_{\mathrm{L},n}^{(K)}$ is $f_s T\sigma^2/2K$. In general, larger the value of K smaller the variance, which means that the influence of noise on the parameters is smaller. Here we perform a

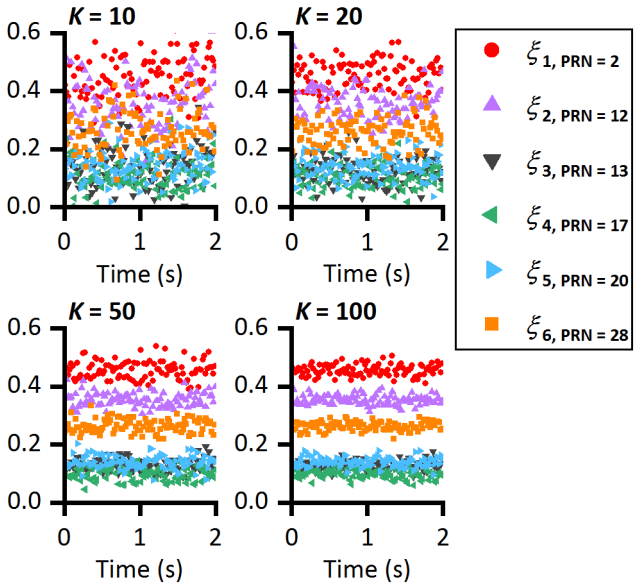

Fig. 6 *Parameters corresponding to all signals with different K*

simulation on the signals that the satellite geometry distribution is shown in Fig. 2. We assume that only the signal with PRN 2 is spoofed. Its spoofing pseudo-code phase is 0.5 chip and spoofing carrier Doppler shift is 250 Hz. And the carrier-to-noise ratio of all signals is 40 dB·Hz. Then, the parameters $(\xi_1, \ldots, \xi_N)$ corresponding to all signals with different K are shown in Fig. 6. Obviously, when K is larger, these parameters are more stable. It means that we can find the mth signal accurately by increasing K to a certain extent.

The simulation results show that the signal with PRN 2 is the signal with the largest parameter. Nevertheless, it should be emphasised that the mth signal is not necessarily a spoofing signal. The proposed SQM-based method can detect spoofing attacks but cannot distinguish between spoofing signals and authentic signals. We will explain this again in Section 4.

3.3 Probability analysis

The probability analysis is mainly for the binary hypothesis test on the mth signal. The pseudo-code phase difference and carrier phase difference between the mth received signal and locally generated signal are ΔC_m and $\Delta\varphi_m$, respectively. Then, the probability P_0 of the hypothesis H_0 and the probability P_1 of the hypothesis H_1 could be deduced as (26)

$$\begin{cases} P_0 = \left(\int_{\kappa_{11}}^{\kappa_{12}} p_{m,1}^{(K)}\left(w_{m,1}^{(K)}\right)\mathrm{d}w_{m,1}^{(K)}\right) \times \left(\int_{\kappa_{21}}^{\kappa_{22}} p_{m,2}^{(K)}\left(w_{m,2}^{(K)}\right)\mathrm{d}w_{m,2}^{(K)}\right) \\ P_1 = 1 - P_0 \end{cases} \tag{26}$$

where κ_{11}, κ_{12}, κ_{21}, and κ_{22} are related to the pseudo-code phase difference threshold T_1 and the carrier phase difference threshold T_2

$$\begin{cases} \kappa_{11} = \dfrac{1-2T_1}{1+2T_1}, \quad \kappa_{12} = \dfrac{1+2T_1}{1-2T_1} \\ \kappa_{21} = -\tan(T_2), \quad \kappa_{22} = \tan(T_2) \end{cases} \tag{27}$$

$w_{m,1}^{(K)}$ represents $\sqrt{\left(I_{\mathrm{L},m}^{(K)}\right)^2 + \left(Q_{\mathrm{L},m}^{(K)}\right)^2}/\sqrt{\left(I_{\mathrm{E},m}^{(K)}\right)^2 + \left(Q_{\mathrm{E},m}^{(K)}\right)^2}$, and $w_{m,2}^{(K)}$ represents $Q_{\mathrm{P},m}^{(K)}/I_{\mathrm{P},m}^{(K)}$. Similar to (16) and (17), we can also obtain $p_{m,1}^{(K)}\left(w_{m,1}^{(K)}\right)$ and $p_{m,2}^{(K)}\left(w_{m,2}^{(K)}\right)$ that are the probability density functions of $w_{m,1}^{(K)}$ and $w_{m,2}^{(K)}$ [24]. The probability density functions are shown in (28) and (29)

(see (28))

(see (29))

The false alarm rate P_{fa} is the probability that the hypothesis H_1 is accepted, but in reality, both ΔC_m and $\Delta\varphi_m$ are equal to zero. Combined with the previous analysis about the probability P_1 of the hypothesis H_1, it could be expressed as

$$P_{\mathrm{fa}} = P_1 \quad \text{when: } \Delta C_m = 0 \text{ and } \Delta\varphi_m = 0 \tag{30}$$

On the other hand, the detection rate P_{d} is the probability that the hypothesis H_1 is correct

$$P_{\mathrm{d}} = P_1 \quad \text{when: } \Delta C_m \neq 0 \text{ or } \Delta\varphi_m \neq 0 \tag{31}$$

According to (26)–(31), it is not difficult to find that the thresholds T_1 and T_2, the carrier-to-noise ratio, and K will affect the false alarm rate P_{fa} and the detection rate P_{d}. Considering that the thresholds are usually calculated based on the required P_{fa} [12], we will not discuss the influence of the thresholds, and set T_1 is 0.1 chip and T_2 is 0.05π radian in the rest of the paper.

The effects of the carrier-to-noise ratio and K on P_{fa} and P_{d} are shown in Figs. 7 and 8. Obviously, with the increase of the carrier-to-noise ratio and K, the false alarm rate P_{fa} becomes lower while the detection rate P_{d} becomes higher. As we mentioned earlier, the variance of $I_{\mathrm{E},m}^{(K)}$, $Q_{\mathrm{E},m}^{(K)}$, $I_{\mathrm{P},m}^{(K)}$, $Q_{\mathrm{P},m}^{(K)}$, $I_{\mathrm{L},m}^{(K)}$, and $Q_{\mathrm{L},m}^{(K)}$ is $f_{\mathrm{s}}T\sigma^2/2K$. According to (15), the variance is also equal to $A_m^2 f_{\mathrm{s}}^2 T/8K(C/N_0)_m$. For the carrier-to-noise ratio and K, their increase can reduce the variance, which is equivalent to reducing the inaccuracy of the

$$\begin{aligned} p_{m,1}^{(K)}\left(w_{m,1}^{(K)}\right) = {} & \frac{2w_{m,1}^{(K)}}{\left(\left(w_{m,1}^{(K)}\right)^2+1\right)} \times \exp\left(-\frac{\left(a_{m,11}^{(K)}w_{m,1}^{(K)}\right)^2 + \left(a_{m,12}^{(K)}\right)^2}{2\left(\left(w_{m,1}^{(K)}\right)^2+1\right)}\right) \\ & \times \left(\left(1 + \frac{\left(a_{m,11}^{(K)}\right)^2 + \left(a_{m,12}^{(K)}w_{m,1}^{(K)}\right)^2}{2\left(\left(w_{m,1}^{(K)}\right)^2+1\right)}\right) \times I_0\left(\frac{a_{m,11}^{(K)}a_{m,12}^{(K)}w_{m,1}^{(K)}}{\left(w_{m,1}^{(K)}\right)^2+1}\right) + \left(\frac{a_{m,11}^{(K)}a_{m,12}^{(K)}w_{m,1}^{(K)}}{\left(w_{m,1}^{(K)}\right)^2+1}\right) \times I_1\left(\frac{a_{m,11}^{(K)}a_{m,12}^{(K)}w_{m,1}^{(K)}}{\left(w_{m,1}^{(K)}\right)^2+1}\right)\right) \\ & \begin{cases} a_{m,11}^{(K)} = \sqrt{2TK(C/N_0)_m}(0.5 + \Delta C_m) \\ a_{m,12}^{(K)} = \sqrt{2TK(C/N_0)_m}(0.5 - \Delta C_m) \end{cases} \end{aligned} \tag{28}$$

$$\begin{aligned} p_{m,2}^{(K)}\left(w_{m,2}^{(K)}\right) = {} & \frac{1}{\pi\left(\left(w_{m,2}^{(K)}\right)^2+1\right)} \times \exp\left(-\frac{\left(a_{m,21}^{(K)}\right)^2 + \left(a_{m,22}^{(K)}\right)^2}{2}\right) \\ & + \frac{a_{m,21}^{(K)} + a_{m,22}^{(K)}w_{m,2}^{(K)}}{\sqrt{2\pi}\left(\left(w_{m,2}^{(K)}\right)^2+1\right)^{3/2}} \times \exp\left(-\frac{\left(a_{m,22}^{(K)} - a_{m,21}^{(K)}w_{m,2}^{(K)}\right)^2}{2\left(\left(w_{m,2}^{(K)}\right)^2+1\right)}\right) \times \left(1 - Q\left(\frac{a_{m,21}^{(K)} + a_{m,22}^{(K)}w_{m,2}^{(K)}}{\sqrt{\left(w_{m,2}^{(K)}\right)^2+1}}\right)\right) \\ & \begin{cases} a_{m,21}^{(K)} = \sqrt{2TK(C/N_0)_m}(1 - |\Delta C_m|)\cos(\Delta\varphi_m) \\ a_{m,22}^{(K)} = \sqrt{2TK(C/N_0)_m}(1 - |\Delta C_m|)\sin(\Delta\varphi_m) \end{cases} \end{aligned} \tag{29}$$

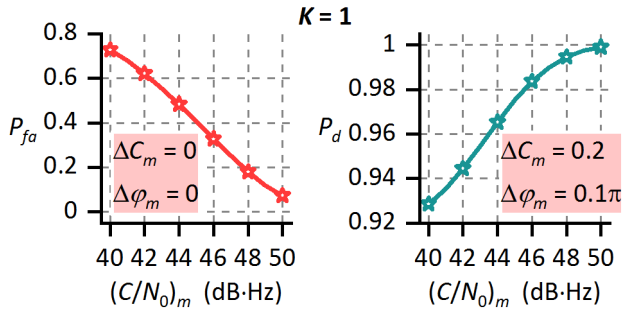

Fig. 7 *False alarm rate and the detection rate under various carrier-to-noise ratios*

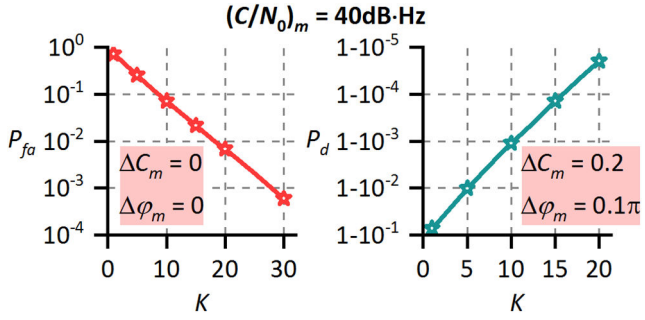

Fig. 8 *False alarm rate and the detection rate with various K*

SQM metrics η_1 and η_2. Therefore, P_{fa} is lower, and P_d is higher. For a certain carrier-to-noise ratio, by increasing K, P_{fa} could be approximated to zero, and P_d could be approximated to one. It proves that the proposed SQM-based method is effective for spoofing detection.

In addition, the larger the pseudo-code phase difference ΔC_m and the carrier phase difference $\Delta \varphi_m$, which means the greater influence affected by spoofing attacks, the higher the detection rate P_d. It can be shown in Fig. 9.

4 Simulations and spoofing detection performance evaluation

A software vector receiver based on Matlab is explored for simulations, and its structure is as shown in Fig. 1. The simulations in this section are performed on the signals generated by a signal source, which can simulate the satellite signals with a pre-set position and time. The spoofing pseudo-code phases and spoofing carrier Doppler shifts of all signals could be adjusted. We regard a simulated signal is authentic when its spoofing pseudo-code phase and spoofing carrier Doppler shift equal to zero. Otherwise, it is a spoofing signal. There are six signals for simulations and they correspond to different satellites. The PRNs for the satellites are 2, 12, 13, 17, 20, and 28. And the geometry distribution of the satellites is shown in Fig. 2. In subsequent simulations, the control of the carrier-to-noise ratio is achieved by adding simulated Gaussian white noise.

Obviously, the correlation peaks do not overlap in the simulations. For the scalar tracking structure, SQM methods are invalid in this scenario. While for the vector tracking structure, the previous analysis results indicate that the proposed SQM-based spoofing detection method is still useful. This is the most significant difference between the application of SQM techniques to the scalar tracking structure and the vector tracking structure. We will verify the feasibility of the proposed SQM-based spoofing detection method for the vector tracking structure through the simulations and evaluate its spoofing detection performance for the cases where the correlation peaks are separated.

4.1 Simulation 1: No spoofing attack

When there is no spoofing attack, the parameters $(\xi_1, \ldots, \xi_6)$ corresponding to all signals are close to zero. As depicted in

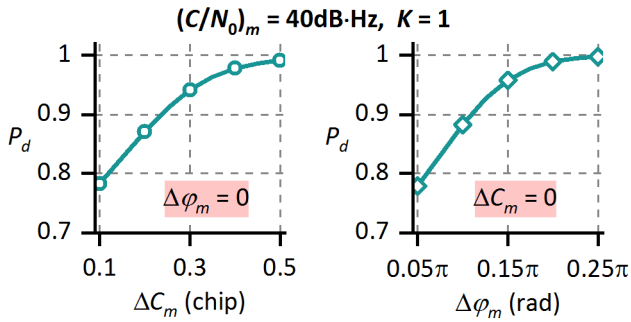

Fig. 9 *Detection rate with various pseudo-code phase differences and carrier phase differences*

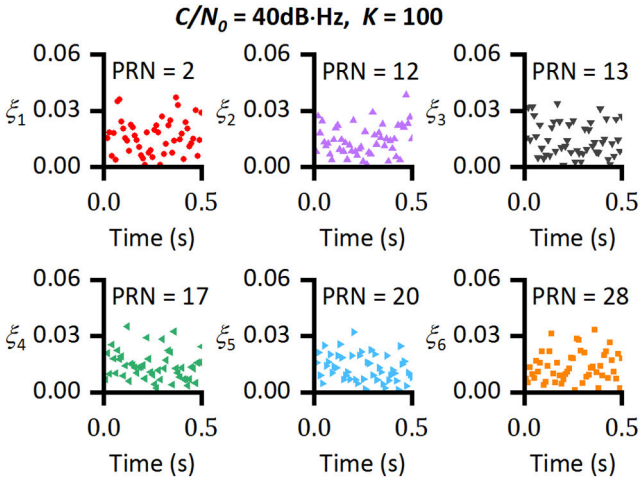

Fig. 10 *Parameters corresponding to all signals when there is no spoofing attack*

Fig. 10, these parameters are approximate, and there is no noticeable size difference. The largest parameters at different times correspond to different signals. Hence the choice of the mth signal could be arbitrary in this case. We choose the signal with PRN 2 for the subsequent binary hypothesis test in Simulation 1.

Here, we are interested in the probability density functions of the SQM metrics η_1 and η_2. As shown in Fig. 11, the probability density functions $p(\eta_1)$ and $p(\eta_2)$ in three cases are tested.

Obviously, the simulation results, which are obtained by counting 20,000 data, are roughly consistent with the theoretical curves. The ideal η_1 and η_2 are approximately equal to zero when there is no spoofing attack. Comparing the three cases, it is not hard to find that there is less error in the case of higher carrier-to-noise ratio and larger K. This is in line with our analysis in the previous section. In addition, we also test the false alarm rate P_{fa} in the three cases. As shown in Table 1, the greater the carrier-to-noise ratio and K, the lower the false alarm rate P_{fa}. Considering that noise will be introduced when collecting the signals generated by the signal source, we can deem that the simulation results are approximate to the theoretical results, which also supports the probability analysis in Section 3.3.

On the other hand, the false alarm rate P_{fa} is about 0.1 when the carrier-to-noise ratio is 40 dB·Hz and K is 10. By increasing K, P_{fa} could be reduced continuously and finally approached zero. It means that the probability of detecting spoofing attacks is close to zero.

4.2 Simulation 2: One spoofing signal

For the case of one spoofing signal, we adopt three spoofing strategies, including spoofing attacks only on pseudo-code, spoofing attacks only on carrier Doppler, and spoofing on both pseudo-code and carrier Doppler.

We implement the three spoofing strategies on each signal separately. The detection rates obtained by simulation statistic and theoretical calculation in the situation of the carrier-to-noise ratio

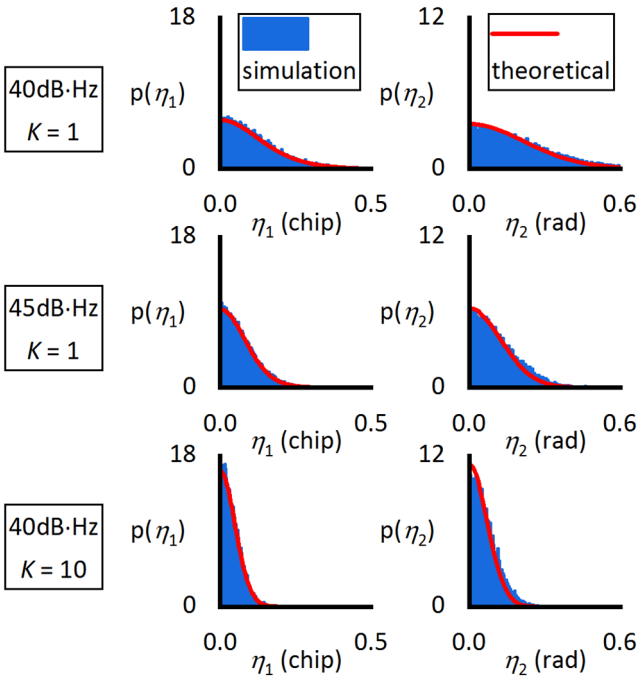

Fig. 11 *Probability density functions of the SQM metrics η_1 and η_2 in three cases when there is no spoofing attack*

Table 1 False alarm rate in three cases

Three Cases		Theoretical P_{fa}	Simulation P_{fa}
C/N_0, dB·Hz	K		
40	1	0.7264	0.7473
45	1	0.4076	0.4321
40	10	0.0719	0.1092

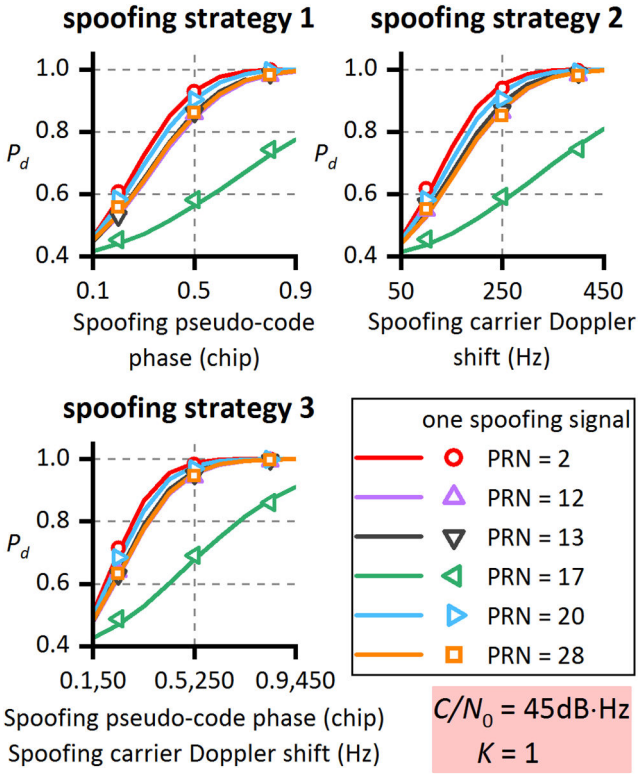

Fig. 12 *Detection rate under three spoofing strategies*

45 dB·Hz and $K = 1$ are compared in Fig. 12. Red indicates the case that the signal with PRN 2 is a spoofing signal and the other signals are authentic. Other colours are similar. The hollow points indicate the simulation results and the solid lines indicate the theoretical results. We emphasise again that the correlation peaks do not overlap in the three spoofing strategies.

Table 2 Detection rate in three cases

Three Cases		Theoretical P_d	Simulation P_d
C/N_0, dB·Hz	K		
40	1	0.9101	0.9107
45	1	0.9550	0.9451
40	10	0.9949	0.9822

Table 3 Spoofing strategy

Spoofing signal, PRN	Spoofing pseudo-code phase, chip	Spoofing carrier Doppler shift, Hz
12	0.5	250
13	0.5	250
17	0.5	250

For the spoofing scenarios in Simulation 2 that all authentic and spoofing signals correspond to different satellites, SQM methods are out of operation for the scalar tracking structure because the correlation peaks do not overlap. Nevertheless, it can be seen from Fig. 12 that for the vector tracking structure, the proposed SQM-based method is still useful for spoofing detection, whether the spoofing attacks are on pseudo-code or on carrier Doppler. It proves that SQM techniques have a wider application range for the vector tracking structure.

In general, for the case of one spoofing signal, the larger the spoofing pseudo-code phase and the spoofing carrier Doppler shift, the larger the pseudo-code phase differences and the carrier phase differences. Then, the detection rate will be greater. On the other hand, for different spoofing signals, even if the spoofing pseudo-code phases and spoofing carrier Doppler shifts are respectively the same, the pseudo-code phase differences and carrier phase differences are different. Hence the detection rate is different for each spoofing signal, as shown in Fig. 12. It is related to the satellite geometry distribution that determines the measurement matrix $\boldsymbol{H}$, which could be concluded from (20) and (21). And the simulation results are consistent with the calculation results, which further supports our theoretical analysis.

In addition, we also test the detection rate P_d in three cases. Only the signal with PRN 2 is a spoofing signal. Its spoofing pseudo-code phase is 0.4 chip and spoofing carrier Doppler shift is 200 Hz. As shown in Table 2, the greater the carrier-to-noise ratio and K, the higher the detection rate P_d. When the carrier-to-noise ratio is 40 dB·Hz and K is 10, P_d is about 0.99. By increasing K, P_d could be increased continuously and finally approached one. It means that the probability of detecting spoofing attacks is close to one.

4.3 Simulation 3: multiple spoofing signals

For the case of multiple spoofing signals, the spoofing strategy is as shown in Table 3, where the carrier-to-noise ratio is 45 dB·Hz.

In this situation, the parameters corresponding to all signals are shown in Fig. 13. Obviously, the signal with PRN 20 corresponds to the largest parameter. This is consistent with what we mentioned in Section 3.2 that the signal corresponding to the largest parameter does not necessarily a spoofing signal. It also means that the proposed SQM-based spoofing detection method for the vector tracking structure cannot identify spoofing signals. While SQM methods are more extensive in the application range for the vector tracking structure than the scalar tracking structure. The vector tracking structure further extends the spoofing detection ability of SQM.

Besides, the probability density functions of the SQM metrics η_1 and η_2, which are derived from the coherent integration results of the signal with PRN 20, are shown in Fig. 14. The simulation results are approximately consistent with the theoretical curves. Compared with the probability density functions in no spoofing environments, which are presented in Fig. 11, obviously, η_1 and η_2

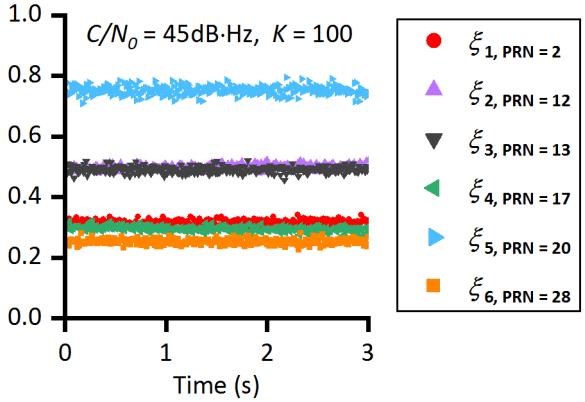

Fig. 13 *Parameters corresponding to all signals*

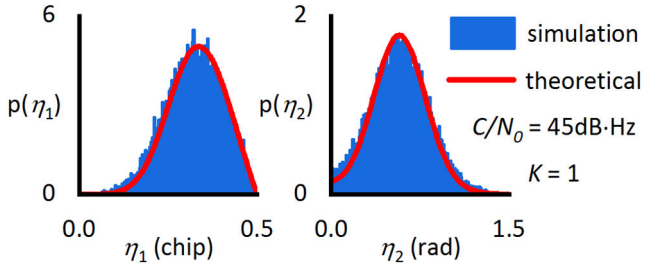

Fig. 14 *Probability density functions of the SQM metrics η_1 and η_2 when there are spoofing attacks*

in Fig. 14 deviate more from zero. It is in line with the fact that spoofing attacks will cause the pseudo-code phase differences $(\Delta C_1, \ldots, \Delta C_N)$ and carrier phase differences $(\Delta\varphi_1, \ldots, \Delta\varphi_N)$ between received signals and locally generated signals to deviate from zero.

The above simulations prove that for the spoofing scenario that the correlation peaks do not overlap, the proposed SQM-based method for the vector tracking structure could detect spoofing attacks on both pseudo-code and carrier Doppler. Besides, with the increasing of the carrier-to-noise ratio and the K, which is the number of the consecutive coherent integration times, the false alarm rate P_{fa} could be reduced to near zero, and the detection rate P_{d} could be increased to near one.

5 Conclusion

For the vector tracking structure, we propose an SQM-based spoofing detection method. Its detection performance is analysed and evaluated through a series of simulations. Analysis and simulation results demonstrate that the inconsistency among received signals due to spoofing attacks can affect the coherent integration results of the vector tracking structure, so the proposed method is useful even for the spoofing scenarios where the correlation peaks do not overlap. It is the most significant difference between the application of SQM techniques to the scalar tracking structure and the vector tracking structure.

On the other hand, the proposed method can detect spoofing attacks on both pseudo-code and carrier Doppler through the pseudo-code phase differences and carrier phase differences between received signals and locally generated signals that are estimated by the coherent integration results. Without modifying the receiver hardware architecture, the proposed methods only use the existing observations in the tracking process, which is highly practical for the vector tracking structure.

In reality, these characteristics mainly come from the vector tracking structure itself. We could naturally consider that the vector tracking structure extends the spoofing detection ability of SQM.

6 Acknowledgments

This work was supported by the National Natural Science Foundation of China (grant nos. 61973181 and 61571255) and the Tsinghua University Initiative Scientific Research Program (grant no. 2018Z05JZY004).

7 References

[1] Kerns, A.J., Shepard, D.P., Bhatti, J.A., *et al.*: 'Unmanned aircraft capture and control via GPS spoofing', *J Field Robot*, 2014, **31**, (4), pp. 617–636

[2] Bhatti, J., Humphreys, T.E.: 'Hostile control of ships via false GPS signals: demonstration and detection', *Navigation*, 2017, **64**, (1), pp. 51–66

[3] Sun, C., Wayn, C.J., Dempster, A.G., *et al.*: 'Moving variance-based signal quality monitoring method for spoofing detection', *GPS Solut.*, 2018, **22**, (83), pp. 1–13

[4] Broumandan, A., Jafarnia-Jahromi, A., Lachapelle, G.: 'Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver', *GPS Solut.*, 2014, **19**, (3), pp. 1–13

[5] Jovanovic, A., Botteron, C., Farine, P.A..: 'Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers'. Proc. IEEE/ION Position, Location and Navigation Symp. (PLANS), Monterey, CA, USA, May 2014, pp. 1258–1271

[6] Ali, P., Ali, B., Lachapelle, G.: 'Characterization of signal quality monitoring techniques for multipath detection in GNSS applications', *Sensors*, 2017, **17**, (7), pp. 1579–1602

[7] Phelts, R.E.: 'Multicorrelator techniques for robust mitigation of threats to GPS signal quality', PhD thesis, Stanford University, 2001

[8] Wesson, K.D., Shepard, D.P., Bhatti, J.A., *et al.*: 'An evaluation of the vestigial signal defense for civil GPS anti-spoofing'. Proc. The 24th Int. Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS), Portland, OR, USA, September 2011, pp. 2646–2656

[9] Hu, Y., Bian, S., Cao, K., *et al.*: 'GNSS spoofing detection based on new signal quality assessment model', *GPS Solut.*, 2018, **22**, (28), pp. 1–13

[10] Yang, Y., Li, H., Lu, M.: 'Performance assessment of signal quality monitoring based GNSS spoofing detection techniques'. Proc. China Satellite Navigation Conf. (CSNC), Xi'an, People's Republic of China, May 2015, pp. 783–793

[11] Jafarnia-Jahromi, A., Broumandan, A., Daneshmand, S., *et al.*: 'Galileo signal authenticity verification using signal quality monitoring methods'. Proc. Int. Conf. on Localization and Global Navigation Satellite Systems (ICL-GNSS), Barcelona, Spain, June 2016, pp. 1–8

[12] Pirsiavash, A., Broumandan, A., Lachapelle, G.: 'Two-dimensional signal quality monitoring for spoofing detection'. Proc. ESA/ESTEC NAVITEC, Noordwijk, The Netherlands, December 2016, pp. 1–12

[13] Li, H., Yang, J.: 'Analysis and simulation of vector tracking algorithms for weak GPS signals'. Proc. Int. Asia Conf. on Informatics in Control, Automation and Robotics, Wuhan, People's Republic of China, March 2010, pp. 215–218

[14] Lashley, M., Bevly, D.M.: 'Comparison of traditional tracking loops and vector based tracking loops for weak GPS signals'. Proc. The Institute of Navigation 2008 Int. Technical Meeting (ION ITM), San Diego, CA, USA, January 2008, pp. 310–316

[15] Lashley, M., Bevly, D.M., Hung, J.Y.: 'Performance analysis of vector tracking algorithms for weak GPS signals in high dynamics', *IEEE. J. Sel. Top. Signal. Process.*, 2009, **3**, (4), pp. 661–673

[16] Liu, J., Cui, X., Lu, M., *et al.*: 'Vector tracking loops in GNSS receivers for dynamic weak signals', *J. Syst. Eng. Electron.*, 2013, **24**, (3), pp. 349–364

[17] Lin, T., Abdizadeh, M., Broumandan, A., *et al.*: 'Interference suppression for high precision navigation using vector-based GNSS software receivers'. Proc. The 24th Int. Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS), Portland, OR, USA, September 2011, pp. 372–383

[18] Li, F., Wu, R., Wang, W.: 'The anti-jamming performance analysis for vector tracking loop'. Proc. China Satellite Navigation Conf. (CSNC), Changsha, People's Republic of China, May 2016, pp. 665–675

[19] Wang, F.: 'GNSS Anti-Spoofing Techniques Based on Multi-Signal Processing', PhD thesis, Tsinghua University, 2018

[20] He, L., Li, H., Lu, M.: 'Dual-antenna GNSS spoofing detection method based on Doppler frequency difference of arrival', *GPS Solut.*, 2019, **23**, (78), pp. 1–14

[21] Juang, J.C.: 'Analysis of global navigation satellite system position deviation under spoofing', *IET Radar Sonar Navig.*, 2009, **3**, (1), pp. 1–7

[22] Zhang, X., Li, H., Yang, C., *et al.*: 'The development of real-time vector receiver on hardware platform and the assessment of anti-spoofing capability'. Proc. China Satellite Navigation Conf. (CSNC), Harbin, People's Republic of China, May 2018, pp. 399–412

[23] Kaplan, E.D.: '*Understanding GPS: principles and applications*' (Artech House, USA., 2006)

[24] Simon, M.K.: '*Probability distributions involving Gaussian random variables a handbook for engineers and scientists*' (Kluwer Academic Pub, The Netherlands, 2006)