Analysis of Positioning Performance of the GNSS Receiver Under Complete and Incomplete Spoofing

Ya Qi, Rui Xu, Jianye Liu and Weihao Dai

Abstract The GNSS receiver is susceptible to malicious spoofing attack and further estimates a wrong position which is considered as an arbitrary preset site from the spoofer. However, when the target receiver is far away from the spoofer, authentic signals are weak rather than submerged by spoofing signals and some authentic satellite signals are survival due to satellite geometry. In this case, the spoofing attack is incomplete and its effects on the positioning estimation of target receivers become complex. In this study, an improved transmitter-based spoofer is realized employing the software-defined receiver and used to analyze the positioning performance of the target receiver under the complete and incomplete spoofing attack. Simulation results show that the target receiver is possibly controlled by the spoofer under complete spoofing attack and its estimated position is equal to the spoofer preset position. Under incomplete spoofing, the estimated position is between the preset position and the genuine position, but is neither.

Keywords GNSS · Software-defined receiver · Spoofing attack
Transmitter-based spoofer · Positioning performance

1 Introduction

Global Navigation Satellite Systems (GNSS) like GPS and Beidou are widely applied in many fields of civilian and military [1]. Unfortunately, the power level of GNSS signal received by ground receivers is extremely low due to the large

Y. Qi · R. Xu (✉) · J. Liu · W. Dai
Navigation Research Centre, Nanjing University of Aeronautics
and Astronautics, Nanjing, China
e-mail: ruixu@nuaa.edu.cn

Y. Qi
e-mail: nuaaqiya@nuaa.edu.cn

Y. Qi · R. Xu · J. Liu · W. Dai
Satellite Communication and Navigation Collaborative Innovation Center, Nanjing, China

J. Sun et al. (eds.), *China Satellite Navigation Conference (CSNC) 2018 Proceedings*, Lecture Notes in Electrical Engineering 498,
https://doi.org/10.1007/978-981-13-0014-1_13

distances between the satellites and the receiver, and finally causes the signals highly vulnerable to interference under complex electromagnetic environment [2, 3].

Spoofing attack is one of the interference and can be divided into generated spoofing and transmitter/repeater spoofing. Due to low-cost and simple implementation, repeater spoofing is carried out in many important researches on spoofing countermeasures over the last decade [4, 5]. Through controlling the time offsets, Doppler frequency offsets and signal power of spoofing signals, the spoofer can perform an aggressive spoofing attack with the help of the techniques, software [6, 7] and hardware tools [8, 9]. Generally, the majority of repeater spoofers emit their received authentic signals with a certain time delay (referring to pseudorange) [10]. As the result, the spoofer simply deceives the target receiver estimating its position near to the transmitter rather than an arbitrary preset position [11, 12]. When the time delays of different signals are controlled and different, the spoofer is able to deceive the target receiver estimating its position to an arbitrary preset site [13, 14].

However, when the target receiver is far away from the spoofer, the spoofing signal power is not strong enough to suppress all the authentic signals and part of authentic satellite signals can also be received by the receiver. In such situation, the spoofing signals are unable to cover all the received authentic signals, the spoofing is incomplete. To analyze the incomplete spoofing effects on positioning performance of the GNSS receiver, a repeater spoofer based on GNSS Software-Defined Receiver (SDR) is constructed in this paper by varying the time delay and signal strength of each satellite spoofing signal. The remainder of this paper consists of four sections. Section 2 presents the influence of complete and incomplete spoofing. Section 3 presents the implementation of repeater spoofing. Section 4 presents the experiments for testing the positioning performance of the GNSS receiver under incomplete spoofing. Finally, conclusions are given in Sect. 5.

2 Repeater Spoofing System

2.1 Signal Model Under Complete and Incomplete Spoofing Attack

Under spoofing attack, the signal s received by the target receiver can be considered as mixed signals of the authentic signals s_{au} from N satellites and the spoofing signals s_{sp} referring to M satellites, as well as noise ε, which is written as:

$$s = s_{au} + s_{sp} + \varepsilon = \sum_{i=1}^{N} s_{au}^{i} + \sum_{j=1}^{M} s_{sp}^{j} + \varepsilon \tag{1}$$

Generally, the spoofing signals are GNSS-like signals, with the same signal structure to the authentic GNSS signals. For example, the GPS L1 signals are composed by 1.023 MHz C/A code, 1575.42 MHz carrier wave and 50 Hz navigation data. The model of the received signal from one satellite is written as:

$$s_{au}^{i} = \sqrt{2P_{au}^{i}}\left[C_{au}^{i}\left(t-\tau^{i}\right)D_{au}^{i}\left(t-\tau^{i}\right)\right]\sin\left(2\pi f_{au}^{i}t+\theta_{au}^{i}\right) \tag{2}$$

where, the superscript i represents the i-th satellite, the subscript au represents the authentic signal while the spoofing signal is denoted by the subscript sp in (3), P_{au}^{i} is the average power, $C_{au}^{i}(\cdot)$ is the C/A code and τ^{i} is the time delay which equals the propagation time of the signal from the satellite to the receiver, $D_{au}^{i}(\cdot)$ is the navigation data, the item of $\sin\left(2\pi f_{au}^{i}t+\theta_{au}^{i}\right)$ is the carrier wave, and f_{au}^{i} is the carrier frequency including the Doppler frequency.

Similarly, the spoofing signals can be expressed as:

$$s_{sp}^{j} = \sqrt{2P_{sp}^{j}}\left[C_{sp}^{j}\left(t-\tau^{j}+\tau_{sp}^{j}\right)D_{sp}^{j}\left(t-\tau^{j}+\tau_{sp}^{j}\right)\right]\sin\left(2\pi f_{sp}^{j}t+\theta_{sp}^{j}\right) \tag{3}$$

where, P_{sp}^{j} and $C_{sp}^{j}(\cdot)$ are the average power and the C/A code of spoofing signals. Nominally, the spoofed signals have the same C/A code sequence $C_{sp}^{j}(\cdot)=C_{au}^{j}(\cdot)$ as the corresponding authentic signals, but with an additional time delay τ_{sp}^{j} which is set according to the spoofing requirement such as the artificial spoofing position. The navigation data $D_{sp}^{j}(\cdot)$ of the spoofing signals is same to that of the corresponding authentic signals for the transmitter-based spoofing and different for the generator-based spoofing. For the spoofing carrier $\sin\left(2\pi f_{sp}^{j}t+\theta_{sp}^{j}\right)$, the frequency is usually same to the authentic frequency or match to the variation of code time delay. For focusing on the position estimation performance of the target receiver, the carrier wave of spoofing signals, in this study, are simplified as the same as authentic signals, that is $f_{sp}^{j}=f_{au}^{j}$ and $\theta_{sp}^{j}=\theta_{au}^{j}$.

An powerful spoofer is considered to control the target receiver completely. In such case, $P_{sp} \gg P_{au}$ and $M \geq N$, the authentic signals vanish in the received signals and the signal model can be shorten as

$$s = \sum_{j=1}^{M} s_{sp}^{j} + \varepsilon \tag{4}$$

In practice, the spoofer is commonly fixed in the ground and its signals are attenuated gradually during the propagation to a long-distance target receiver. In this case, the authentic signal is weak but not totally suppressed, $P_{sp} \approx P_{au}$. On the other hand, long distance possible leads to different satellite geometry, and hence different satellites observed by the target receiver, $M < N$. The two incomplete spoofing situations cause that the target receiver collects authentic and spoofing signals simultaneously and the effects of the authentic signals cannot be ignored. The signal model under incomplete spoofing attack is same to (1).

- Situation 1: $P_{sp} \approx P_{au}$

When spoofing signal power is not strong enough, $P_{sp} \approx P_{au}$, it is obvious that the spoofing signal still has influence on the target receiver operating in tracking, and an illustration of complete and incomplete spoofing attack is given in Fig. 1.

When the spoofing signal power is much larger than the authentic signal power, as shown in Fig. 1 (upper), the spoofer will drag the correlation peak away from the genuine peak to the counterfeit peak when the spoofing occurs. The estimating error τ'_{sp} equals to preset time delay τ_{sp}, which is the signal delay of the spoofing signal. The correlation peak calculated from the value of non-coherent integration is influenced by the signal power. For lower spoofing signal power, as shown in Fig. 1 (bottom), the spoofing signals are no longer dominant in the tracking loop, and the correlation curve of received signals, which is the combination peak in Fig. 1 (bottom), will be bilaterally asymmetric. In this case, the phase detector of code tracking loop will adjust code phase to correct the output of correlation, and the introduced estimating error τ'_{sp} is smaller than the preset time delay τ_{sp}.

- Situation 2: $M < N$

When the satellite geometry received by the target receiver changes, the positioning performance will vary accordingly. Assuming that several satellite signals from a certain region are attacked by spoofing signals, the estimated position of the target receiver will deviate from the authentic site. According to the principle of three-sphere intersection measurement as shown in Fig. 2, the influence in the line between the target receiver and the area where satellite signals are deceived is the most obvious. When the preset signal delays lag behind the authentic signals, $\tau_{sp} > 0$, the estimated position will shift to the opposite direction of the area where the satellite signals are spoofed. The relation between the preset signal delay τ_{sp} and the offset distance is nonlinear, which needs further research in the future.

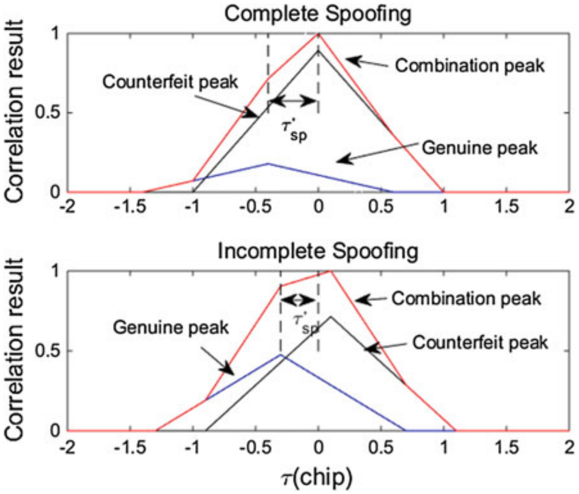


Fig. 1 Correlation results under complete spoofing (upper) and incomplete spoofing (bottom) attacks

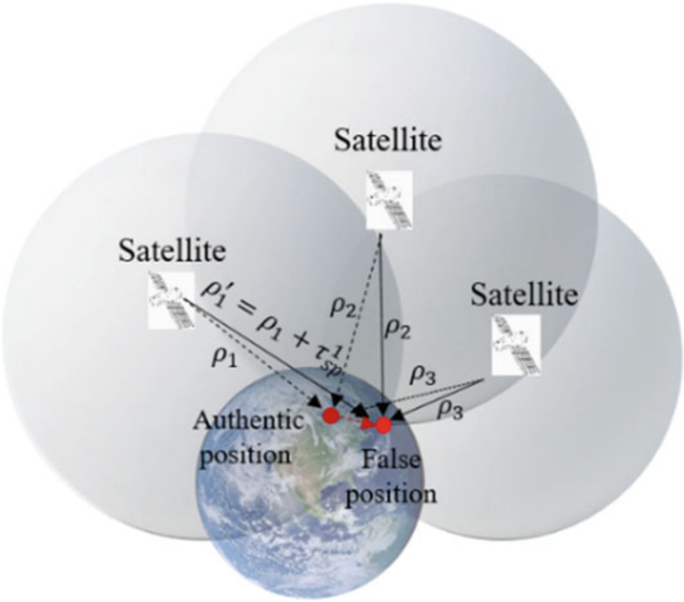


Fig. 2 The illustration of three-sphere intersection measurement of the incomplete spoofing

2.2 Positioning Model Under Spoofing Environment

The GNSS receiver obtains the pseudoranges between the receiver and satellites and then estimates the position with at least four pseudoranges. The pseudorange of the i-th authentic GNSS signal ρ_i^{au} can be expressed as:

$$\rho_i^{au} = r_i + \delta t_u + \varepsilon_p \tag{5}$$

$$r_i = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} \tag{6}$$

where, r_i is the distance between the receiver and the i-th satellite, δt_u is the clock error of the receiver, which is related to the GNSS receiver clock, ε_p is the sum of other errors. x_j, y_j, z_j $(j = 1, 2, 3, 4\ldots)$ and x, y, z represent the coordinates of the i-th satellite and the receiver under Earth Center Fixed coordinate system. The j-th spoofing GNSS signal ρ_j^{sp} has the same pseudorange model as the authentic signal:

$$\rho_j^{sp} = \rho_j^{au} + \tau_{sp}^j + \varepsilon_j = r_j + \delta t_u + \tau_{sp}^j + \varepsilon_j' \tag{7}$$

where, τ_{sp}^j is the product of the preset time offset τ_{sp} and the speed of light c $\left(\tau_{sp}^j = \tau_{sp} \times c\right)$, ε_j is the noise produced by the spoofer.

For complete spoofing, all the authentic signals are submerged by spoofing signals. The positioning equations can be expressed as:

$$\begin{cases} \rho_1 = \rho_1^{sp} = r_1 + \delta t_u + \tau_{sp}^1 + \varepsilon_1' \\ \qquad\qquad \vdots \\ \rho_M = \rho_M^{sp} = r_M + \delta t_u + \tau_{sp}^M + \varepsilon_M' \end{cases} \tag{8}$$

Under complete spoofing, when all the spoofing signals have the same preset time delay $\tau_{sp}^j = \tau_{sp}$, the common time delay τ_{sp} can be viewed as the clock error increment of the target receiver, $\delta t_u' = (\delta t_u + \tau_{sp})$, and the preset site of the spoofer can only be the position of the transmitter. When time delays vary from spoofing signals, theoretically, the spoofer can drag the target receiver to any excepted location through the control of preset time delay τ_{sp}^i.

For incomplete spoofing, the authentic signals are weak but not totally suppressed. The positioning equations can be expressed as:

$$\begin{cases} \rho_1 = \rho_1^{sp} = r_1 + \delta t_u + \tau_{sp}^1 + \varepsilon_1' \\ \qquad\qquad \vdots \\ \rho_M = \rho_M^{sp} = r_M + \delta t_u + \tau_{sp}^M + \varepsilon_M' \\ \rho_{M+1} = \rho_{M+1}^{au} = r_{M+1} + \delta t_u + \varepsilon_{M+1} \\ \qquad\qquad \vdots \\ \rho_N = \rho_N^{au} = r_N + \delta t_u + \varepsilon_N \end{cases} \tag{9}$$

In this case, the position of the target receiver is influenced by both spoofing signals and authentic signals. The effect of incomplete spoofing is analyzed in the Sect. 2.1. The change on estimated pseudoranges can be viewed as the change on distance between the receiver and the *i*-th satellite, as shown in (10), and revealed in the deviation of estimated position, as shown in (11).

$$\begin{cases} r_1' = r_1 + \tau_{sp}^1 \\ \qquad \vdots \\ r_M' = r_M + \tau_{sp}^M \\ r_{M+1}' = r_{M+1} \\ \qquad \vdots \\ r_N' = r_N \end{cases} \tag{10}$$

$$r_j' = \sqrt{(x_j - x')^2 + (y_j - y')^2 + (z_j - z')^2} \tag{11}$$

where, x', y', z' represent the coordinates of the target receiver under Earth Center Fixed coordinate system.

3 Implementation of Repeater Spoofing

The spoofer receives the GPS L1 signals, where the necessary parameters of the spoofing signals are obtained through sampling, acquisition and tracking. According to (2), the authentic satellite signals are composed by spreading code, carrier wave and navigation data, which are obtained from tracking results. Though separating and reconstructing each satellite signal, we can get a replica of the authentic signals. To affect the target receiver operating in tracking mode, the C/A code sequence, navigation data and carrier wave of spoofing signal are same to the authentic, as shown in (3), with the preset time offsets τ_{sp} reflecting in spreading code phase and signal power P_{sp} different.

Considering the possibility of incomplete spoofing, the number of spoofing signals and the spoofing signal power are under control in accordance with the requirements of tests. Through adjusting the parameters of spoofing signals, spoofing attacks are simulated to analyze the positioning performance of the target receiver under the incomplete spoofing.

4 Experiment and Analysis

4.1 Experiment Method and Environment

Data was received by the GNSS Software-Defined Receiver on the roof of No. 1 building, college of automation engineering, Nanjing University of Aeronautics and Astronautics, on September 18, 2017. The position measured by a dual-frequency commercial receiver is 118.7926358°E, 31.9388758°N, 51.82-m Height. The parameters of the target GNSS receiver are shown in the Table 1.

In the simulation, the GPS satellites are divided into four regions according to satellite distribution with the azimuth angle 0–360° at intervals of 90°, as shown in Fig. 3. The satellites respectively contained by the four regions are PRN 24 and 15 (Northeast Region—Region I), PRN 10 and 32 (Southeast Region—Region II), PRN 21 (Southwest Region—Region III), PRN 12 and 25 (Northwest Region—Region IV).

To analyze the positioning performance of GNSS receiver under the incomplete spoofing, two tests are carried out:

Table 1 The parameters of the target GNSS receiver

Sampling frequency	16.3676 MHz
Intermediate frequency	4.12397 MHz
PLL bandwidth@Integration time	10 Hz@1 ms
DLL bandwidth@Integration time	1 Hz@1 ms
Early-late chip spacing	0.5 chip

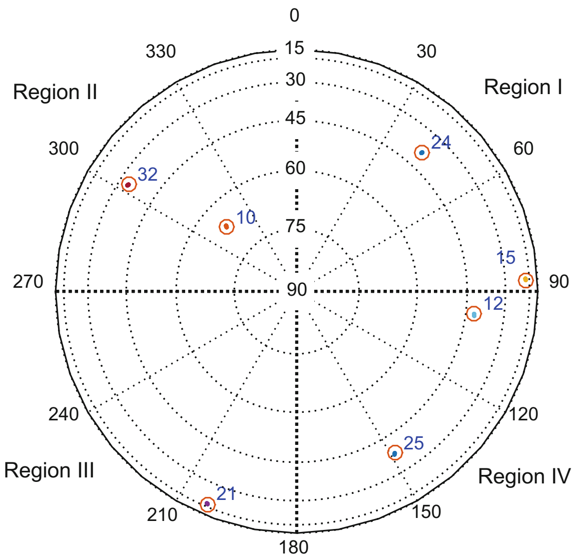


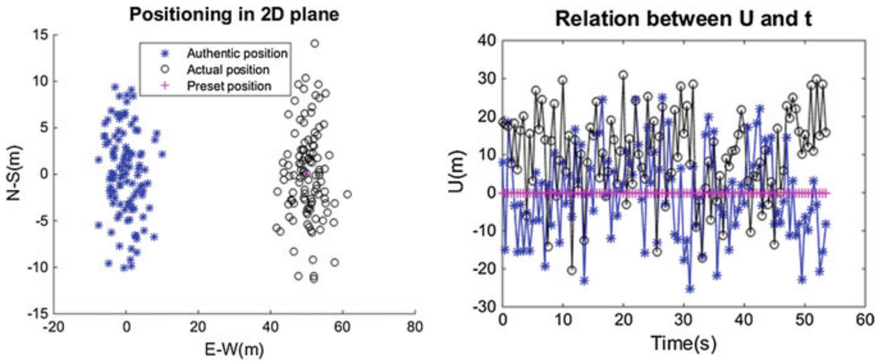
Fig. 3 Satellite spatial distribution

Test 1: The spoofing attack is complete. According the preset position (50 m away from the receiver-spoofer in the direction toward the east), the preset time delays τ_{sp}^{i} vary from different satellite signals $\left(\tau_{sp}^{i} \neq \tau_{sp}^{j}, i \neq j, i \in [1, N], j \in [1, N]\right)$. In this test, the preset time delays of PRN 24, 15, 12, 25, 21, 32, 10 are −28, −13, −18, −12, 38, 60, 50 m respectively.

Test 2: The spoofing attack is incomplete. We assume that one region of the satellite distribution is attacked by spoofing signals, and the preset time delay of spoofing signals is 50 m $\left(\tau_{sp}^{i} = 50\,\text{m}, i \in [1, M], M < N\right)$. Considering the influence of spoofing signal power, the test is divided into two cases: (a) the spoofing signal power is large enough to submerge the authentic signals $\left(P_{au} \ll P_{sp}\right)$ and (b) the spoofing signal power decays during the propagation and is similar to the authentic signal power $\left(P_{au} \approx P_{sp}\right)$.

4.2 Simulation Results and Analysis

Figure 4 shows the positioning results of target receiver under complete spoofing of Test 1. In the results, we set the authentic position of target receiver as the reference position. To a certain extent, the estimated position of target receiver is nearly same as the preset position, which is in agreement with the analysis in Sect. 2.2. In this case, the spoofing signals play a dominant role in the position and fool the target receiver to any position with suitable settings of time delay $\tau_{sp}^{i}(i \in [1, N])$.

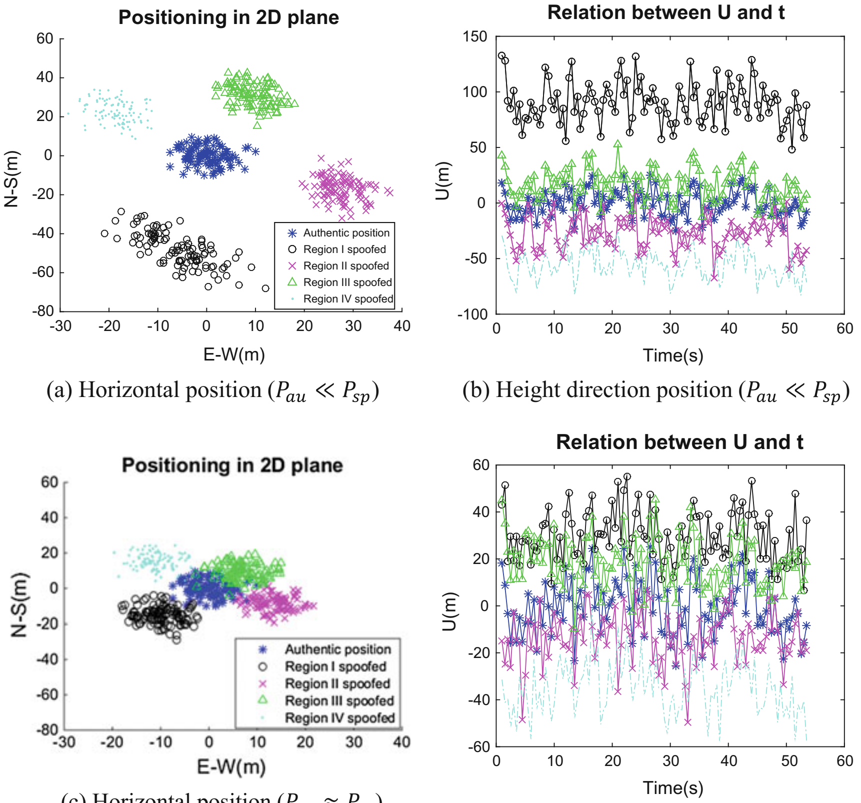


(a) Horizontal position

(b) Height direction position

Fig. 4 Positioning results of target receiver under complete spoofing

Figure 5 shows the positioning results of target receiver under incomplete spoofing of Test 2. As shown in Fig. 5a, c, the estimating error τ'_{sp} reflecting in the deviation is related to spoofing signal power. The deviations of case (b) are mostly smaller than that of case (a). Compared with complete spoofing, the incomplete spoofing with smaller spoofing power is influenced by authentic signals and the positioning deviation is smaller accordingly. Under incomplete spoofing, the estimated position deviation of target receiver is related to satellite geometry obtained by the receiver. In the horizontal direction, the estimated location of target receiver is related to the azimuth angle of spoofed satellites. For example, when the signals from satellites in the Region I (Azimuth: 0–90°) under spoofing attack, the target receiver position shifts to the Region III (Azimuth: 180–270°), and the deviations are 9.47 m and 6.63 m in the north, 30.98 m and 8.88 m in the east respectively. The offset distance depends on the time delay which is affected by the spoofing signal power and authentic signal power. However, the position of the target receiver in height direction does not show a clear regularity, as shown in Fig. 5b, d. Though experiments carried out in this paper, the analyses of the incomplete spoofing influence on the GNSS receiver in the Sect. 2 are verified.



(a) Horizontal position ($P_{au} \ll P_{sp}$)

(b) Height direction position ($P_{au} \ll P_{sp}$)

(c) Horizontal position ($P_{au} \approx P_{sp}$)

(d) Height direction position ($P_{au} \approx P_{sp}$)

Fig. 5 Positioning results of target receiver under incomplete spoofing

5 Conclusion

The GNSS repeater-based spoofer poses a greater threat to civilian receiver at present. When the site of the spoofer is far away from the target receiver, the influence of spoofing signals will be complex. In this paper, the positioning performance of a GNSS receiver under complete and incomplete spoofing are described in detail. The theoretical analyses and simulation results show the following conclusions:

(a) Complete spoofing attack, theoretically, can deceive the positioning result of the target receiver to any expected position with suitable settings of signal delays.
(b) Under incomplete spoofing attack, which revealing in the spoofing power or the coverage of signals incomplete, the existence of authentic signals has influence on the positioning results. When the spoofing power is incomplete, the actual

deviation τ'_{sp} is smaller than the preset deviation τ_{sp}; when the coverage of signals is incomplete, the actual position will shift in the line between the authentic position and the area where the spoofed satellites lie, and the deviation is related to the distance between the receiver and the satellite, the preset time delay and spoofing signal power.

Further study will consider the influence of incomplete spoofing on the spoofing process, such as the influence on code loop and tracking state.

Acknowledgements The authors are grateful for financial support from the National Natural Science Foundation of China (NSFC, www.nsfc.gov.cn) which supports this work under grant No. 61603181.

References

1. Ioannides RT, Pany T, Gibbons G (2016) Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. Proc IEEE 104(6):1174–1194
2. Motella B, Pini M, Fantino M, Mulassano P, Nicola M, Fortuny-Guasch, J et al (2011) Performance assessment of low cost GPS receivers under civilian spoofing attacks. Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, IEEE, pp 1–8
3. Haider Z, Khalid S (2017) Survey on effective GPS spoofing countermeasures. In: Sixth international conference on innovative computing technology, IEEE, pp 573–577
4. Gao Y, Li H, Lu M, Feng Z (2013) Intermediate spoofing strategies and countermeasures. Tsinghua Science and Technology 18(6):599–605
5. Bhatti J, Humphreys TE (2017) Hostile control of ships via false GPS signals: demonstration and detection. Navigation 64(1):51–66
6. Psiaki ML, Humphreys TE (2016) GNSS spoofing and detection. Proc IEEE 104(6):1258–1270
7. Huang L, Lv ZC, Wang FX (2012) Spoofing pattern research on GNSS receivers. J Astronaut 33(7):884–890
8. Shepard DP, Bhatti JA, Humphreys TE, Fansler AA (2012) Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In: ION GNSS conference, pp 3591–3605
9. Humphreys TE, Ledvina BM, Psiaki ML, O'Hanlon BW, Kintner PM (2008) Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: International technical meeting of the satellite division of the institute of navigation, pp 2314–2325
10. Broumandan A, Jafarnia-Jahromi A, Lachapelle G (2015) Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. GPS Solutions 19 (3):475–487
11. Bian S, Hu Y, Ji B (2017) Research status and prospect of GNSS anti-spoofing technology. SCIENTIA SINICA Informationis 47(3):275–287
12. Chen L, Han S, Meng W, Gong Z (2015) A spoofing mitigation algorithm based on subspace projection for GNSS receiver. In: China satellite navigation conference (CSNC) 2015 proceedings: vol I, pp 727–737. Springer, Berlin, Heidelberg
13. Huang J, Presti LL, Motella B, Pini M (2016) GNSS spoofing detection: theoretical analysis and performance of the ratio test metric in open sky. ICT Express 2(1):37–40
14. Kerns AJ, Shepard DP, Bhatti JA, Humphreys TE (2014) Unmanned aircraft capture and control via GPS spoofing. J Field Robot 31(4):617–636