THE JOURNAL OF NAVIGATION (2018), **71**, 1111–1129.
doi:10.1017/S0373463318000206

GNSS Spoofing Detection Technique Using Fraction Parts of Double-difference Carrier Phases

Yanfeng Hu[1], Shaofeng Bian[1], Bing Ji[1] and Juan Li[2]

[1](*Department of Navigation Engineering, Naval University of Engineering, Wuhan, China*)
[2](*College of Electromechanical Engineering, Qingdao Agricultural University, Qingdao, China*)
(E-mail: daohang_yanfeng@163.com)

With electronic warfare increasingly complicated and military confrontations increasingly intense, the potential security threat to satellite navigation has become a difficult issue to deal with. Traditional satellite navigation anti-interference technology generally refers to jamming, but less consideration has been given to spoofing. It should be noted that the potential risk induced by spoofing interference is worse than that caused by jamming as the loss of positioning integrity may not be immediately obvious. This paper introduces a spoofing detection method based on a two-antenna structure using fraction parts of double-difference carrier phase observables. If all spoofing signals are transmitted by one single antenna, a spoofing detection hypothesis test can be carried out through the normalisation of double-difference carrier phase observables, without need to consider the integer ambiguity problem, measure the baseline vector and estimate the real directions of signals. The detection scheme adopts an M of N algorithm (if M or more of the test values exceed the threshold, the algorithm declares the presence of a spoofing signal), integrating carrier phase measurements of all the available satellites. Finally, the proposed method is verified by real experiments. This spoofing detection method can easily be applied to GNSS anti-spoofing receivers without changing their architecture and has simple and effective characteristics.

KEYWORDS

1. GNSS. 2. Spoofing detection. 3. Reliability. 4. Double-difference carrier phases. 5. Fraction parts.

Submitted: 2 August 2016. Accepted: 18 March 2018. First published online: 30 April 2018.

1. INTRODUCTION. Global Navigation Satellite Systems (GNSS) can offer all-weather services such as position, velocity and time to many worldwide applications. With rapid economic development, GNSS are playing a more and more crucial role in communications and transportation. There has been much concern about the availability and accuracy of GNSS, but until recently, only limited attention has been paid to the threats to safety when GNSS are targeted. In 2001, the United States Department of Transportation

released a transportation report, which highlighted the dangers of GNSS spoofing (Volpe, 2001). Jamming means broadcasting high-power interference to make the accuracy of GNSS receivers decrease or even stop working. Spoofing is a more sophisticated interference pattern, which can make GNSS receivers output incorrect navigation information (such as position, velocity and time), through transmitting false GNSS signals. GNSS spoofing attacks which may cause a serious threat to security are much more dangerous than jamming (Humphreys et al., 2008) as the errors may not immediately apparent to the user, and thus may contribute to an incident as a result of incorrect information. In 2011, Iran's military authorities announced that they successfully captured a modern military Unmanned Air Vehicle (UAV) controlled by the United States (US) Central Intelligence Agency (CIA), which appeared to use a spoofing attack for military purposes. This incident greatly shocked the US military and government (Wesson et al., 2012a; Hu et al., 2018).

1.1. *GNSS Anti-spoofing solutions.* Today, a variety of anti-spoofing measures are available for safeguarding GNSS receivers against spoofing attacks (Kuhn, 2005; Bardout, 2011). These countermeasures based on GNSS receivers can be generally divided into two types: cryptographic techniques and non-cryptographic techniques.

Cryptographic techniques are classified into three categories: spreading code cryptographic measures (Humphreys, 2013), Navigation Message Authentication (NMA) measures (Wesson et al., 2012b; Kerns et al., 2014) and codeless cross correlation measures (Heng et al., 2015; O'Hanlon et al., 2010; Psiaki et al., 2013a). The first two require obvious modifications in the signal structure, but they are impractical for immediate use because of their significant cost and complexity. The third does not need to change the signal inner architecture. It is a relatively practical approach compared with the first two. From previously published papers (Heng et al., 2015; O'Hanlon et al., 2010), the reference receiver is generally assumed to be reliable (non-spoofed). Psiaki et al. (2013b) extended the application of the dual-receiver P(Y)-code correlation method to a network of receivers with high availability.

Non-cryptographic techniques can be classified into two categories: external assistance and signal processing. The first refers to those techniques that need external assistance from other devices, such as inertial sensors (accelerometer, angular acceleration sensor, etc) (Khanafseh et al., 2014; Lee et al., 2015), odometers and high stability clocks (Hwang and McGraw, 2014; Jafarnia-Jahromi et al., 2013; Shepard et al., 2012). Also, compound navigation modes such as multi-GNSS, GNSS/Regional Navigation Satellite Systems (RNSS) and GNSS/Inertial Navigation Systems (INS), can effectively cope with GNSS spoofing attacks. The second focuses on analysing the features of received signals, without the aid of other devices. Generally, spoofing signals may have different features in some aspects such as paths of propagation, absolute signal power, relative power, noise level and multipath. GNSS receivers can detect the existence of spoofing signals by analysing abnormal features (Akos, 2012; Broumandan et al., 2012; Dehghanian et al., 2012; Jafarnia-Jahromi et al., 2012).

1.2. *New spoofing detection method using fraction parts of double-difference carrier phases.* Generally, a spoofer transmits all of the false signals from a single antenna, as it is quite difficult to solve problems such as time synchronisation that exist for a multi-antenna-spoofer (Humphreys et al., 2008; Wesson et al., 2012b). This paper introduces a two-antenna spoofing detection method into a new test in which fraction parts of double-difference carrier phase observables are used. Psiaki et al. (2013a; 2013b; 2014)

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

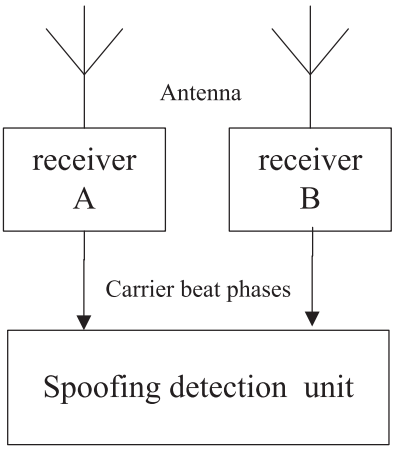

Figure 1. The primary structure of the spoofing detection system.

investigated a spoofing detection method based on single-difference processing. Broumandan et al. (2016) and Jafarnia-Jahromi et al. (2014) have researched a spoofing detection method based on double-difference processing with the integer problem taken into account. In contrast, the method proposed in this paper gives emphasis to the use of the fraction parts of double-difference carrier phases without considering the integer ambiguity problem. The proposed method adopts the concept of the M of N (Lee et al., 2015) detection scheme which can work well with only single-epoch-carrier-phase observation information. If M or more of the test values exceed the threshold, the algorithm declares the presence of a spoofing signal. The decision scheme used for this detection system, which integrates all double-difference carrier phase observables available, has high reliability in resistance to spoofing attacks for a single-antenna spoofer.

1.3. *Organisation of the remainder of this paper.* Section 2 describes the two-antenna structure which provides the framework for the spoofing detection system. Section 3 introduces the primary processing flow of the spoofing detection unit and proposes a double-difference carrier phase observables normalisation method which supplies a theoretical basis for subsequent detection schemes. Section 4 presents the spoofing detection hypothesis test and the M of N algorithm (Lee et al., 2015) for the decision scheme. Section 5 reports on two experiments for the purpose of verifying the proposed spoofing detection method. Finally, Section 6 summarises the paper.

2. SPOOFING DETECTION SYSTEM STRUCTURES.

Our detection system mainly consists of two GNSS receivers (receiver A and receiver B) and a spoofing detection unit. This system is depicted in Figure 1. The antennae of receivers A and B are respectively expressed as Antenna A and Antenna B. $\vec{b}_{BA}$ denotes the baseline vector from Antenna A to Antenna B, of which the direction is from A to B (depicted in Figure 2). $\vec{r}^{\,j}$ denotes the authentic signal propagation vector from satellite j to the GNSS receiver and $\vec{r}^{\,sp}$ denotes the spoofing signal propagation vector from the spoofer to the GNSS receiver. When it meets the terms $|\vec{b}_{BA}| \ll \vec{r}^{\,j}$, $|\vec{b}_{BA}| \ll \vec{r}^{\,sp}$, the signal propagation vector to the phase centre of Antenna A can be assumed to be parallel to that of Antenna B.

The primary principle of this detection system is to use the two-antenna geometry to analyse the features of the in-space signal. As shown in Figure 2, in the no-spoofing case,

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

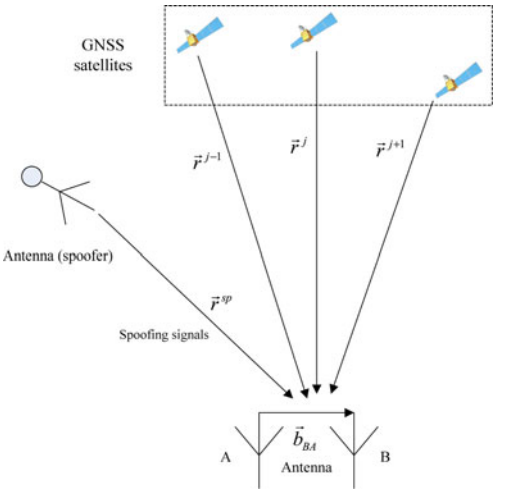

Figure 2. Spoofing attack scenario.

the propagation paths of satellites available are $(\ldots, \vec{r}^{\,j-1}, \vec{r}^{\,j}, \vec{r}^{\,j+1})$, which are generally different from one another; in the spoofed case, different GNSS signals come from the same direction, namely $\vec{r}^{\,sp}$.

The spoofing detection unit is used to judge whether spoofing is present or not, according to the carrier beat phases from two GNSS receivers. This module can serve as a separate module with its own hardware and software. It can also be incorporated into one of the GNSS receivers (A or B). It can also be just a set of software which can run well on a PC or other platforms.

The spoofing detection unit gets the carrier phase observation φ_A^j $(j = 1 \ldots N)$ from GNSS receiver A and φ_B^j from GNSS receiver B. Then it obtains single-difference carrier phase $\Delta\varphi_{BA}^j$ and double-difference carrier phase $\Delta\varphi_{BA}^{ij}$ $(i \neq j)$. To eliminate the influence of GNSS integer ambiguity resolution, the fraction parts, namely ϕ_{BA}^{ij}, can be obtained by use of the rounding-off method. When ϕ_{BA}^{ij} is obtained, the unit enters the decision scheme stage, which will be introduced in the next chapter.

3. DOUBLE-DIFFERENCE CARRIER PHASES NORMALISATION. The proposed spoofing detection method is based on double-difference carrier phase observations, the characteristics of which are different in the non-spoofed case and in the spoofed case. However, due to the existence of integer ambiguity, the double-difference carrier phase observations are not directly available for use, and this needs to be normalised in some way. The flow diagram of this unit is shown in Figure 3.

3.1. *Specific analysis of non-spoofed case and spoofed case.* The single-difference carrier phase model for the non-spoofed case is:

$$\begin{aligned}\Delta\varphi_{BA}^j &= \varphi_B^j - \varphi_A^j \\ &= -\lambda^{-1}(\vec{r}^{\,j})^T A\vec{b}_{BA} + \Delta N_{BA}^j + n_{mul\_BA}^j + n_{ther\_BA}^j\end{aligned} \tag{1}$$

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

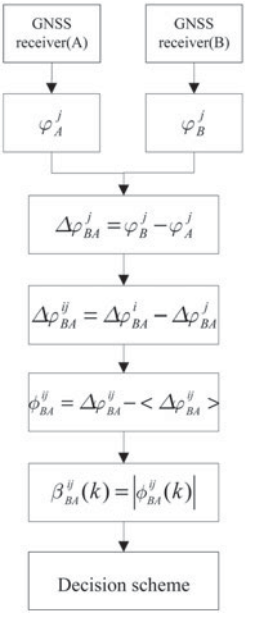

Figure 3. Work flowchart of spoofing detection unit.

where φ_B^j and φ_A^j respectively represent the beat carrier phases of the signal from satellite j received by Antenna A and Antenna B. The single-difference carrier phase is denoted as $\Delta\varphi_{BA}^j$, the nominal carrier wavelength is λ, the transfer matrix from body coordinates to reference coordinates is A ($\vec{r}^j$ is defined in the reference coordinates and $\vec{b}_{BA}$ is defined in the local antenna body coordinates), the single-difference integer ambiguity term is ΔN_{BA}^j, the single-difference multipath noise term is $n_{mul\_BA}^j$ (zero-mean Gaussian noise, standard deviation is σ_{mul}) and the single-difference thermal noise term is $n_{ther\_BA}^j$ (zero-mean Gaussian noise, standard deviation is σ_{ther}).

The receiver thermal noise standard deviation σ_t can be estimated according to the following formula (Betz, 2000).

$$\sigma_t = \frac{1}{2\pi}\sqrt{\frac{B_L}{C/N_0}\left[1 + \frac{1}{2T_{\text{coh}}C/N_0}\right]} \tag{2}$$

where B_L is the noise bandwidth of the phase-lock loop. As B_L decreases, the filtering effect gets better, and the performance of tracking high dynamic signals gets worse. That is to say, the value of B_L cannot be extremely high or extremely low. As for an on board user, the reasonable range of B_L is 1 Hz ~25 Hz. In this paper, B_L = 20Hz is taken as an average example. σ_t denotes the standard deviation of receiver thermal noise from φ_B^j (or φ_A^j) and σ_{ther} refers to the standard deviation of the single-difference thermal noise term $n_{ther\_BA}^j$ from $(\varphi_B^j - \varphi_A^j)$. According to signal processing theory, σ_{ther} is $\sqrt{2}$ times as much as σ_t in the single-difference process. When the received carrier-to-noise ratio for each branch of signals is 35 dB-Hz, and T_{coh} = 1 ms is the integration time, we can get $\sigma_{ther} = \sqrt{2}\sigma_t \approx 0{\cdot}0193$(cycles). The single-difference multipath error standard deviation is $\sigma_{mul} = 0{\cdot}33$(rad) $\approx 0{\cdot}0525$(cycles) (Psiaki et al., 2014). The multipath sigma formula is

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

simplified in order to simulate an average multipath environment. Considering the flexibility of multipath signals, such as in complex urban conditions, further research is needed to improve the model.

The double-difference carrier phase in the non-spoofed case can be expressed as:

$$\begin{aligned}\Delta\varphi_{BA}^{ij} &= \Delta\varphi_{BA}^{i} - \Delta\varphi_{BA}^{j} \\ &= -\lambda^{-1}(\vec{r}^{\,i} - \vec{r}^{\,j})^{T} A\vec{b}_{BA} + (\Delta N_{BA}^{i} - \Delta N_{BA}^{j}) \\ &\quad + (n_{mul\_BA}^{i} - n_{mul\_BA}^{j}) + (n_{ther\_BA}^{i} - n_{ther\_BA}^{j}) \\ &= -\lambda^{-1}(\vec{r}^{\,i} - \vec{r}^{\,j})^{T} A\vec{b}_{BA} + \Delta N_{BA}^{ij} + n_{mul\_BA}^{ij} + n_{ther\_BA}^{ij}\end{aligned} \tag{3}$$

where $\Delta\varphi_{BA}^{ij}$ denotes the double-difference carrier phase, ΔN_{BA}^{ij} is the double-difference integer-ambiguity term, $n_{mul\_BA}^{ij}$ (zero-mean Gaussian noise, standard deviation is $\sqrt{2}\sigma_{mul}$) is the double-difference multipath noise term and $n_{ther\_BA}^{ij}$ (zero-mean Gaussian noise, standard deviation is $\sqrt{2}\sigma_{ther}$) the double-difference thermal noise term. σ_{mul} represents the standard deviation of $n_{ther\_BA}^{i}$, and $n_{ther\_BA}^{ij}$ equals $(n_{ther\_BA}^{i} - n_{ther\_BA}^{j})$. Obviously, the standard deviation of $n_{ther\_BA}^{ij}$ is $\sqrt{2}\sigma_{ther}$, according to signal processing theory. Similarly, the standard deviation of $n_{mul\_BA}^{ij}$ is $\sqrt{2}\sigma_{mul}$.

The single-difference carrier phase model in the spoofed case can be expressed as:

$$\begin{aligned}\Delta\varphi_{BA}^{j} &= \varphi_{B}^{j} - \varphi_{A}^{j} \\ &= -\lambda^{-1}(\vec{r}^{\,sp})^{T} A\vec{b}_{BA} + \Delta N_{BA}^{j} + n_{mul\_BA} + n_{ther\_BA}^{j}\end{aligned} \tag{4}$$

where n_{mul_BA} represents the single-difference multipath noise term. As all the false signals have the same propagation, all the spoofing signals have the same multipath noise term and the same single-difference multipath noise term.

The double-difference carrier phase in the spoofed case is:

$$\begin{aligned}\Delta\varphi_{BA}^{ij} &= \Delta\varphi_{BA}^{i} - \Delta\varphi_{BA}^{j} \\ &= (\Delta N_{BA}^{i} - \Delta N_{BA}^{j}) + (n_{ther\_BA}^{i} - n_{ther\_BA}^{j}) \\ &= \Delta N_{BA}^{ij} + n_{ther\_BA}^{ij}\end{aligned} \tag{5}$$

In Equation (5), the double-difference carrier phase in the spoofed case only includes the double-difference integer-ambiguity term and the single-difference thermal noise term, since the $-\lambda^{-1}(\vec{r}^{\,sp})^{T} A\vec{b}_{BA}$ term and the n_{mul_BA} term are eliminated through double difference. If ΔN_{BA}^{ij} can be removed, $\Delta\varphi_{BA}^{ij}$ should only include $n_{ther\_BA}^{ij}$.

3.2. *Algorithm to obtain the fraction parts of double-difference carrier phase.* In order to obtain $\Delta\varphi_{BA}^{ij}$, $\vec{r}^{\,j}$, A and ΔN_{BA}^{ij} must be known accurately. However, there is much difficulty in doing so. Here, a practical way is proposed to obtain $\Delta\varphi_{BA}^{ij}$ while $\vec{r}^{\,j}$, A, and ΔN_{BA}^{ij} can be ignored.

$$\begin{aligned}\phi_{BA}^{ij} &= \Delta\varphi_{BA}^{ij} - <\Delta\varphi_{BA}^{ij}> \\ &= f(\Delta\varphi_{BA}^{ij})\end{aligned} \tag{6}$$

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

where $<\Delta\varphi_{BA}^{ij}>$ means taking the Rounding Numbers (omitting decimal fractions smaller than 0·5 and counting all others) of $\Delta\varphi_{BA}^{ij}$; ϕ_{BA}^{ij} ranging from −0·5 cycles to 0·5 cycles denotes the normalised result of $\Delta\varphi_{BA}^{ij}$. $f(x) = x - <x>$ is a user-defined function.

For example, $\Delta\varphi_{BA}^{ij}$

$$-1{\cdot}22, 0{\cdot}51, 3{\cdot}42, 5$$

After normalisation, ϕ_{BA}^{ij}

$$-0{\cdot}22, -0{\cdot}49, 0{\cdot}42, 0$$

In the spoofed case, the normalised result is equivalent to that of eliminating the double-difference integer-ambiguity term ΔN_{BA}^{ij}. In the non-spoofed case, $-\lambda^{-1}(\vec{r}^{\,i} - \vec{r}^{\,j})^T A\vec{b}_{BA}$ will not always be an integer, so ϕ_{BA}^{ij} will not always be close to a value of zero, which is different from that in the spoofed case.

4. DECISION SCHEME.

In Section 3, the eliminating of the impacts of the integer ambiguity results in normalised measurement values. This section presents a final judgement model.

4.1. *Spoofing detection hypothesis test for decision scheme.*

Through the normalisation mentioned above, ϕ_{BA}^{ij} is obtained which ranges from −0.5 cycles to 0.5 cycles. In the spoofed case, $\phi_{BA\_sp}^{ij}$ (referring to ϕ_{BA}^{ij}, in the spoofed case) is approximately equal to $n_{ther\_BA}^{ij}$ (zero-mean Gaussian noise, standard deviation is $\sqrt{2}\sigma_{ther}$).

$$\phi_{BA\_sp}^{ij} = f(n_{ther\_BA}^{ij}) \approx n_{ther\_BA}^{ij}, \sigma_{sp} = \sqrt{2}\sigma_{ther} \tag{7}$$

In the non-spoofed case, a new parameter γ^{ij} is introduced, which ranges from −0·5 cycles to 0·5 cycles.

$$-\lambda^{-1}(\vec{r}^{\,i} - \vec{r}^{\,j})^T A\vec{b}_{BA} = N^{ij} + \gamma^{ij} \tag{8}$$

Then $\Delta\varphi_{BA\_au}^{ij}$ is obtained as follows:

$$\Delta\varphi_{BA\_au}^{ij} = N^{ij} + \Delta N_{BA}^{ij} + \gamma^{ij} + n_{mul\_BA}^{ij} + n_{ther\_BA}^{ij} \tag{9}$$

Then we can get $\phi_{BA\_au}^{ij}$ as:

$$\phi_{BA\_au}^{ij} = f(\Delta\varphi_{BA\_au}^{ij}) = f(\gamma^{ij} + n_{mul\_BA}^{ij} + n_{ther\_BA}^{ij}), \sigma_{au} = \sqrt{2\sigma_{mul}^2 + 2\sigma_{ther}^2} \tag{10}$$

Herein, a detection test is designed to discriminate between the following two hypotheses. Under the hypothesis H_0, spoofing is absent and under the hypothesis H_1, spoofing is present.

$$\begin{cases} H_0 : p(z|H_0), \text{spoofing is absent} \\ H_1 : p(z|H_1), \text{spoofing is present} \end{cases} \tag{11}$$

where z refers to ϕ_{BA}^{ij} and m refers to γ^{ij}. A generalised likelihood ratio test can be designed. Let T_h be the threshold. When $|z|$ is less than T_h, H_0 is trustworthy and when $|z|$ is no less than T_h, H_1 is trustworthy.

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

As for the non-spoofed case, $(\gamma^{ij} + n^{ij}_{mul\_BA} + n^{ij}_{ther\_BA})$ obeys a Gaussian distribution with the mean m, shown in Equation (12).

$$\begin{cases} x = m + n^{ij}_{mul\_BA} + n^{ij}_{ther\_BA} \\ p(x) = \dfrac{1}{\sqrt{2\pi}\sigma_{au}} \exp\left(-\dfrac{(x-m)^2}{2\sigma^2_{au}}\right) \end{cases} \tag{12}$$

Based on the normalised mechanism discussed above, we can get the possible values of x, as shown in Equation (13).

$$z = f(x) = f(N+z), N = \cdots, -2, -1, 0, 1, 2, \cdots \tag{13}$$

As z ranges from $-0{\cdot}5$ cycles to $0{\cdot}5$ cycles, $p(N+z)$ is far less than $\min(p(z), p(1+z), p(-1+z))$, when N is bigger than 1, according to Equation (12). Through approximate processing, we can get the following expression:

$$p(z|H_0) = \sum_{N=-\infty}^{\infty} p(N+z) \approx p(z) + p(1+z) + p(-1+z) \tag{14}$$

Combining Equations (12) and (13), we can obtain $p(z|H_0)$, as shown in Equation (14).

$$p(z|H_0) \approx \frac{1}{\sqrt{2\pi}\sigma_{au}} \left\{ \begin{array}{l} \exp\left(-\dfrac{(z-m)^2}{2\sigma^2_{au}}\right) + \exp\left(-\dfrac{(1+z-m)^2}{2\sigma^2_{au}}\right) \\ + \exp\left(-\dfrac{(-1+z-m)^2}{2\sigma^2_{au}}\right) \end{array} \right\} \tag{15}$$

According to Equation (15), the false alarm probability P_{fam} can be expressed as:

$$\begin{aligned} P_{fam} &= \int_{-T_h}^{T_h} p(z|H_0)dz \\ &\approx \frac{1}{2}\left[\begin{array}{l} erf\left(\dfrac{m+T_h}{\sqrt{2}\sigma_{au}}\right) - erf\left(\dfrac{m-T_h}{\sqrt{2}\sigma_{au}}\right) + erf\left(\dfrac{1+T_h-m}{\sqrt{2}\sigma_{au}}\right) \\ -erf\left(\dfrac{1-T_h-m}{\sqrt{2}\sigma_{au}}\right) + erf\left(\dfrac{1+T_h+m}{\sqrt{2}\sigma_{au}}\right) - erf\left(\dfrac{1-T_h+m}{\sqrt{2}\sigma_{au}}\right) \end{array} \right] \end{aligned} \tag{16}$$

In the spoofed case, it is easy to get the following expression according to Equation (7)

$$p(z|H_1) = \frac{1}{\sqrt{2\pi}\sigma_{sp}} \exp\left(-\frac{z^2}{2\sigma^2_{sp}}\right) \tag{17}$$

Then the detection probability is

$$P_d = \int_{-T_h}^{T_h} p(z|H_1)dz = 2\int_0^{T_h} p(z|H_1)dz = erf\left(\frac{T_h}{\sqrt{2}\sigma_{sp}}\right) \tag{18}$$

Herein, the variation tendency of P_{fam} with the rise of T_h leads to different values of $|m|$ as shown in Figure 4.

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

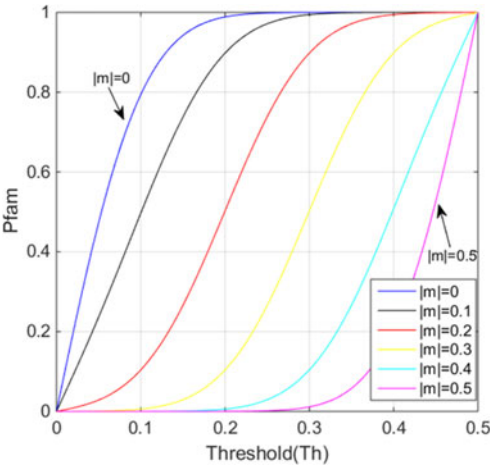

Figure 4. Probability of false alarm for different |m| values.

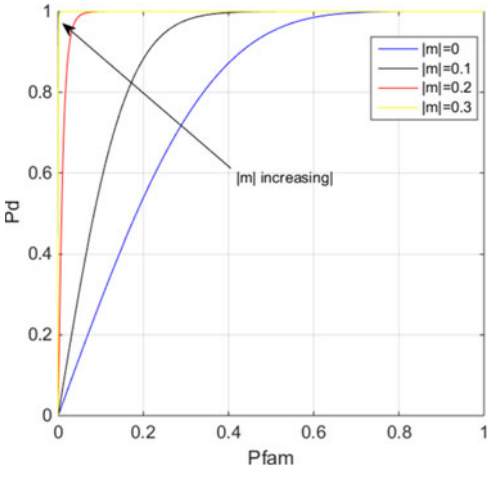

Figure 5. ROC curves for different |m| values.

Figure 4 shows that when $|m|$ is constant, the false alarm probability P_{fam} increases as the threshold T_h rises; when T_h is constant, P_{fam} decreases as $|m|$ rises. Therefore, in order to make P_{fam} lower, the threshold must be lowered since it is infeasible to raise $|m|$. However, γ^{ij} can hardly be known in advance but it varies with time. The larger $|m|$ is, the better the performance of spoofing detection will be (see Figure 5). If $|m|$ is unknown, it is impossible to obtain P_{fam}. Accordingly, suppose that γ^{ij} obeys a uniform distribution ranging from $-0{\cdot}5$ cycles to $0{\cdot}5$ cycles. The new definition of false alarm probability P_{fa} can be defined as:

$$P_{fa} = \frac{1}{Q}\sum_{k=1}^{Q} P_{fam}\left(z \left| \gamma^{ij} = \frac{k}{Q} - 0{\cdot}5\right.\right) \tag{19}$$

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

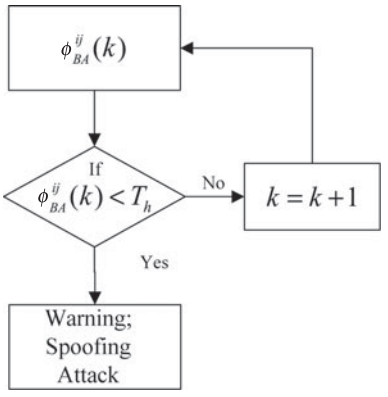

Figure 6. Flow chart of decision scheme with one single set of double-difference carrier phase.

The detailed derivation process is as follows. According to the theorem of total probability,

$$P(B) = \sum_{k=1}^{Q} P(B|A_k)P(A_k) \tag{20}$$

where $P(B)$ refers to P_{fa}, A_k refers to $\gamma^{ij} = \frac{k}{Q} - 0{\cdot}5$ and $P(A_k) = \frac{1}{Q}$. Thus, the detailed derivation process is expressed as:

$$\begin{aligned} P_{fa} &= P(B) \\ &= \sum_{k=1}^{Q} P(B|A_k)P(A_k) \\ &= \frac{1}{Q}\sum_{k=1}^{Q} P(B|A_k) \\ &= \frac{1}{Q}\sum_{k=1}^{Q} P_{fam}\left(z \left| \gamma^{ij} = \frac{k}{Q} - 0{\cdot}5\right.\right) \end{aligned} \tag{21}$$

At this point, we obtain the calculation method of P_{fa}, which is a significant step for spoofing detection.

4.2. *M of N algorithm for decision scheme.* When there is a single set of double-difference carrier phase observations available, the threshold is set as T_h. In this case, the decision scheme for spoofing detection will work, as shown in Figure 6. When ϕ_{BA}^{ij} is less than T_h, it gives a warning that spoofing is present.

According to Equation (21), Q should be large enough to make P_{fa} close to the real value. Here Q is set as 10,000, and then an ROC curve connecting (P_{fa}, P_d) pairs for different thresholds T_h can be obtained, as shown in Figure 7. For example, if P_d = 99·99%, then T_h = 0.106 (cycles) and P_{fa} = 21·19%, which indicates that the false alarm probability is high. If so, a multi-set of double-difference carrier phase observations should be taken into account.

As shown in Figure 8, when the same N satellites are available to both of the GNSS receivers, (N-1)-set of double-difference carrier phase observations can be obtained. At a

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

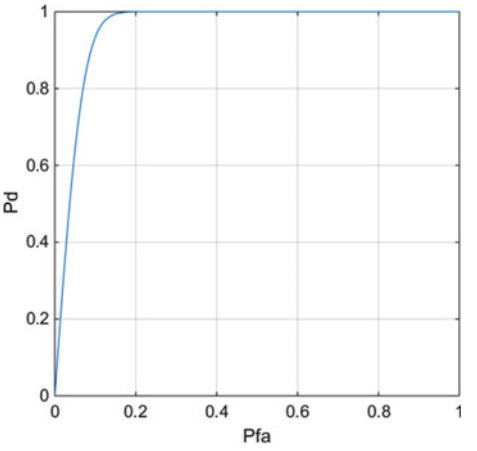

Figure 7. ROC curve of pairwise check connecting (P_{fa}, P_d) pairs.

given time, if M-set values surpass the pre-set threshold, the spoofing detection unit gives a warning about the existence of a spoofing attack. Then the probability of false alarm P_{FA} and the probability of detection P_D can be derived from Equations (22) and (23).

$$\begin{aligned} P_{FA} &= \Pr ob(Sp \geq M|H_1) \\ &= \sum_{x=M}^{N-1} \binom{N-1}{x} P_{fa}^{x}(1-P_{fa})^{N-1-x} \end{aligned} \tag{22}$$

$$\begin{aligned} P_D &= \Pr ob(Sp \geq M|H_0) \\ &= \sum_{x=M}^{N-1} \binom{N-1}{x} P_{d}^{x}(1-P_{d})^{N-1-x} \end{aligned} \tag{23}$$

When the threshold is fixed at $T_h = 0{\cdot}106$ cycles, $P_{fa} = 21{\cdot}19\%$ and $P_d = 99{\cdot}99\%$ can be obtained. Figures 9 and 10 show that for the established M, P_{FA} increases with N, while P_D decreases with N. When M always chooses the maximal value, namely $(N-1)$, P_{FA} decreases as N increases, as is shown in Figure 9. Similarly, when M always chooses the maximal value, P_D decreases as N increases, as shown in Figure 10. With $M = N - 1 = 7$ as an example, it is easy to obtain $P_{FA} \approx 1{\cdot}918 \times 10^{-5}$ and $P_D \approx 99{\cdot}93\%$.

Without loss of generality, we set $N = 8$ $(M = 1, 2, 3, \ldots, 7)$ as an example to analyse the detection performance theoretically. Figure 11 shows the detection probability of different M values, with the increase of T_h. Figure 12 shows the probability of false alarm for different M values, with the increase of T_h. The detection probability P_D and the probability of false alarm P_{FA} increase with T_h. Furthermore, P_D and P_{FA} decrease as M increases. ROC curves of pairwise checks connecting (P_{FA}, P_D) pairs are shown in Figure 13. Obviously, the bigger M is, the better the spoofing detection performance.

5. EXPERIMENTS.

To verify the proposed method, two experiments under two conditions—spoofing conditions and authentic conditions, were carried out. From the published literature, it is not easy to obtain complete equipment for spoofing and anti-spoofing

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

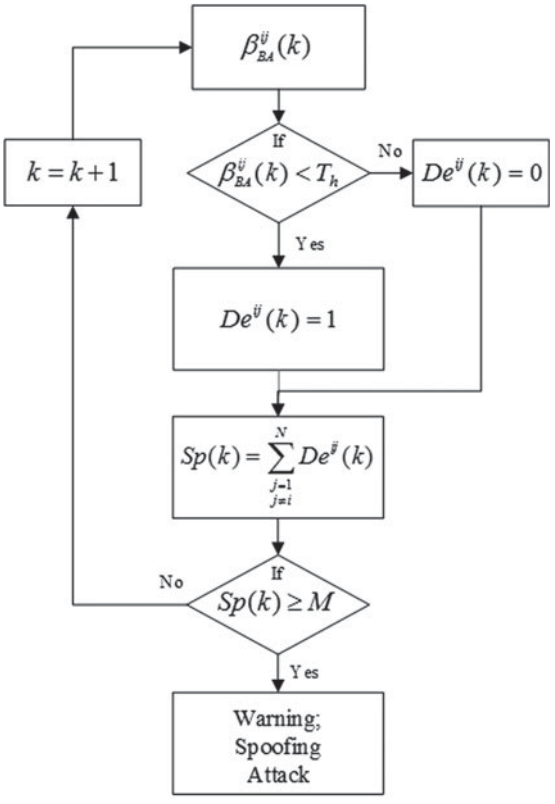

Figure 8. Flow chart of M of $(N-1)$ algorithm.

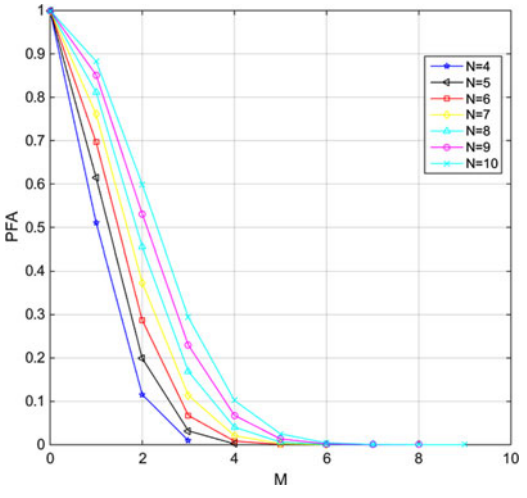

Figure 9. Variation tendency of P_{FA} with M.

experiments especially in the domestic arena and it is illegal to spread spoofing signals outdoors. Therefore, the experiment under spoofing conditions was carried out using a GNSS signal transponder (THC-TRANS-GB series) which can bring outdoor GNSS satellite

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

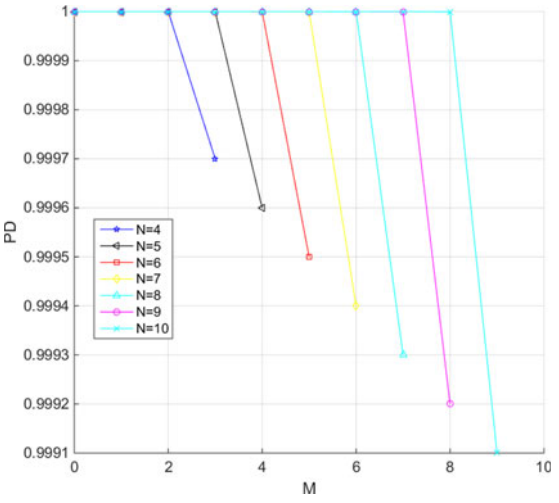

Figure 10. Variation tendency of P_D with M.

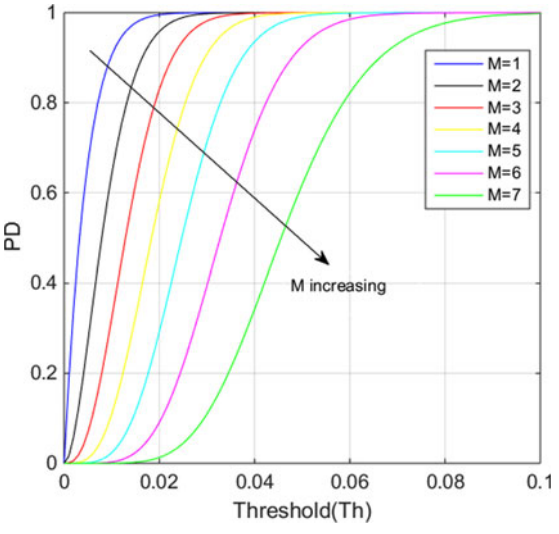

Figure 11. Probability of detection for different M.

signals indoors. In general, all the retransmitting GNSS signals are from the same indoor transmitting antenna of the GNSS signal transponder, which means all GNSS PRNs have the same propagation path.

In the experiments, we employed two Hi-Target V8 GNSS receivers working in Global Positioning System (GPS) L1C mode. The elevation masks for satellites were set at 15° and the sample interval of carrier phase observations was set as 5 seconds. The distance between the two receivers was about 50 cm. The two receivers can automatically record and save original observation data, which we copied to the PC for follow-up processing.

5.1. *Experiment in the non-spoofed case.* The experiment time was 10:14–10:44 on 9 February 2018. We put the two receivers on a high iron frame located at the roof of No. 113

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

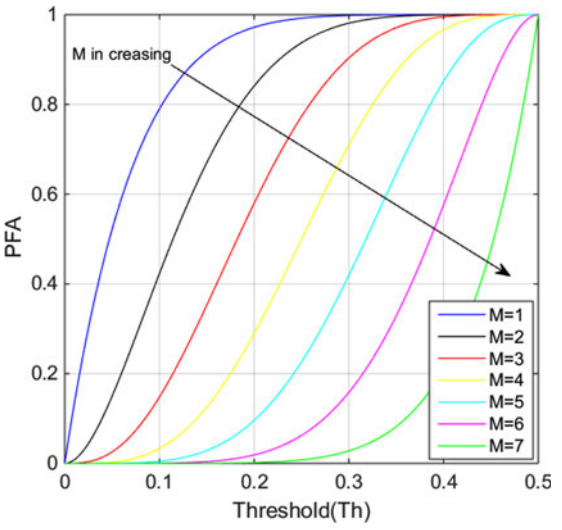

Figure 12. Probability of false alarm for different M.

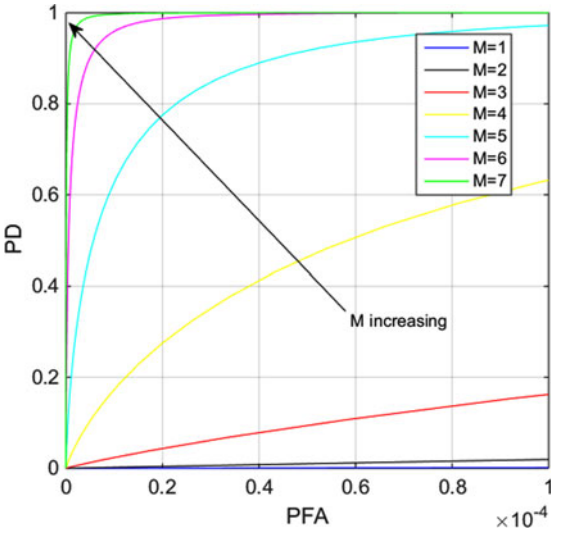

Figure 13. ROC curves of pairwise check connecting (P_{FA}, P_D) pairs.

building of College of Electrical Engineering, Naval University of Engineering, as shown in Figure 14.

Through post-processing of the static data, the distribution of available GPS satellites in the non-spoofed case was obtained, as shown in Figures 15 and 16. We found that over 30 minutes, there were eight satellites (PRN 2, PRN 5, PRN 13, PRN 15, PRN 20, PRN 21, PRN 24 and PRN 29) which were always available.

The seven groups of the double-difference carrier phase observations can be obtained based on the carrier phase observations of the eight available satellites. By normalisation, ϕ_{BA}^{ij} can be obtained as shown in Figure 17. When the threshold is fixed at $T_h = 0{\cdot}106$ cycles, the test parameter sp can be obtained as shown in Figure 18.

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

Figure 14. Experiment scene in the non-spoofed case.

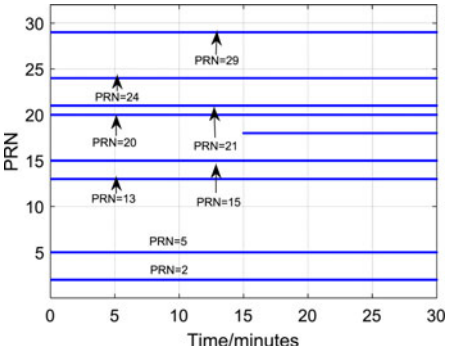

Figure 15. Visibility of GPS satellites in the non-spoofed case.

As shown in Figure 17, the normalised carrier differences in the non-spoofed case change considerably between −0·5∼0·5. Taking the blue curve as an example, when the normalised carrier differences are around the −0·5 or 0·5 values, a constant phase cycle slip appears among the adjacent values. That is consistent with theoretical analysis based on Equation (6): −3·49, −3·51− > −0·49, 0·49. As shown in Figure 18, all the values of *sp* are not more than 2, which means as the threshold of *sp* is set as 3∼7, there will be no false alarms for the spoofing detection unit, in the non-spoofed case.

5.2. *Experiment in the spoofed case.* Experiment Time was 10:14–10:44 on 10 February 2018. The outdoor antenna of the GNSS signal transponder was placed on the high iron frame located at the roof of No. 113 building of College of Electrical Engineering and the indoor antenna of GNSS signal transponder was placed in the corner of the laboratory, as shown in Figure 19.

Through post-processing of the static data, the distribution of available GPS satellites in the spoofed case is exactly the same as that in the non-spoofed case, since the motion period of GPS satellites is about 24 hours.

The seven groups of the double-difference carrier phase observations can be obtained based on the carrier phase observations of the eight available satellites. After normalisation, can be obtained as shown in Figure 20. When the threshold is fixed at = 0·106 cycles, the test parameter *sp* can be obtained as shown in Figure 21.

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

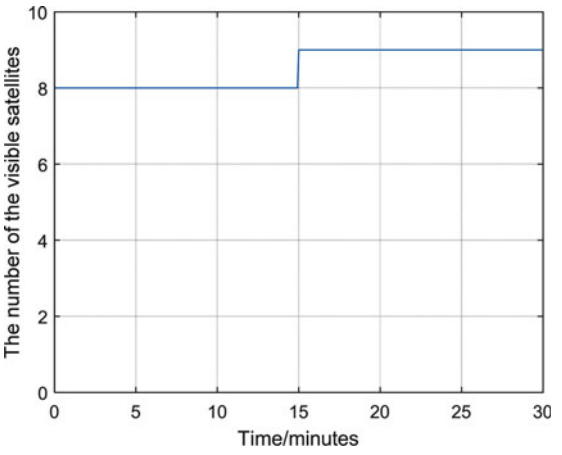

Figure 16. Number of available GPS satellites in the non-spoofed case.

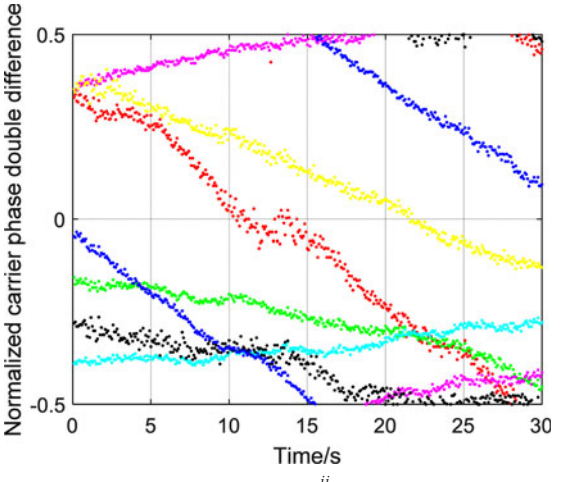

Figure 17. Variation tendency of ϕ_{BA}^{ij} in the non-spoofed case.

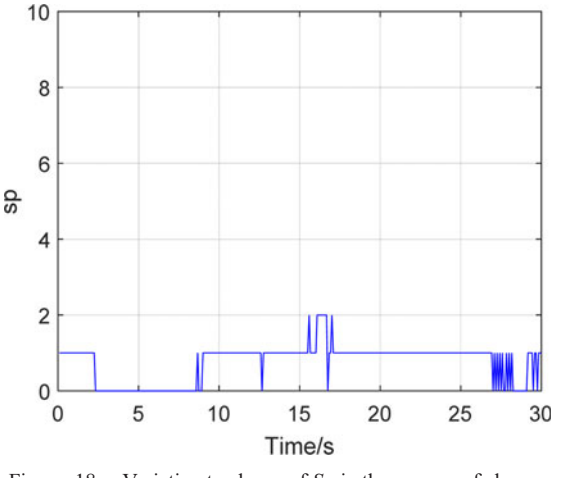

Figure 18. Variation tendency of Sp in the non-spoofed case.

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

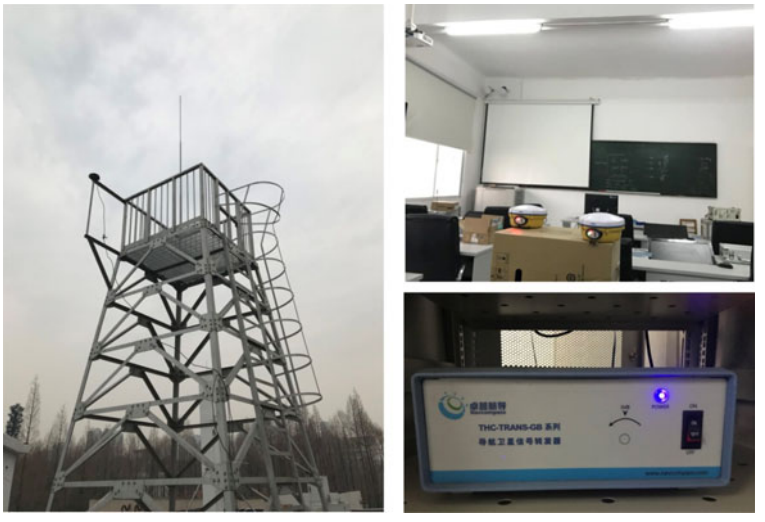

Figure 19. Experiment scene in the spoofed case.

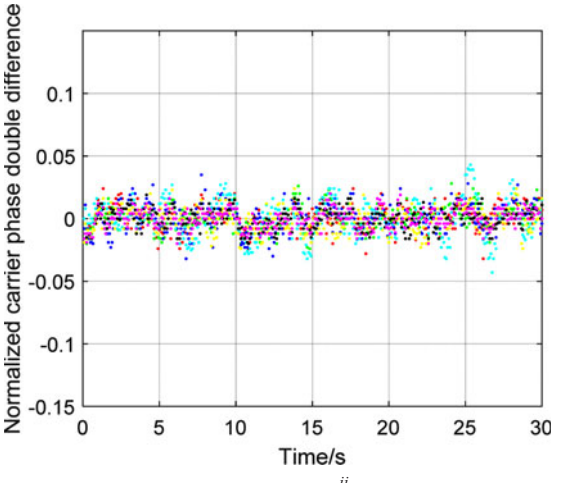

Figure 20. Variation tendency of ϕ_{BA}^{ij} in the spoofed case.

As shown in Figure 20, the normalised carrier differences in the spoofed case fluctuate slightly between −0·05∼0·05. As is shown in Figure 21, all the values of *sp* are 7, which means as the threshold of *sp* is set as 7, the spoofing detection can effectively alert the user to the spoofing attacks.

6. SUMMARY. This paper has presented a GNSS spoofing detection method using fraction parts of double-difference carrier phases. The detection system is based on a two-antenna architecture, which does not need to change the internal hardware structure of the two GNSS receivers. This detection unit can take the form of a software module and can be integrated into one of the two GNSS receivers, or as an independent software module which can run well on a PC or other platforms. The detection algorithm of the spoofing

https://doi.org/10.1017/S0373463318000206 Published online by Cambridge University Press

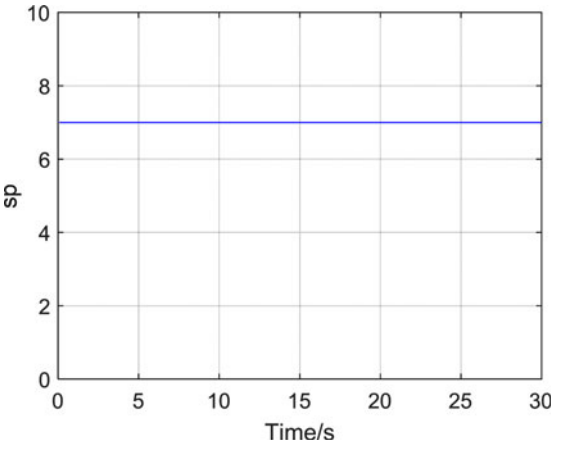

Figure 21. Variation tendency of *Sp* in the spoofed case.

detection system is highly reliable and also relatively simple. It can effectively cope with spoofing attacks with all spoofing signals from the same spoofing transmitting antenna quite well, without the need to know the baseline vector of the two antennae, the directions of authentic signals and the location of the spoofing transmitting antenna. Because of the problem of integer ambiguity, it is quite difficult to calculate the real carrier phases of the signal accurately. The fraction parts of double-difference carrier phases can be obtained by normalisation, and so it is not necessary to calculate the integer ambiguity values. In the decision scheme, the M of N algorithm involving all of the $(N-1)$-set of fraction parts of double-difference carrier phases, can function well in detecting the spoofing.

To improve the robustness of this method, it is important to take T_h and M into account. The use of multi-calendar metadata to make decision and analysis is also worthy of study.

In summary, the spoofing detection system described in this paper is easy to apply to a GNSS anti-spoofing receiver, with simple and effective characteristics. However, further developments are needed in order to produce a sufficiently reliable detection system for other spoofing scenarios.

ACKNOWLEDGMENT

This paper is supported by the Natural Science Foundation of China (Nos. 41704034, 41674037, 41631072).

REFERENCES

Akos, D. (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *Navigation*, **59**, 281–290.

Bardout, Y. (2011). Authentication of GNSS position: An assessment of spoofing detection methods. *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Portland, OA.

Betz, J. W. (2000). Effect of narrowband interference on GPS code tracking accuracy. *Proceedings of the National Technical Meeting of the ION*, Anaheim, CA.

Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J. and Lachapelle, G. (2012). GNSS spoofing detection in handheld receivers based on signal spatial correlation. Position, *Location and Navigation Symposium-PLANS IEEE*, Myrtle Beach, SC.

Broumandan, A., Jafarnia-Jahromi, A., Daneshmand, S., and Lachapelle, G. (2016). Overview of Spatial Processing Approaches for GNSS Structural Interference Detection and Mitigation. *Proceedings of the IEEE*, **104**, 1246–1257.

Dehghanian, V., Nielsen, J. and Lachapelle, G. (2012). GNSS spoofing detection based on receiver C/No estimates. *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Nashville, TN.

Heng, L., Work, D. and Gao, G. (2015). GPS Signal Authentication from Cooperative Peers. *IEEE Transactions on Intelligent Transportation Systems*, **16**, 1794–1805.

Humphreys, T., Ledvina, B., Psiaki, M., O'Hanlon, B. and Kintner, M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proceedings of the 21st International Technical Meeting of The Satellite Division of the Institute of Navigation*, Savannah, GA.

Humphreys, T. (2013). Detection Strategy for Cryptographic GNSS Anti-Spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, **49**, 1073–1090.

Hu, Y., Bian, S., Cao, K., and Ji, B. (2018). GNSS spoofing detection based on new signal quality assessment model. *GPS Solutions*, (online, https://doi.org/10.1007/s10291-017-0693-7).

Hwang, P. and McGraw, G. (2014). Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis. *Position, Location and Navigation Symposium-PLANS IEEE*, Monterey, CA.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. and Lachapelle, G. (2012). GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. *International Journal of Satellite Communications and Networking*, **30**, 181–191.

Jafarnia-Jahromi, A., Daneshmand, S., Broumandan, A., Nielsen J. and Lachapelle G. (2013). PVT Solution Authentication Based on Monitoring the Clock State for a Moving GNSS Receiver. *European Navigation Conference*, Vienna, Austria.

Jafarnia-Jahromi, A, Broumandan, A, Daneshmand, S, Sokhandan, N. and Lachapelle, G. (2014). A double antenna approach toward detection, classification and mitigation of GNSS structural interference. *Proceedings of NAVITEC*, Noordwijk, Netherlands.

Kerns, A., Wesson, K. and Humphreys, T. (2014). A blueprint for civil GPS navigation message authentication. *Position, Location and Navigation Symposium-PLANS IEEE*, Monterey, CA.

Khanafseh, S., Roshan, N., Langel, S., Chan, F., Joerger, M. and Pervan, B. (2014). GPS spoofing detection using RAIM with INS coupling. *Position, Location and Navigation Symposium-PLANS IEEE*, Monterey, CA.

Kuhn, M. (2005). An asymmetric security mechanism for navigation signals. Information Hiding. Springer Berlin Heidelberg.

Lee, J., Kwon, K., An, D. and Shim, D. (2015). GPS spoofing detection using accelerometers and performance analysis with probability of detection. *International Journal of Control, Automation and Systems*, **13**, 951–959.

O'Hanlon, B., Psiaki, M., Humphreys, T. and Bhatti, J. (2010). Real-time spoofing detection in a narrow-band civil GPS receiver. *Proceedings of the 23th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Portland, OA.

Psiaki, M., Powell, S. and O'Hanlon, B. (2013a). GNSS Spoofing Detection: Correlating Carrier Phase with Rapid Antenna Motion. *GPS World*, **24**, 53–58.

Psiaki, M., O'Hanlon, B., Bhatti, J., Shepard, D. and Humphreys, T. (2013b). GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems*, **49**, 2250–2267.

Psiaki, M., O'Hanlon, B., Powel, S., Wesson, D. and Humphreys, T. (2014). GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase. *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation*, Tampa, FL.

Shepard, D., Humphreys, T. and Fansler, A. (2012). Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, **5**, 146–153.

Volpe, J. (2001). Vulnerability assessment of the transportation infrastructure relying on the global positioning system. *US Department of Transportation*.

Wesson, K., Shepard, D. and Humphreys, T. (2012a). Straight talk on anti-spoofing. *GPS World*, **23**, 32–39.

Wesson, K., Rothlisberger, M. and Humphreys, T. (2012b). Practical cryptographic civil GPS signal authentication. *Navigation*, **59**, 177–193.