IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 4, 2020, accepted June 12, 2020, date of publication June 16, 2020, date of current version June 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3002804

A New GNSS Spoofing Detection Method Using Two Antennas

JIAJIA CHEN[1,2], YING XU[1], HONG YUAN[1], AND YIGE YUAN[3]

[1]Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China
[2]School of Electronic, Electrical and Communicating Engineering, University of Chinese Academy of Sciences, Beijing 100049, China
[3]School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, China

Corresponding author: Hong Yuan (yuanhong@aircas.ac.cn)

This work was supported in part by the Youth Innovation Promotion Association CAS under Grant E03314020D, and in part by the ZFS19001D-KDXT under Grant Y9E0152M26.

ABSTRACT The security of global navigation satellite system (GNSS) has attracted a lot of attention recently. The spoofing detection method using multi-antenna array is one of the most efficient spoofing detection methods due to its unique geometry space. However, it is either based on the assumption that all spoofing signals come from the same direction or it requires additional inertial measurement unit (IMU) or multi-antenna attitude solution to obtain attitude information. In this paper, we propose a new GNSS spoofing detection method using only two off-the-shelf antennas. This method can detect a single spoofing signal or spoofing signals from multiple directions, and does not require any attitude information. This method employs the carrier phase and the known baseline length to estimate the baseline vector. Its theoretical performance can be assessed by the sum of squared error (*SSE*) test statistic. Static and dynamic experiments both prove that this method can distinguish the spoofing signal from the real signal effectively without any delay.

INDEX TERMS Carrier phase, global navigation satellite system, spoofing detection, two antennas.

I. INTRODUCTION

GNSS has been widely used in many key areas such as location services, weather forecasting, transportation, system timing and emergency rescue. However, GNSS signals can be interfered quite easily due to their low ground signal power [1]. In a verification experiment, the attacker successfully guided the hovering drone to the ground by using low-cost GNSS spoofing devices [2]. In another experiment, the attacker successfully induced the yacht full of passengers to deviate from the course without any warnings [3]. Therefore, it is necessary to conduct GNSS anti-spoofing researches as the destructiveness of spoofing attacks is already obvious [4].

Traditional receiver autonomous integrity detection (RAIM) only considers the consistency of pseudoranges, which is not enough to deal with the increasingly advanced spoofing attack methods [5]. In view of the existing GNSS spoofing technologies, many papers have proposed a variety of spoofing detection methods that can be divided into three types [6]–[24]. One kind of method is Navigation Message Authentication (NMA). This method encrypts civilian GNSS navigation data, and the receivers utilize the obtained signatures to ensure the security of GNSS signals [6]. However, this method requires changes to the current navigation message structure, which is very costly and difficult to implement. In addition, NMA technology is not able to achieve fast spoofing detection responses since it may require additional signal processing of the encrypted messages [7].

Another kind of method utilizes advanced RAIM technologies to detect the features of signals, such as the absolute power level of signals, PRN code correlation function, signal correlation peak, and other features [8]–[15]. The advanced RAIM method is relatively simple to implement. It only requires appropriate modifications to the software and hardware of the off-the-shelf receivers. But it may only be able to detect spoofing signals at the beginning of an attack and fail in recognition when the receiver has traced them.

The third kind of method employs the difference of spatial geometry between the spoofing signals with the real GNSS signals to perform spoofing detection [16]. It is one of the most efficient methods since the spatial geometry information of GNSS satellites is almost impossible to imitate. This method usually applies the carrier phase information received

The associate editor coordinating the review of this manuscript and approving it for publication was Li He.

by the multi-antenna array to estimate the directions of arrival (DOAs) of the signals [17], [18]. Traditional spoofing detection methods using multi-antenna array are either based on the assumption that all spoofing signals come from the same direction [19]–[22], or that they need to employ a IMU or multi-antenna attitude solution to obtain the attitude information of the antenna array [23], [24]. For the former, this method can effectively detect the spoofing signals when a single antenna broadcasts multiple spoofing signals. However, it cannot effectively work when there is a single spoofing signal or spoofing signals come from multiple directions. For the latter, the spoofing signals must be strictly phase synchronized with the real signals in order to achieve identical DOAs, and the coordinates of the antenna array are needed to be known in advance. Due to the impossibility of this situation, this method is a very robust way to quickly detect complex spoofing signals. However, the hardware cost of this method is relatively high since IMU or more than four antennas are required to gain attitude information.

In this paper, we propose a new GNSS spoofing detection method. This method employs two low-cost GNSS antennas to form a baseline vector and does not require IMU to provide attitude information. The baseline vector can be figured out by combining carrier phase double difference data with ephemeris data. We utilize the known baseline length to modify the calculated baseline vector, and take the corrected value as the approximation of the real value. After normalizing the baseline vector, the presence of spoofing signals can be assessed by *SSE* test statistic. This method is able to realize fast real-time detection, and detect a single spoofing signal or spoofing signals from multiple directions.

The remainder of this paper is divided into 4 sections. Section II describes the structure and the spoofing detection hypothesis test of the system. In Section III, the false alarm performance in the absence of spoofing signals is presented. Section IV describes the detection performance of the system in static and dynamic scenarios respectively. The last part summarizes the research results.

II. SPOOFING DETECTION HYPOTHESIS TEST

A. STRUCTURE OF SYSTEM

The spoofing detection system consisting of two GNSS antennas, two GNSS receivers and one signal processing unit is shown in Fig. 1. The baseline vector b_{BA} is formed by two GNSS antennas connected to a common reference oscillator. We employ antennas of the same model and batch to eliminate the errors caused by the inconsistency of the antenna phase center as much as possible. The length of baseline vector is quite easy to obtain, which we think is known in this paper. The inputs of the signal processing unit are the carrier phase and ephemeris observation data of all tracked signals received by the two antennas. The real-time spoofing detection results are the outputs of the signal processing unit.

The ionospheric and tropospheric errors of the antennas are considered to be completely identical as the baseline length is quite short [25]. The carrier phase single difference observation equation for satellite i is described as:

$$\begin{aligned}\Delta\tilde{\varphi}^i_{BA}\lambda &= \varphi^i_B\lambda - \varphi^i_A\lambda \\ &= \Delta\rho^i_{BA} + c\cdot V_{ij} + \Delta N^i_{BA}\lambda + n^i_{rBA}\lambda \\ &= (\hat{r}^i)^T\Delta X_{BA} + c\cdot V_{ij} + \Delta N^i_{BA}\lambda + n^i_{rBA}\lambda \end{aligned} \quad (1)$$

where φ^i_B and φ^i_A are the carrier phase observations of GNSS satellite i received by antenna B and A respectively. λ is the wavelength of the GNSS signal, $\Delta\rho^i_{BA}$ is the pseudorange difference measured by two antennas, c is the speed of light, V_{ij} is the receivers clock bias, and ΔN^i_{BA} is ambiguity of whole cycles. n^i_{rBA} is the zero-mean additive white Gaussian noise (AWGN). $\hat{r}^i$ is a $[3\times 1]$ matrix calculated from the broadcast ephemeris describing direction cosine from GNSS satellite i to antenna. ΔX_{BA} is a $[3\times 1]$ matrix describing the baseline vector based on earth-centered earth-fixed (ECEF), and $\Delta X_{BA} = [\Delta x_{BA}, \Delta y_{BA}, \Delta z_{BA}]^T$. ΔN^i_{BA} is easy to determine as the baseline length is quite short [26], so (1) can be written as:

$$\begin{aligned}\Delta\varphi^i_{BA}\lambda &= (\Delta\tilde{\varphi}^i_{BA} - \Delta N^i_{BA})\lambda \\ &= (\hat{r}^i)^T\Delta X_{BA} + c\cdot V_{ij} + n^i_{rBA}\lambda \end{aligned} \quad (2)$$

The corresponding observation equation of carrier phase double difference is given as follows:

$$\Delta\varphi^{ij}_{BA}\lambda = (\hat{r}^{ij})^T\Delta X_{BA} + n^{ij}_{rBA}\lambda \quad (3)$$

where $\Delta\varphi^{ij}_{BA}$ is the carrier phase double difference, $\hat{r}^{ij}$ is the direction cosine difference of satellite i and j, and n^{ij}_{rBA} is still the AWGN. Therefore, $\Delta\varphi^{ij}_{BA}$ follows the normal distribution.

When the number of observation satellites is N, the carrier phase double difference observation equation can be represented in matrix form as:

$$\Delta\varphi_{BA}\lambda = H\Delta X_{BA} + n_{rBA}\lambda \quad (4)$$

where $\Delta\varphi_{BA}$ is a $[(\mathrm{N}-1)\times 1]$ matrix describing carrier phase double difference between N−1 satellites and the reference

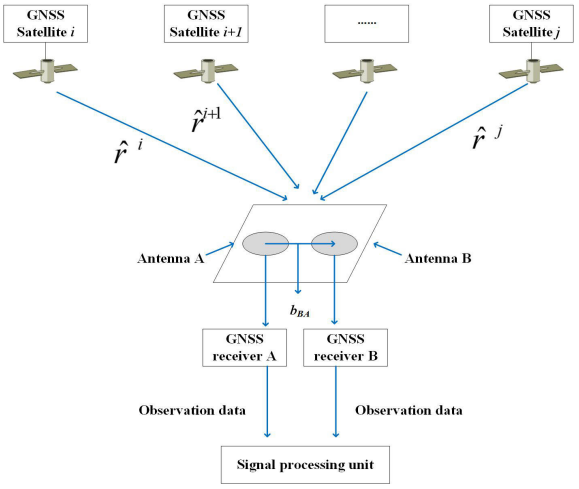


FIGURE 1. Structure of the spoofing detection system.

satellite i. H is a [(N−1) × 3] matrix describing direction cosine difference between N−1 satellites and reference satellite i. n_{rBA} is a [(N−1) × 1] observation noise matrix following independent normal distribution.

We employ the least squares method to calculate (4), and then ΔX_{BA} is obtained as;

$$\Delta X_{BA} = (H^T H)^{-1} H^T \Delta\varphi_{BA}\lambda \tag{5}$$

It is clear to see that ΔX_{BA} follows the normal distribution as $\Delta\varphi_{BA}$ does because ΔX_{BA} is positively correlated with $\Delta\varphi_{BA}$. We describe ΔX_{BA} as:

$$\begin{bmatrix} \Delta x_{BA} \sim N(b_x, \sigma_x^2) \\ \Delta y_{BA} \sim N(b_y, \sigma_y^2) \\ \Delta z_{BA} \sim N(b_z, \sigma_z^2) \end{bmatrix} \tag{6}$$

B. BASELINE VECTOR DIRECTION IS KNOWN

ΔX_{BA} can be normalized by (7) if the real baseline vector b_{BA} is known:

$$\Delta X'_{BA} = (\Delta X_{BA} - b_{BA})/\sigma_X \tag{7}$$

where $\Delta X'_{BA} = [\Delta x'_{BA}, \Delta y'_{BA}, \Delta z'_{BA}]^T$, $b_{BA} = [b_x, b_y, b_z]^T$, $\sigma_X = [\sigma_x, \sigma_y, \sigma_z]^T$. The quality of the solution for the baseline vector can be assessed by *SSE* test statistics. The *SSE* test metric is defined as follows:

$$SSE = \Delta x'^2_{BA} + \Delta y'^2_{BA} + \Delta z'^2_{BA} \tag{8}$$

The carrier phase observations match with the DOAs of the signals in the absence of spoofing signals, and then $\Delta X'_{BA}$ follows the standard normal distribution. The *SSE* metric follows the chi-square distribution with 3 degrees of freedom. In another case, significant deviation occurs between ΔX_{BA} and b_{BA}, and $\Delta X'_{BA}$ no longer follows the standard normal distribution if there are spoofing signals. The *SSE* metric follows the non-central chi-square distribution with a degree of freedom of 3 and non-zero non-centrality parameter γ:

$$\begin{aligned} &H_0(no\ \text{spoofing}): SSE \sim \chi^2(3) \\ &H_1(\text{spoofing}) : SSE \sim \chi'^2(3, \gamma) \end{aligned} \tag{9}$$

We assume that the satellite signal j is interfered by the meaconing spoofing signal, and the corresponding equation of carrier phase double difference is obtained as follows:

$$\Delta\varphi^{ij}_{spBA} = \Delta\varphi^{ij}_{BA} + \Delta\varphi^{ij}_{spau} \tag{10}$$

where $\Delta\varphi^{ij}_{spBA}$ and $\Delta\varphi^{ij}_{BA}$ are the carrier phase double difference of the spoofing signal and real signal respectively. $\Delta\varphi^{ij}_{spau}$ is the offset between $\Delta\varphi^{ij}_{spBA}$ and $\Delta\varphi^{ij}_{BA}$. We rewrite (2) as the following form, they are completely identical:

$$\Delta\varphi^{i}_{BA}\lambda = |d|\cos\theta_i + c \cdot V_{ij} + n^i_{rBA}\lambda \tag{11}$$

where d is the length of baseline vector, θ_i is the DOA of the signal, then (3) can also be written as the following form:

$$\Delta\varphi^{ij}_{BA}\lambda = |d|(\cos\theta_i - \cos\theta_j) + n^{ij}_{rBA}\lambda \tag{12}$$

Then we solve (12) and (10) simultaneously to work out $\Delta\varphi^{ij}_{spau}$:

$$\begin{aligned} \Delta\varphi^{ij}_{spau}\lambda &= \Delta\varphi^{ij}_{spBA}\lambda - \Delta\varphi^{ij}_{BA}\lambda \\ &= |d| \cdot (\cos\theta_{spj} - \cos\theta_j) + n^{ij}_{spau}\lambda \\ &= |d| \cdot \Delta\cos\theta_{spau} + n^{ij}_{spau}\lambda \end{aligned} \tag{13}$$

where θ_{spj} and θ_j are the DOAs of spoofing signal and real signal respectively. $\Delta\cos\theta_{spau}$ is the cosine difference of DOAs between the spooning signal and the real signal. It is obvious to see that $\Delta\varphi^{ij}_{spau}$ is positively correlated with d and $\Delta\cos\theta_{spau}$ from (13). As mentioned above, ΔX_{BA} is positively correlated with $\Delta\varphi^{ij}_{spau}$ and *SSE* test metric is the statistic of ΔX_{BA}. We can come to the conclusion that *SSE* test metric is positively correlated with d and $\Delta\cos\theta_{spau}$. The probability density functions (pdfs) of *SSE* test metric for the H_0 and H_1 hypotheses are shown in Fig. 2 by using Monte Carlo simulations.

We can clearly see that the H_0 hypothesis shown by blue lines in Fig. 2 perfectly follows $\chi^2(3)$ shown by red lines under any lengths of baseline vector. The *SSE* test metric for H_1 shown by gray lines significantly deviates from H_0, and is positively correlated with d and $\Delta\cos\theta_{spau}$, which is consistent with the results mentioned above. According to the Newman-Pearson criterion, we can set an appropriate threshold to effectively detect spoofing signals under a certain false alarm rate [27]. The receiver operating characteristic (ROC) curves under different parameters are shown in Fig. 3. It can be seen that as d and $\Delta\cos\theta_{spau}$ increase, the performance of spoofing detection improves. When $d = 5\lambda$ and $\Delta\cos\theta_{spau} = 0.10$, the ROC curve is very close to the theoretical performance boundary.

C. BASELINE VECTOR DIRECTION IS UNKNOWN

In the discussion above, we assume that b_{BA} is known. However, it is actually unknown since the IMU is not adopted to obtain the attitude information of the antennas in this system. Therefore, we need to estimate the unknown b_{BA}.

We mark b'_{BA} as the estimated value of b_{BA}. It can be iteratively calculated form iterative equation as the following form:

$$b'_{n+1} = b'_n + \delta_{Xn} \tag{14}$$

where $b'_{n+1} = [\Delta x_{n+1}, \Delta y_{n+1}, \Delta z_{n+1}]^T$, $b'_n = [\Delta x_n, \Delta y_n, \Delta z_n]^T$, $\delta_{Xn} = [\delta_{xn}, \delta_{yn}, \delta_{zn}]^T$, and then d can be expressed as:

$$\begin{aligned} d &= \sqrt{\Delta x^2_{n+1} + \Delta y^2_{n+1} + \Delta z^2_{n+1}} \\ &= \sqrt{(\Delta x_n + \delta_x)^2 + (\Delta y_n + \delta_y)^2 + (\Delta z_n + \delta_z)^2} \end{aligned} \tag{15}$$

We make use of the first order Taylor expansion to linearize (15) as follows:

$$d = \sqrt{\Delta x^2_n + \Delta y^2_n + \Delta z^2_n} + l_{Xn}\delta_{Xn} \tag{16}$$

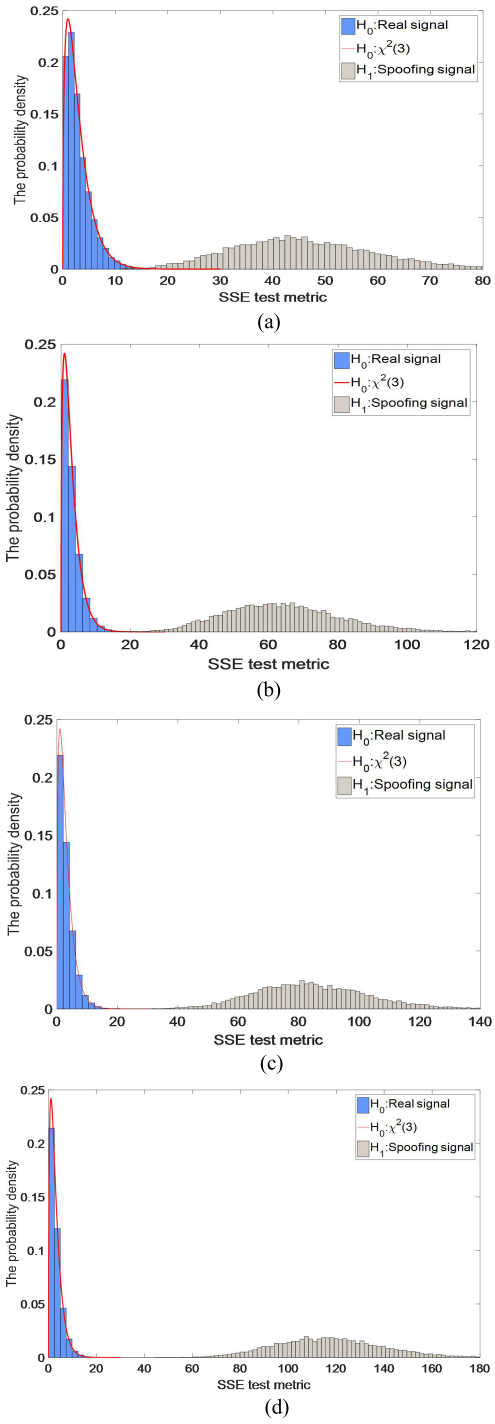


FIGURE 2. Pdfs of *SSE* test metric for H_0 and H_1 hypotheses. (a) $d = 4\lambda$, $\Delta\cos\theta_{spau} = 0.06$. (b) $d = 4\lambda$, $\Delta\cos\theta_{spau} = 0.10$. (c) $d = 5\lambda$, $\Delta\cos\theta_{spau} = 0.06$. (d) $d = 5\lambda$, $\Delta\cos\theta_{spau} = 0.10$.

where $l_{Xn} = [l_{xn}, l_{yn}, l_{zn}]^T$, $l_{xn} = \Delta x_n / \sqrt{\Delta x_n^2 + \Delta y_n^2 + \Delta z_n^2}$, $l_{yn} = \Delta y_n / \sqrt{\Delta x_n^2 + \Delta y_n^2 + \Delta z_n^2}$, $l_{zn} = \Delta z_n / \sqrt{\Delta x_n^2 + \Delta y_n^2 + \Delta z_n^2}$.

Eq. (5) is plugged into (14), and we solve it with (16) simultaneously as the following form:

$$\begin{cases} d = \sqrt{\Delta x_n^2 + \Delta y_n^2 + \Delta z_n^2} + l_{Xn}\delta_{Xn} \\ \Delta X_n + \delta_{Xn} = (H^T H)^{-1} H^T \Delta\varphi_{BA}\lambda \end{cases} \tag{17}$$

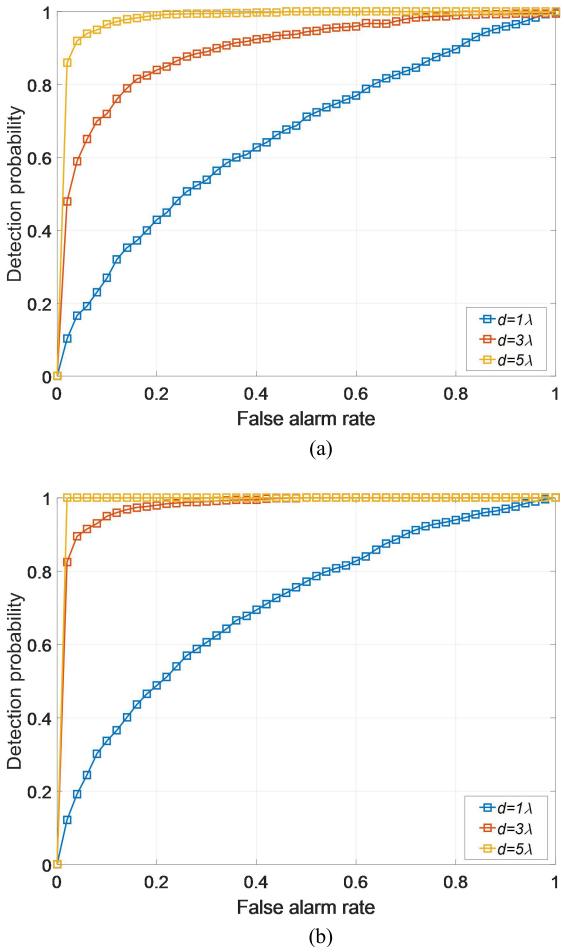


FIGURE 3. The ROC curves under different parameters. (a) $\Delta\cos\theta_{spau} = 0.06$. (b) $\Delta\cos\theta_{spau} = 0.10$.

δ_{Xn} can be obtained by employing the least squares method. The result calculated by (5) is taken as the initial value of (14). The stable value after several iterations is b'_{BA}, it is an approximation of b_{BA}. The recalculated pdfs of *SSE* test metric by employing b'_{BA} are shown in Fig. 4.

The recalculated pdfs of H_0 and H_1 are shown by the blue lines and gray lines in Fig.4 respectively. It is clear to see that the pdfs of H_0 deviate slightly from $\chi^2(3)$ shown by red lines since b'_{BA} is the estimated value of b_{BA}. The R-squared and F-test statistics between H_0 hypothesis and $\chi^2(3)$ are shown in Table 1.

We usually apply R-squared statistic to evaluate the degree of fitting. The closer R-squared is to 1, the better the statistical model fits the data and the stronger ability of model interpretation is. The R-squared in Table 1 is quite close to 1 under any lengths of baseline vector. On the other hand, the effect of F-test is to evaluate whether the variances of two samples are coincident. We can know through the table look-up method that there is a high correlation between the H_0 hypothesis and $\chi^2(3)$ under any lengths of baseline vector. Therefore, $\chi^2(3)$ is a valid approximation for the H_0 hypothesis. We can still effectively detect spoofing signals by setting a reasonable threshold.

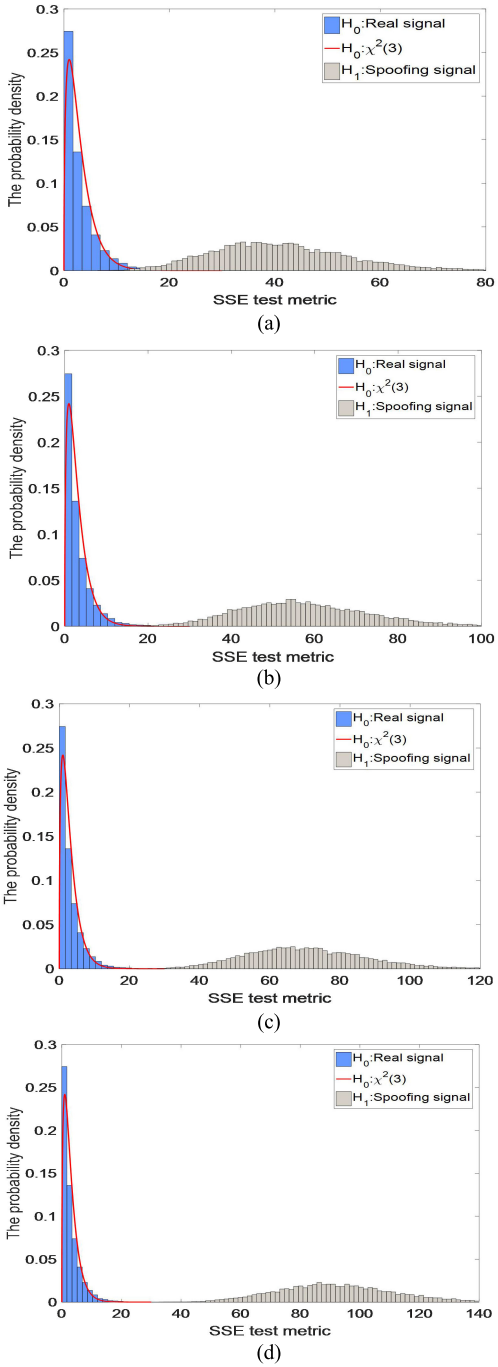


FIGURE 4. Recalculated pdfs of *SSE* test metric for H_0 and H_1 hypotheses. (a) $d = 4\lambda$, $\Delta\cos\theta_{spau} = 0.06$. (b) $d = 4\lambda$, $\Delta\cos\theta_{spau} = 0.10$. (c) $d = 5\lambda$, $\Delta\cos\theta_{spau} = 0.06$. (d) $d = 5\lambda$, $\Delta\cos\theta_{spau} = 0.10$.

III. FALSE ALARM PERFORMANCE

The two antennas spoofing detection system is installed at the roof of aerospace information research institute in Beijing for assessing the false alarm performance of the method proposed in this paper, as shown in Fig. 5. The receivers used in this experiment are the packaged Ublox Neo-M8n modules. The laptop running the software of spoofing detection serves as the signal processing unit of the system. The receivers accept

TABLE 1. R-squared and F-test statistics.

d	R-squared	F-test
2λ	0.887	1.041
4λ	0.886	1.065
6λ	0.875	1.060
8λ	0.879	1.062
10λ	0.881	1.056

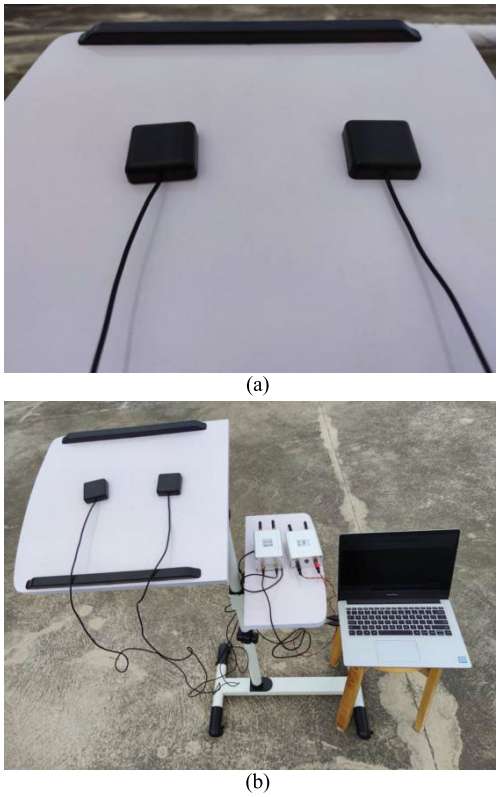


FIGURE 5. The spoofing detection system. (a) The two antennas of GNSS spoofing detection system installed on the same plane. (b) The receivers and signal processing unit of spoofing detection system.

non-spoofing GNSS signals and send them to the laptop to estimate the baseline vector and corresponding *SSE* test metric. The results of spoofing detection and positioning are given by the laptop in real time.

The representative results for the estimated antenna baseline vector are shown in Fig. 6. The observation time of each group is about 11 minutes. The baseline length of the two sets is 2λ and 4λ respectively. The observed data of baseline vector ΔX_{BA} shown by the blue curve follow the normal distribution since the existence of AWGN. This is consistent with the conclusion mentioned above in Section II. At the same time, the corrected data b'_{BA} shown by the red curve are obviously smoother than observed data and closer to the real value.

The mean and standard deviation of the observed and corrected data are given in Table 2. We can readily see that

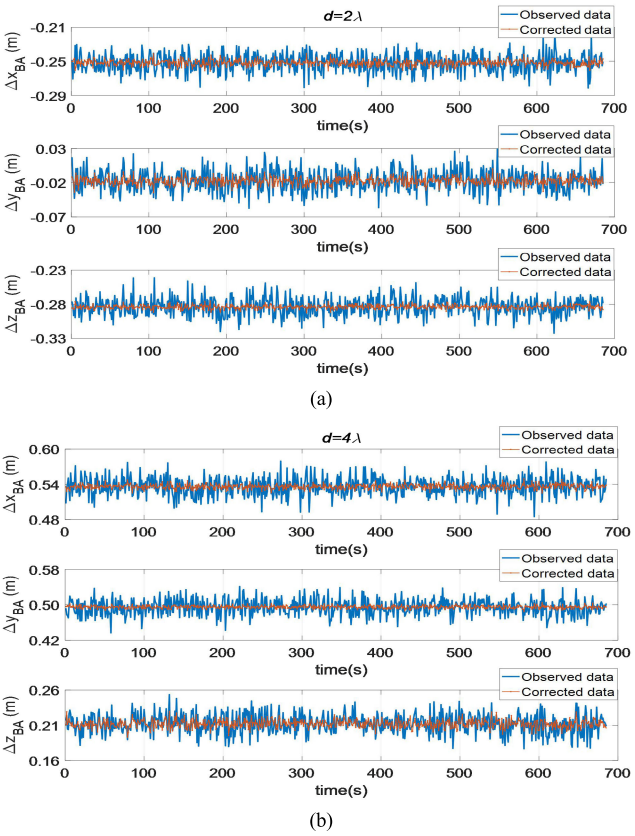


FIGURE 6. The observed and corrected data of the baseline vector. (a) $d = 2\lambda$, $b_{BA} = [-0.252\text{m}, -0.017\text{m}, -0.284\text{m}]^T$. (b) $d = 4\lambda$, $b_{BA} = [0.536\text{m}, 0.495\text{m}, 0.212\text{m}]^T$.

TABLE 2. The mean and standard deviation of the observed and corrected data.

d	Situation	Parameter	Δx_{BA}	Δy_{BA}	Δz_{BA}
2λ	observed	mean (m)	-0.250	-0.017	-0.283
		std (m)	0.011	0.015	0.013
	corrected	mean (m)	-0.252	-0.018	-0.284
		std (m)	0.004	0.006	0.003
4λ	observed	mean (m)	0.535	0.496	0.210
		std (m)	0.015	0.018	0.014
	corrected	mean (m)	0.536	0.496	0.212
		std (m)	0.004	0.003	0.006

the mean of corrected data is quite close to the real value, and the standard deviation of the corrected data is obviously smaller than the observed data. Therefore, it is an effective statistical estimation method to employ the corrected data as the approximation of the real baseline vector.

We set an appropriate threshold $SSE_{th} = 30$ based on the cumulative distribution function (CDF) of the $\chi^2(3)$, and the corresponding theoretical false alarm rate is 1.38×10^{-6}. We define two satellite signal status tags. We mark it as "real" when the *SSE* test metric is smaller than SSE_{th}, indicating that the currently received satellite signals are all non-spoofing. Otherwise we mark it as "spoofing", indicating that at least one spoofing signal is existing. The *SSE* test metric is shown in Fig. 7. The status tags are all "real" since the system receives real signals during the whole experiment period, and the false alarm rate is zero.

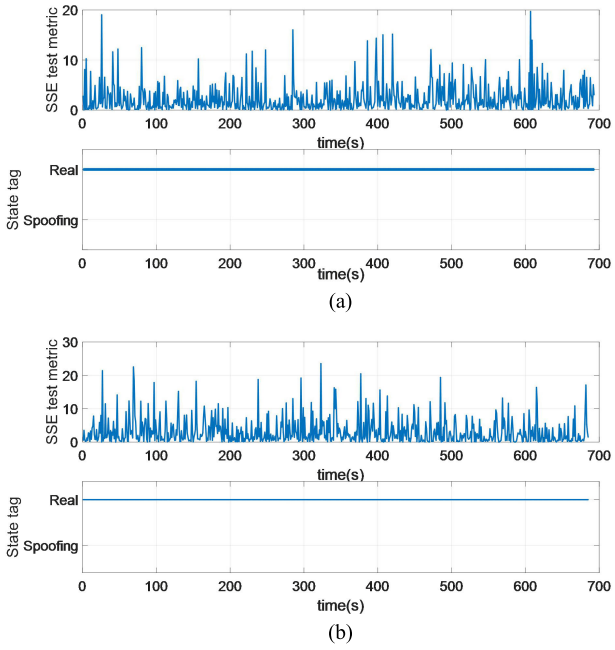


FIGURE 7. The *SSE* test metric and status tags of real signals. (a) $d = 2\lambda$. (b) $d = 4\lambda$.

IV. DETECTION PERFORMANCE

A. STATIC SCENARIO WITH ONE SPOOFING SOURCE

The estimated baseline vector of static scenario with one spoofing source is shown in Fig. 8. We employ a GNSS signal re-transmitter as the source of meaconing attack to interfere with one GNSS signal. To ensure that the receiver can successfully trace the spoofing signal, we use a low-noise amplifier to properly amplify the signal. At the same time, the amplifier power should be as low as possible in order to avoid possible interferences with the other actual GNSS signals.

The test time of each set is 180s. We turn on the re-transmitter at 30s and turn off it at 150s. The baseline length of the two sets is 2λ and 4λ respectively. When the re-transmitter is in the off state at 0-30s and 150s-180s, the observed data of the baseline vector follow the normal distribution. The receivers immediately trace the spoofing signal as the power of the spoofing signal is greater than the real signal when the re-transmitter is turned on at 30s. The observed data deviate significantly as shown by the blue curve from 30s to 150s. The corrected data shown by the red curve are quite close to the real value and fluctuates very little in this scenario.

The results calculated for *SSE* test metric and status tags are shown in Fig. 9. The *SSE* test metric increases sharply without any delay when the re-transmitter starts to work at 30s. The

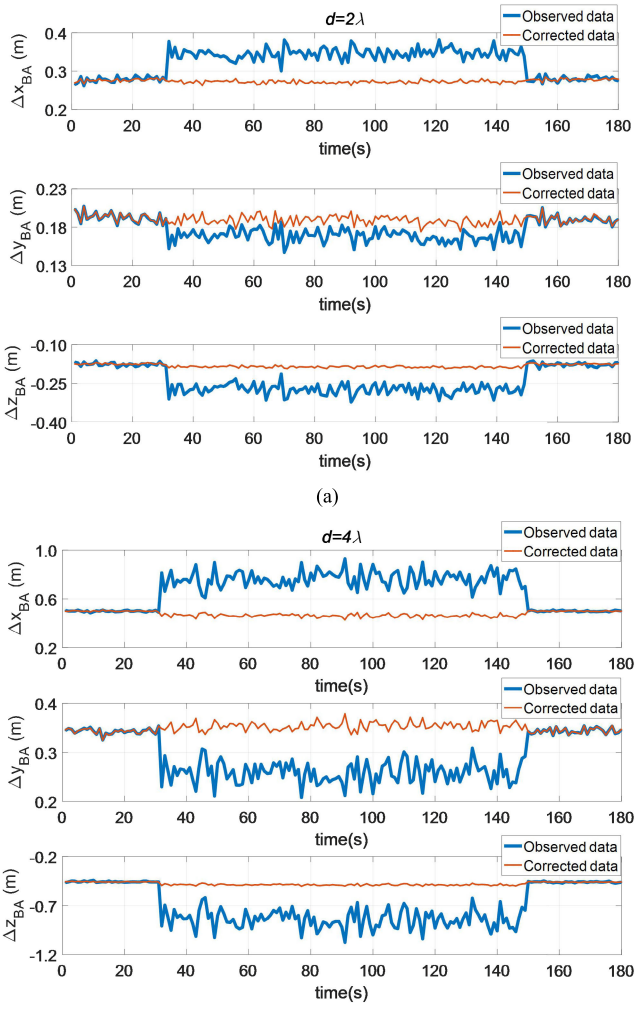


FIGURE 8. The estimated baseline vector in the static scenario. (a) $d = 2\lambda$. (b) $d = 4\lambda$.

SSE test metric is greater than the threshold from 30s to 150s except at 69s in Fig. 9 (a), and the detection probability $P_{D1} = 99.2\%$. The *SSE* test metric is much greater than the threshold and the status tags are marked as "spoofing" from 30s to 150s in Fig. 9 (b), and the detection probability $P_{D2} = 100\%$. This indicates that as the length of the baseline vector increases, the detection probability of the system increases.

In this static scenario, the maximum of *SSE* test metric with baseline length of 2λ is 583, whereas the maximum of *SSE* test metric with baseline length of 4λ is up to 1274. This indicates that as the baseline length increases, so does the *SSE* test metric. The *SSE* test metric is positively correlated with baseline length d, which consistent with the results discussed in Section II (see Fig. 4).

A typical set of positioning estimation by the receiver is shown in Fig. 10. The receiver traces 7 GPS satellite signals simultaneously in this static scenario. The re-transmitter interferes with one GNSS signal immediately and have a certain impact on the positioning results by the receiver when it is turned on at 30s. The maximum positioning error has reached to 0.21 meters at 93s.

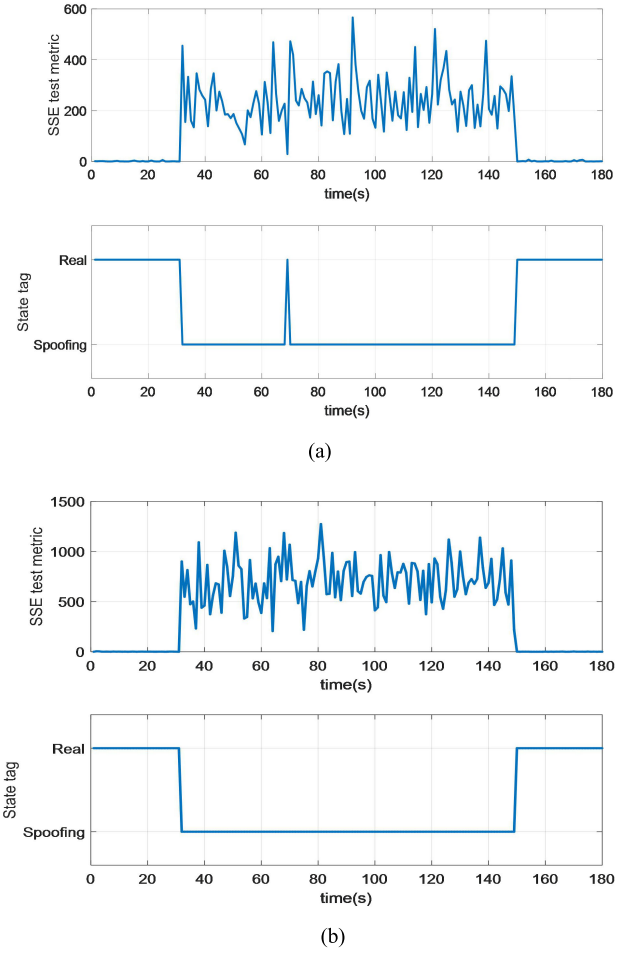


FIGURE 9. The *SSE* test metric and status tags in the static scenario with one spoofing source. (a) $d = 2\lambda$. (b) $d = 4\lambda$.

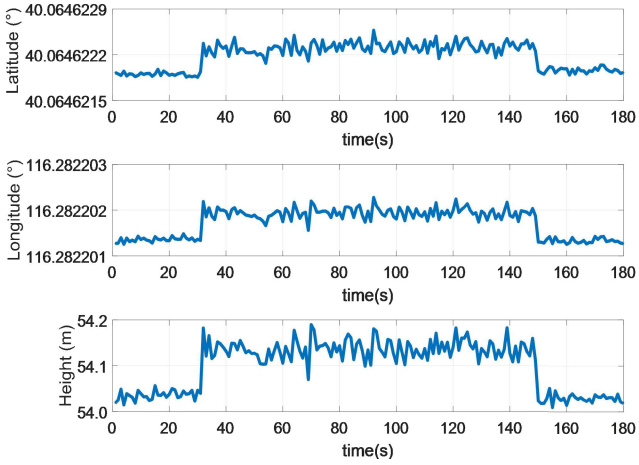


FIGURE 10. Positioning estimation by the receiver in the static scenario with one spoofing source.

B. STATIC SCENARIO WITH TWO SPOOFING SOURCES

In this scenario, we employ two GNSS signal re-transmitters to interfere with two signals from different directions, respectively. The *SSE* test metric and status tags are shown in Fig. 11 (a). The positioning estimation by the receiver

is shown in Fig. 11 (b). The test time is still 180s and the baseline length is 4λ.

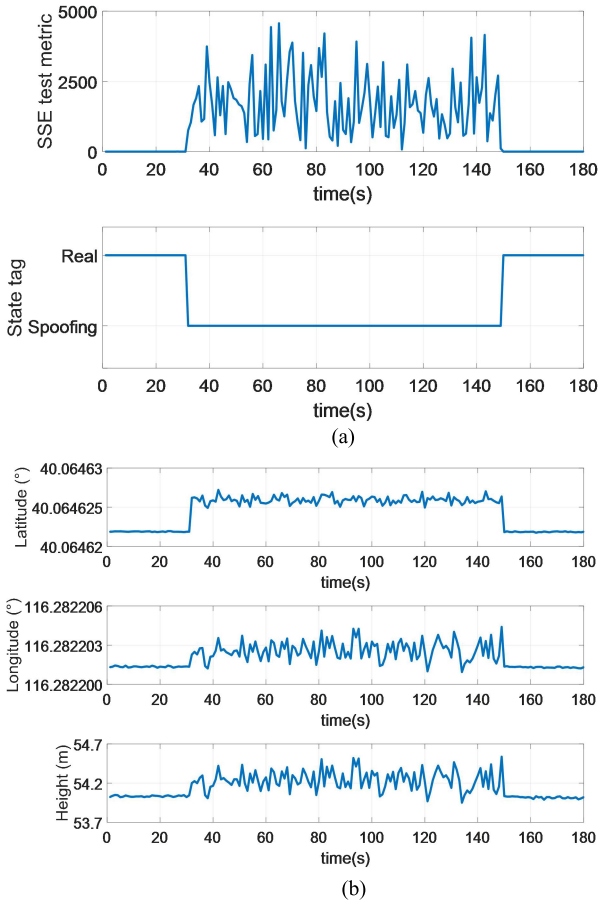


FIGURE 11. Static scenario test results with two spoofing sources. (a) The *SSE* test metric and status tags. (b) Positioning estimation by the receiver.

The maximum of *SSE* test metric is 4565 in this scenario, which is much greater than that in Fig. 9 and the detection probability $P_{D3} = 100\%$. Compared with the traditional method which can only detect the spoofing signals from the same direction [28], this system can effectively detect the spoofing signals from multiple directions. With the increase of the number of spoofing signals, the *SSE* test metric also significantly rises. On the other hand, the maximum positioning error in Fig. 11 (b) has reached to 0.76 meters at 149s. Compared with Fig. 10, it is clear to see that the positioning error increases significantly when multiple signals are spoofing.

C. DYNAMIC SCENARIO

In the dynamic test scenario, the antenna of the GNSS re-transmitter is fixed on a tripod, as shown in Fig. 12. We install the two antennas spoofing detection system on a movable work platform. We move the work platform to simulate the low-speed motion of users. The work platform moving linearly in the east-west direction gradually approaches the tripod and then moves away. If the power level of the re-transmitter is high enough, the receiver will only trace the spoofing signal due to the limited area of the experimental

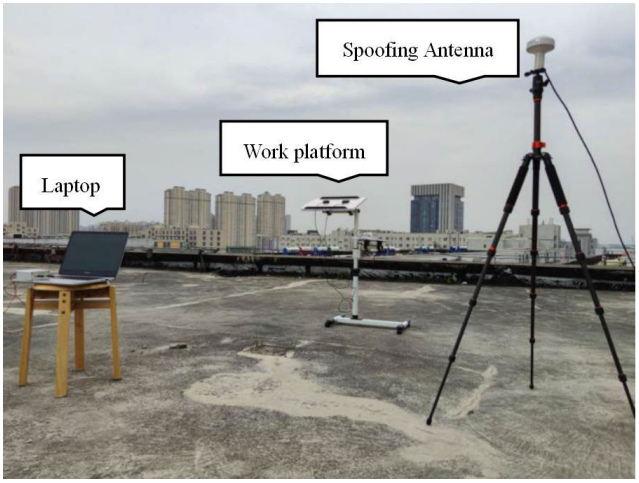


FIGURE 12. The layout of the dynamic test scenario at the rooftop of the building.

field. Therefore, the power level of the re-transmitter is turned down as much as possible and slightly higher than the real signal in order to demonstrate the whole process of the receivers being capturing the spoofing signal.

The *SSE* test metric and status tags of the dynamic scenario are shown in Fig. 13. The entire test time is 160s, and we can divide it into four stages. In the first stage, the working platform moves slowly from a distance to the re-transmitter antenna at 0-25s. The receivers trace the real GNSS signals at this time since the power of the spoofing signal is quite weak. The *SSE* test metric is obviously smaller than the threshold, and the status tags are all marked as ''real''.

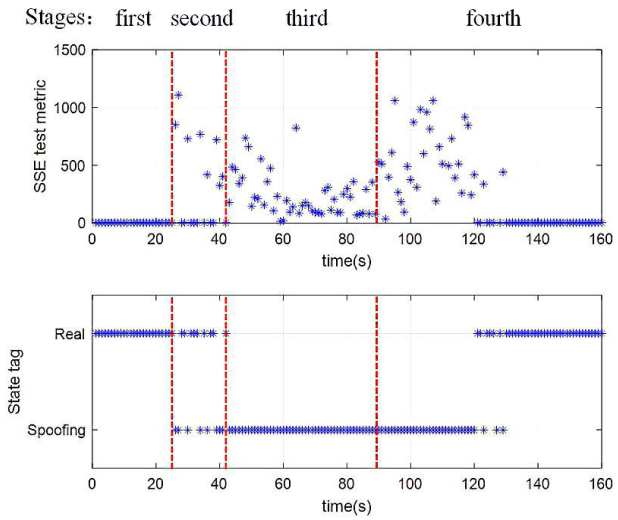


FIGURE 13. The *SSE* test metric and status tags in the dynamic scenario.

In the second stage, the working platform begins to approach the re-transmitter antenna at 26s-42s. It can be seen that the traced signals of the receivers become very unstable due to the close power of the spoofing signal and the real signal. In other words, the spoofing signal captures the tracking loops of the receivers and leads to frequent lock-lose of the receivers at this stage. The *SSE* test metric varies dramatically

and its maximum value reaches 1109 at 27s. The maximal value of the *SSE* test metric is similar with the corresponding value calculated in the static test scenario (see Fig. 9). The signal status tags swing back and forth between ''real'' and ''spoofing''.

In the third stage, the real signal is overwhelmed by the spoofing signal at 43s-89s, and the receivers trace the spoofing signal since the power of the spoofing signal is obviously greater than the real signal. In this stage, the *SSE* test metric exceeds the threshold a lot, and the signal status tags are all marked as ''spoofing''.

At the same time, it is clearly to see that the *SSE* test metric in this stage is significantly smaller than that in the second stage. The maximum of *SSE* test metric in this stage is 820 at 64s. The DOAs of the spoofing signal and the real signal are close due to the working platform approaches the re-transmitter antenna. Therefore, the cosine difference of the DOAs shows a decreasing trend, and so does the *SSE* metric. This is completely consistent with the conclusions discussed in Section II (see Fig. 4).

In the fourth stage, the working platform is moving away from the re-transmitter antenna gradually after 90s, which is the opposite of the above process, and we will not repeat it here.

The estimated results of baseline vector and positioning in the dynamic scenario are shown in Fig. 14. The variation rule of observed data shown by the blue curve is consistent with the *SSE* test metric. The observed data of baseline vector follow the normal distribution when the receivers trace the real signal at 0-25s. It begins to shift and jitter significantly as the receivers are capturing the spoofing signal step by step at 26s-42s. The remarkable bias occurs between the observed and real data of baseline vector when the receivers trace the spoofing signal at 43s-89s.

The corrected data of the baseline vector are shown by the red curve in Fig. 14. Compared with the observed data, the corrected data are quite stable and close to the real value.

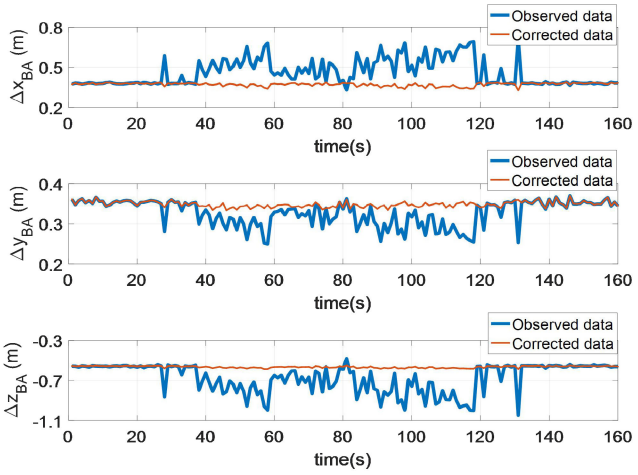


FIGURE 14. The estimated baseline vector in the dynamic scenario.

It changes very little with the generation of spoofing signals during the whole observation period.

In this test scenario, the receivers trace 8 GPS satellite signals simultaneously. The estimated results of positioning shown in Fig. 15 change slightly since the re-transmitter we used only interferes with one GPS satellite signal. The maximum positioning error is up to about 0.67 meters at 133s. Considering the current precision of single-point positioning (usually around 10 meters), it is difficult for users to judge whether there are spoofing signals by the deviation of the positioning results. Comparing Fig. 13 with Fig. 15, the *SSE* test metric is a robust anti-spoofing index of navigation signals as it is more sensitive to detect spoofing signals.

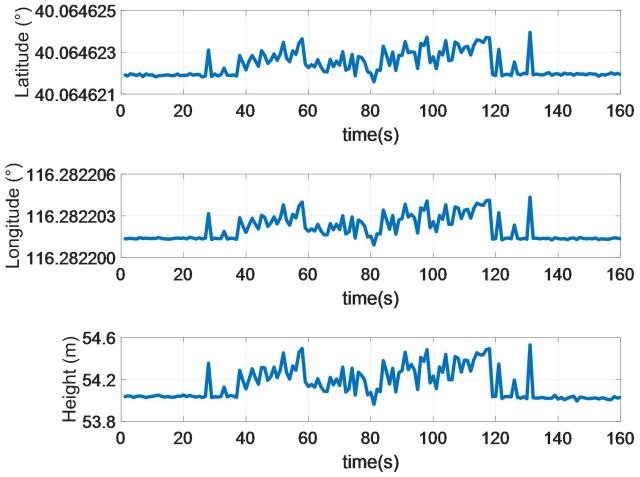


FIGURE 15. Positioning estimation by receiver in the dynamic scenario.

V. SUMMARY AND CONCLUSIONS

In this paper, we propose a new GNSS spoofing detection method using two antennas. Compared with the traditional multi-antenna spoofing detection methods, this method only needs two low-cost GNSS antennas, and does not require the IMU to provide additional attitude information. This method can detect one single spoofing signal or spoofing signals from multiple directions. In addition, we propose a method to estimate the baseline vector using the baseline vector length and carrier phase observations. The *SSE* test metric is employed to evaluate the quality of the solution. In the static scenario, the *SSE* test metric increases significantly when the spoofing signal appears. Therefore, the system is able to detect spoofing signals with near-zero false alarm rate without any delay by setting a reasonable threshold. Moreover, with the increase of baseline vector length, the detection probability of the system increases. In the dynamic scenario, the signal frequent lock-lose due to its instability. The *SSE* test metric fluctuates dramatically during the process of the receiver being gradually capturing spoofing signals. The system can still effectively detect the spoofing signal after the receiver stably trace the spoofing signal. In the future work, we will combine RAIM algorithms for joint detection in order to solve the possible instability in dynamic scenarios.

REFERENCES

[1] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. ION GNSS*, Sep. 2005, pp. 1285–1290.

[2] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, Jul. 2014.

[3] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *Navigation*, vol. 64, no. 1, pp. 51–66, Mar. 2017.

[4] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surv.*, vol. 48, no. 4, pp. 1–31, May 2016.

[5] S. Hewitson and J. Wang, "GNSS receiver autonomous integrity monitoring (RAIM) performance analysis," *GPS Solutions*, vol. 10, no. 3, pp. 155–170, Jul. 2006.

[6] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

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

[8] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," in *Proc. 5th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2010, pp. 1–6.

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

[10] C. Tanil, S. Khanafseh, and B. Pervan, "GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory," in *Proc. ION GNSS*, Tampa, FL, USA, Sep. 2015, pp. 3345–3357.

[11] L. Fu, J. Zhang, R. Li, X. Cao, and J. Wang, "Vision-aided RAIM: A new method for GPS integrity monitoring in approach and landing phase," *Sensors*, vol. 15, no. 9, pp. 22854–22873, Sep. 2015.

[12] J. Liu, B. Cai, D. Lu, and J. Wang, "An enhanced RAIM method for satellite-based positioning using track constraint," *IEEE Access*, vol. 7, pp. 54390–54409, 2019.

[13] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements," *Int. J. Satell. Commun. Netw.*, vol. 30, no. 4, p. 181191, Jul./Aug. 2012.

[14] B. W. O'Hanlon and M. L. Psiaki, "Real-time spoofing detection using correlation between two civil GPS receiver," in *Proc. ION GNSS*, Nashville, TN, USA, Sep. 2012, pp. 3584–3590.

[15] S. Han, D. Luo, W. Meng, and C. Li, "Antispoofing RAIM for dual-recursion particle filter of GNSS calculation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 52, no. 2, pp. 836–851, Apr. 2016.

[16] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," *Proc. IEEE*, vol. 104, no. 6, pp. 1246–1257, Jun. 2016.

[17] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "Low-complexity spoofing mitigation," *GPS World Mag.*, vol. 22, pp. 44–46, Dec. 2011.

[18] P. F. Swaszek, R. J. Hartnett, M. V. Kempe, and G. W. Johnson, "Analysis of a simple, multi-receiver GPS spoof detector," in *Proc. ION ITM*, San Diego, CA, USA, Jan. 2013, pp. 884–892.

[19] P. F. Swaszek and R. J. Hartnett, "A multiple COTS receiver GNSS spoof detector–extensions," in *Proc. ION ITM*, San Diego, CA, USA, Jan. 2014, pp. 1–12.

[20] D. Borio and C. Gioia, "A dual-antenna spoofing detection system using GNSS commercial receivers," in *Proc. ION GNSS 28th. Int. Tech. Meeting Satell. Division*, Tampa, FL, USA, Sep. 2015, pp. 325–330.

[21] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, and T. E. Humphreys, "GNSS spoofing detection using two-antenna differential carrier phase," in *Proc. ION GNSS 27st. Int. Tech. Meeting Satell. Division*, Tampa, FL, USA, Sep. 2014, pp. 2776–2800.

[22] A. J. Jahromi, A. Broumandan, and G. Lachapelle, "GNSS signal authenticity verification using carrier phase measurements with multiple receivers," in *Proc. 8th ESA Workshop Satell. Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Noordwijk, The Netherlands, Dec. 2016, pp. 1–11.

[23] P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals, and R. J. Hartnett, "GNSS spoof detection using shipboard IMU measurements," in *Proc. ION GNSS 27th Int. Tech. Meeting Satell. Division*, Tampa, FL, USA, 2014, pp. 745–758.

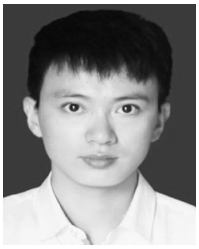
[24] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, "Performance analysis of joint multi-antenna spoofing detection and attitude estimation," in *Proc. Int. Tech. Meeting The Inst. Navigat.*, San Diego, CA, USA, Jan. 2013, pp. 864–872.

[25] P. Enge, "The global positioning system signals, measurements, and performance," *Int. J. Wireless Inf. Netw.*, vol. 1, no. 2, pp. 83–105, 1994.

[26] Z. Liu, J. Liu, W. Jiang, and T. Li, "Ambiguity resolution of double-difference GPS short-baseline using genetic algorithm," *Geomatics Inf. Sci. Wuhan Univ.*, vol. 31, no. 7, pp. 607–609, Jul. 2006.

[27] B. Parkinson and J. Spilker, *The Global Positioning System: Theory Application*. Washington, DC, USA: AIAA, 1996.

[28] F. Wang, H. Li, and M. Lu, "GNSS spoofing detection based on unsynchronized double-antenna measurements," *IEEE Access*, vol. 6, pp. 31203–31212, 2018.



JIAJIA CHEN received the B.S. degree in electronic and information engineering from Nantong University, Nantong, China, in 2012, and the M.S. degree in electronic and communication engineering from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2015. He is currently pursuing the Ph.D. degree with the School of Electronic, Electrical, and Communicating Engineering, University of Chinese Academy of Sciences, Beijing, China. His current research interests include security of GNSS and multipath mitigation.

YING XU received the Ph.D. degree in signal processing from the Beijing Institute of Technology, China, in 2009. She is currently a Research Professor, a Ph.D. Supervisor, and the Vice Director of the Navigation Technology Research Laboratory, Academy of Opto-Electronics, Chinese Academy of Sciences. Her research interests include satellite navigation technology and its augmentation technology, and multi-source fusion localization theory and methods.

HONG YUAN received the M.S. and Ph.D. degrees from the Shaanxi Astronomy Observatory, Shaanxi, China, in 1995. From 1995 to 2004, he has worked with the Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences. Since 2004, he has been working with the Academy of Opto-Electronics, Chinese Academy of Sciences. He is the author of more than 60 articles and more than 30 inventions. His research interests include satellite navigation, ionospheric sounding, and ionospheric wave propagation.

YIGE YUAN received the B.S. degree in information security from Xidian University, Shaanxi, China, in 2020. She is currently pursuing the Ph.D. degree with the School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing, China. Her research interest includes security of GNSS.