Zhou et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:44
https://doi.org/10.1186/s13638-018-1048-y

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Calculation of the lower limit of the spoofing-signal ratio for a GNSS receiver-spoofer

Meng Zhou*, Hong Li and Mingquan Lu

Abstract

A receiver-spoofer is one of the most covert global navigation satellite system (GNSS) spoofing attacks and can only be effectively detected by the combination of multiple anti-spoofing technologies. In this paper, an analysis of influencing parameters for receiver-spoofers indicates that the ratio of the spoofing signal amplitude versus the authentic signal amplitude (spoofing-signal ratio) is a key parameter for spoofing results. For a spoofer to ensure covertness, the goal is to maintain a low spoofing-signal ratio. The carrier phase difference and code phase difference between authentic signals and spoofing signals resulted in errors in the position estimation of the target receiver increase the lower limit of the spoofing-signal ratio required for successful spoofing. A spoofing signal alters the phase of local replicate code based on the original balance of a receiver phase discriminator to seize control. Based on this principle, the lower limit of the spoofing-signal ratio that corresponds to various phase discriminator spacings, carrier phase differences, and code phase differences is deduced in this paper. Two tests are designed for the simulation source and authentic navigation signals to verify the deduced formula. The lower limit of the spoofing-signal ratio obtained from these tests matches the calculated results, which proves the validity and effectiveness of the derived algorithm.

Keywords: Spoofing-signal ratio, Lower limit, Carrier phase discriminator, Signal simulation

1 Introduction

A global navigation satellite system (GNSS) is a space-based radio navigation and positioning system that can provide information that can be used to derive three-dimensional coordinates, velocity, and time in all-weather conditions for users anywhere on the surface of the Earth or near-Earth space. GNSSs have been extensively employed in many areas, including precision agriculture, scientific research, environment monitoring, emergency and disaster assessment, safety assurance, positioning of celestial bodies, construction engineering and natural resources, and smart transportation. GNSSs have also created significant social and economic benefits. However, the safety and security of GNSSs have become an increasing concern. If a GNSS signal is inadvertently interfered with or is maliciously attacked, the GNSS user experience will be affected. In severe cases, an accident caused by interference or attack may generate irreversible economic loss or create a significant threat to individual safety. Therefore, a study of GNSS signal anti-interference and anti-spoofing becomes the focus.

1.1 Spoofing attack

1.1.1 Spoofing via navigation signal simulator

Initially, a navigation signal simulator was developed to test receiver performance. However, the high-fidelity simulation of an authentic navigation signal raised considerable concerns about GNSS signal security. In 2002, Warner and Johnston et al. rented one simulator and proved that this equipment could spoof popular handheld civilian global positioning system (GPS) receivers in the market [1].

1.1.2 Repeater spoofing

An encrypted navigation signal in a GNSS system, e.g., P code in a GPS, does not have a public interface specification. Therefore, it cannot be spoofed by a navigation signal simulator. However, for this type of navigation signal, the so-called repeater spoofing is an effective spoofing method. As shown in Fig. 1, this spoofing method

* Correspondence: maggice-sun@163.com
Department of Electronic Engineering, Tsinghua University, Beijing, China

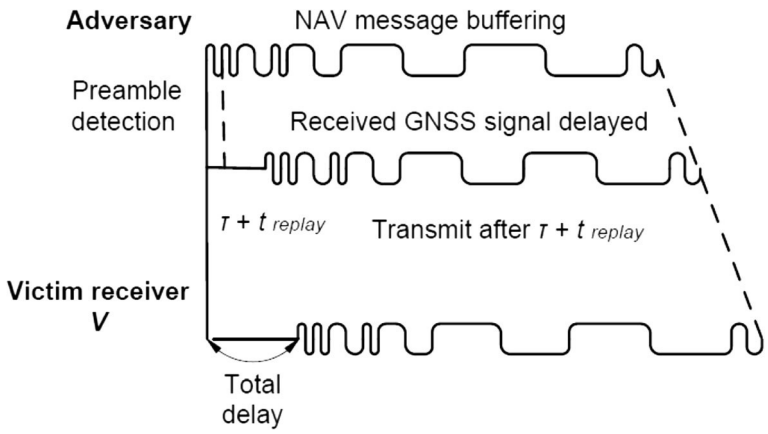

Fig. 1 Schematic of repeater spoofing

forwards a received navigation signal to an interference receiver. When a repeater spoofing signal captures control of the receiver, a high-power suppressing signal is emitted to force the receiver into a trapped state to ensure that a spoofing signal can be accepted by the receiver, resulting in significant errors in positioning [2].

1.1.3 Receiver-spoofer

The concept of a receiver-spoofer was initially proposed by Todd E. Humphreys et al. at the University of Texas in 2008 [3–5]. Receiver signal tracking is not interrupted during spoofing, and the power used does not need to be significantly higher than that of an authentic signal. Therefore, a receiver-spoofer has an extremely high level of covertness. The principle is shown in Fig. 2. Based on a received authentic navigation signal, the relative position and the velocity versus the target receiver, a spoofing device calculates the pseudo-range and Doppler shift of an authentic navigation signal received by a target receiver and generates a spoofing signal that is synchronous with the authentic signal. Because this signal is similar to the authentic signal, it takes control without being noticed by the target receiver.

Todd E. Humphreys et al. successfully spoofed an electric power grid monitoring system time authorization terminal [6], an unmanned aerial vehicle [7], and civilian vessels [8] via this spoofing platform.

1.2 Anti-spoofing technology

Anti-spoofing refers to the operation of employing a certain measure or technology to detect and eliminate a GNSS spoofing signal or to hinder the ability of an attacker to spoof a target. Current anti-spoofing technology relies on two approaches. The first approach is to distinguish authentic and spoofing signals via comparison. A GNSS interface specification is publicly available, and a navigation signal generated by a spoofing device cannot be identical to an authentic signal. As the simulation accuracy of a spoofing signal increases, the cost increases as well. Therefore, the spoofing signal can be identified by finding the difference between the spoofing signal and the authentic signal. The second approach is to detect signal abnormality during spoofing. For power suppression spoofing, an alarm is generated by detecting power abnormalities. For a receiver-spoofer, a warning is generated by detecting correlation distortion in the code loop. Based on the two approaches, this study on anti-spoofing measures focuses on the following aspects:

1.2.1 Improving the signal processing algorithm

A new detection process is added to the signal processing algorithm to detect carrier magnitude hop, signal power abnormality, and distortion of correlation [9]. In most circumstances, a spoofing attack is detectable. These methods are easily implemented and do not require major hardware changes. However, the selection of an adequate detection threshold to achieve a balance between a false alarm and a positive detection is critical.

1.2.2 Signal encryption

The essence of signal encryption is to generate unpredictable navigation information that prevents an attacker from counterfeiting a similar signal for spoofing. Currently, numerous institutions have conducted thorough studies of this anti-spoofing technology [10, 11]. A disadvantage of this method is that the signal architecture of a navigation system must be changed, which requires design changes for satellite transmitters and ground receivers. For a relative mature navigation system, such as a GPS, anti-spoofing via this approach is very expensive. For a navigation system in the experimental stage, implementation of signal encryption in the signal architecture is an effective approach to improving the security and reliability of the entire navigation system.

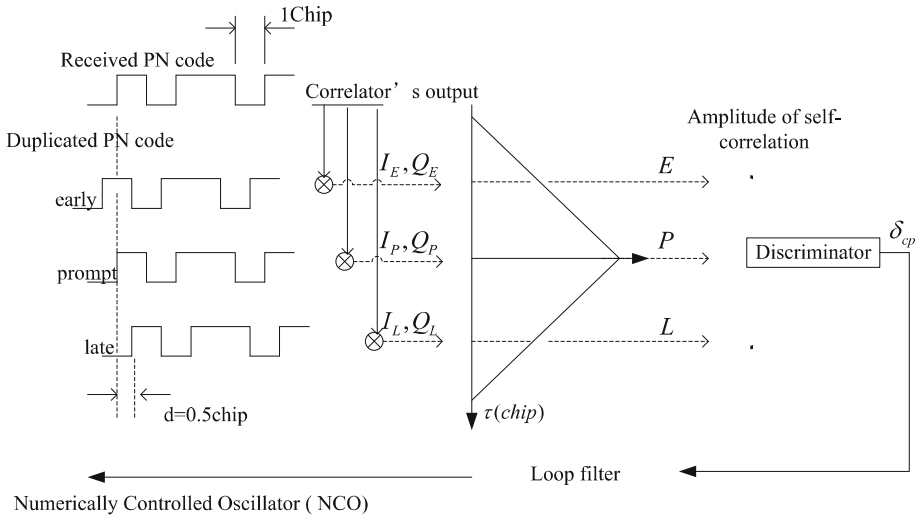

Fig. 2 Principle of receiver code loop operation

1.2.3 Leveraging external accessories

This detection measure leverages receiver accessories to monitor an abnormal hop in position, velocity, or clock [12]. For a receiver with external reference information, when a spoofing attack causes a significant difference between the result calculated by a receiver and the external reference information, the received signal may contain a spoofing signal.

1.2.4 Signal direction detection

Carrier phase-based signal direction monitoring is a common spoofing detection method [13]. If an attacker needs to ensure that the direction of the counterfeited signal is the same as or close to that of an authentic signal, the cost of doing so is generally high. In most scenarios, if a receiver can measure the direction of a received carrier, it can easily discriminate between a spoofing signal and an authentic signal.

Analysis of spoofing attacks and anti-spoofing technology indicates that a receiver-spoofer is superior to other spoofing methods in terms of covertness and practicality, and its detection is difficult. Typically, a receiver-spoofer can only be detected by a combination of multiple anti-spoof measures, e.g., a combination of power detection and correlation distortion detection. Therefore, a study of the characteristics and key parameters of this spoofing attack and the analysis of its performance will improve the effectiveness of the anti-spoofing technology for navigation systems and ensure that defending measures are targeted.

2 Analysis of key parameters that affect the probability of spoofing success

The principle of the receiver code loop [14] is shown in Fig. 2.

The signal received by a receiver undergoes correlation and coherent integration with locally generated early, prompt, and late PN codes to integrate the I and Q branches and calculate the self-correlation amplitudes E, P, and L. Because the navigation signal PN code self-correlation function is symmetric along the y-axis, when a received signal aligns with the local code, E should be equal to L. If the calculated E is unequal to L, the receiver concludes that the local code is misaligned and will generate a phase discrimination result based on the difference between E and L. This difference is adjusted via a numeric control oscillator (NCO) to complete code phase alignment. Therefore, calculating E and L is the key to code phase alignment. The spoofing signal seizes control by affecting this value.

At this moment, E and L are calculated via Formula (1):

$$E = \sqrt{I_{\mathrm{E}}^2 + Q_{\mathrm{E}}^2} = aR(\tau_{\mathrm{E}})|\ \mathrm{sinc}(f_{\mathrm{e}}T_{\mathrm{coh}})| L = \sqrt{I_{\mathrm{L}}^2 + Q_{\mathrm{L}}^2} = aR(\tau_{\mathrm{L}})|\ \mathrm{sinc}(f_{\mathrm{e}}T_{\mathrm{coh}})| \tag{1}$$

Of which I_{E}, Q_{E}, I_{L}, and Q_{L} represent the early/late correlation integration of I/Q branch. a represents the amplitude of signals. $R(\bullet)$ represents the unitized correlation function of PN codes. τ_{E} and τ_{L} represent the phase difference between early/late local code and received code. f_{e} represents the frequency differences of a local replicate carrier versus received signals. T_{coh}represents the correlation and coherent integration period. E and L are approximately equal.

When an authentic signal and a spoofing signal coexist, the signal at the receiver is a superposition of the two signals.

$$S(t) = S_{\mathrm{R}}(t) + S_{\mathrm{S}}(t) \tag{2}$$

Of which $S(t)$ represents the received signal. $S_{\mathrm{R}}(t)$ represents the authentic signal. $S_{\mathrm{S}}(t)$ represents the spoofing signal.

At this moment, the phase discriminator output is shown in Fig. 3.

$$K = \sqrt{(I_K + I'_K)^2 + (Q_K + Q'_K)^2} = \sqrt{(A \cdot R_K(\tau_R)|\ \mathrm{sinc}(f_e T_{coh})|)^2 + (\eta A \cdot R_K(\tau_S)|\ \mathrm{sinc}(f_e' T_{coh})|)^2 + 2\eta A^2 R_K(\tau_R) R(\tau_S)|\ \mathrm{sinc}(f_e T_{coh})||\ \mathrm{sinc}(f_e' T_{coh})|\ \cos(\phi - \phi')} \quad (3)$$

Here, K represents the early/late non-coherent integration. τ_R and τ_S represent the phase differences of the local replicate code versus an authentic signal and a spoofing signal, respectively. $R_K(\tau_R)$ and $R_K(\tau_S)$ represent the normalized early/late correlation functions for authentic signals and spoofing signals, respectively. A and η represent the amplitude of authentic signals and the ratio of the spoofing signal amplitude to the authentic signal amplitude. f_e and $\dot{f}_e$ represent the frequency differences of a local replicate carrier versus authentic signals and spoofing signals. ϕ and $\dot{\phi}$ represent the carrier phases of authentic signals and spoofing signals.

These parameters have an impact on the spoofing process. In addition to these parameters, the phase discriminator spacing d is also a factor that will affect the calculation of E and L, since it is a parameter of the correlation function $R(.)$, which will be expressed in Formulae (9), (25), and (28). For brevity, noises from the I and Q branches are not included in the formula. Therefore, when loop noise is considered, the signal-to-noise ratio (SNR) is also a factor that impacts the spoofing process.

Considering numerous factors in the spoofing process, analyzing all factors is a complicated task. These parameters can be divided into three types. The first type is determined by the configuration of the target receiver, including the correlation and coherent integration period T_{coh}, phase discriminator spacing d, and authentic signal amplitude A. As these parameters are not controllable by a spoofing platform, these parameters are set to typical values, and the investigation is based on typical scenarios.

The second type is determined by the receiver authentic signal lock-in state during a spoofing attack, which includes the frequency difference between an authentic signal and a local replicate carrier (f_e) and the phase difference between an authentic signal and local replicate code (τ_R). A reasonable assumption is as follows: before spoofing, the target receiver steadily tracks an authentic signal. Therefore, f_e and τ_R are approximately equal to 0.

The last type is closely related to a spoofing signal; these parameters include the frequency difference between a spoofing signal and a local replicate carrier ($\dot{f}_e$), the phase difference between a spoofing signal and local replicate code (τ_S), the phase difference between an authentic signal carrier and a spoofing signal carrier ($\phi - \dot{\phi}$), and the ratio of the spoofing signal amplitude versus the authentic signal amplitude (η). The spoofing device always prefers that the first three parameters are close to 0, which is very difficult to achieve due to various reasons such as measurement error and device cost. Only η is a controllable parameter for the spoofing device. Therefore, η is the most important parameter for generating a spoofing signal and is the focus of numerous anti-spoofing attack studies. The spoofing-signal ratio (η) is defined as the ratio of the spoofing signal amplitude to the authentic signal amplitude. Based on the above assumption and the parameter analysis

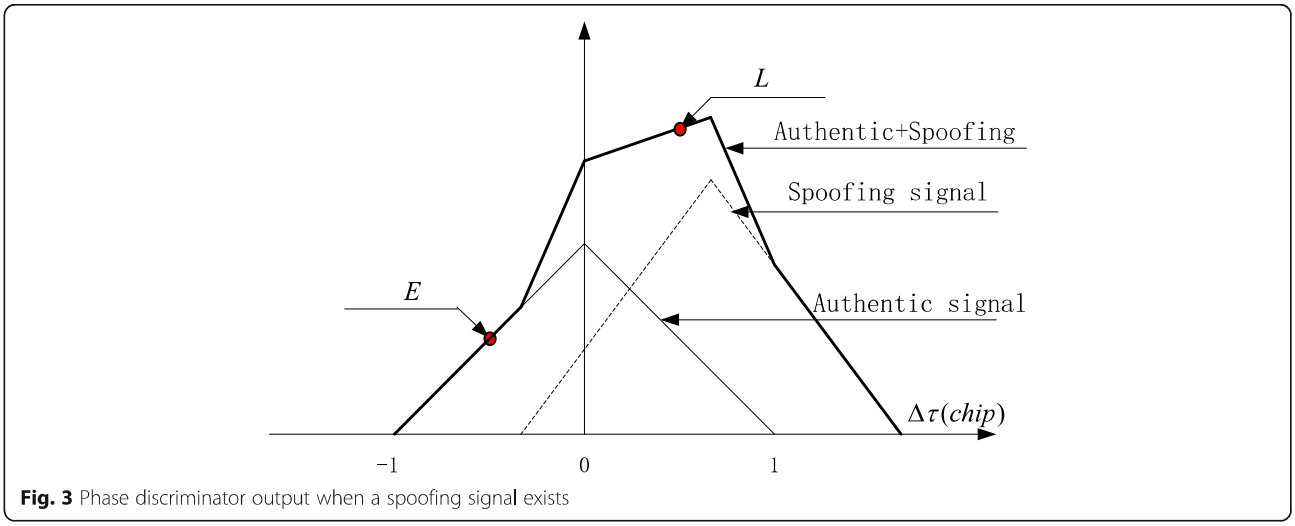

Fig. 3 Phase discriminator output when a spoofing signal exists

method, the lower limit of η required for successful spoofing in various conditions is deduced in the following sections.

3 Deduction of a formula for the lower limit of the spoofing-signal ratio

When the carrier frequency and phase from the spoofing device align with an authentic signal that is originally locked by the target receiver, the lower limit of the spoofing-signal ratio required for a spoofing device to seize control of a receiver code loop is deduced in reference [15]. We have the following:

When the phase discriminator spacing of the target receiver is equal to 0.5 chip, the lower limit of the spoofing-signal ratio is as follows:

$$\begin{cases} \inf\{\eta\} = 1 & \tau_0 \le 1 \\ \inf\{\eta\} = \dfrac{1}{2-\tau_0} & 1.5 > \tau_0 > 1 \\ \inf\{\eta\} = \infty & 1.5 \le \tau_0 \end{cases} \tag{4}$$

When the phase discriminator spacing of the target receiver is less than 0.5 chip, the lower limit of the spoofing-signal ratio is as follows:

$$\begin{cases} \inf\{\eta\} = 1 & \tau_0 \le 1 \\ \inf\{\eta\} = \dfrac{2d}{1+2d-\tau_0} & 1+d > \tau_0 > 1 \\ \inf\{\eta\} = \infty & 1+d \le \tau_0 \end{cases} \tag{5}$$

When the phase discriminator spacing of the target receiver exceeds 0.5 chip, the lower limit of the spoofing-signal ratio is as follows:

$$\begin{cases} \inf\{\eta\} = 1 & \tau_0 \le 2d \\ \inf\{\eta\} = \dfrac{2(1-d)}{2-\tau_0} & 1+d > \tau_0 > 2d \\ \inf\{\eta\} = \infty & 1+d \le \tau_0 \end{cases} \tag{6}$$

Here τ_0 represents the code phase difference between a spoofing signal and an authentic signal; this error is caused by an inaccurate estimation of the target receiver position by the spoofer. d represents the phase discriminator spacing of the target receiver. $\inf\{\eta\}$ is the lower limit of the spoofing-signal ratio required for successful spoofing under various τ_0.

In a real scenario, a spoofing signal has difficulty aligning with an authentic signal carrier received by the target receiver, or achieving this alignment is extremely expensive, e.g., high precision distance measurement technology (radar) can be employed to measure the relative position of the two signals. Therefore, these conclusions are only meaningful in a laboratory environment and have a very limited reference value for actual spoofing and anti-spoofing practice. This paper focuses on a scenario with a misaligned carrier and analyzes and deduces the lower limit of the spoofing-signal ratio required for successful spoofing.

The mechanism of a receiver-spoofer is as follows: the code phase of a spoofing signal is gradually changed to influence the code loop phase discriminator output and the disrupt receiver lock-in process on an authentic signal; the phase of the receiver local replicate code in the code loop is gradually induced to align with the code phase of the spoofing signal and drift from the authentic signal, after which receiver control is seized [3]. Assume that the spoofing signal code waits for the loop phase discriminator to stabilize before changing phases. Each phase change is referred to as a traction.

To simplify the deduction of the lower limit of the spoofing-signal ratio, assume that the frequencies of the spoofing signal, authentic signal, and receiver local replicate code are identical. This assumption requires that a spoofing device can accurately obtain velocity information about the target receiver, which is achievable in most spoofing scenarios, including a stationary receiver, ships, and steadily moving vehicles. With this assumption, f_e and $\dot{f}_e$ in Formula (3) are approximately equal to 0. Therefore, Formula (3) is simplified as follows:

$$\begin{aligned} S_K &= \sqrt{(I_K + I'_K)^2 + (Q_K + Q'_K)^2} = \\ &= \sqrt{(A \cdot R(\tau_K))^2 + (\eta A \cdot R(\tau'_K))^2 + 2\eta A^2 R(\tau_K) R(\tau'_K) \cos(\phi - \phi')} \\ K &= E, L \end{aligned} \tag{7}$$

The impact of the frequency difference is removed. The phase discrimination result is directly affected by the code phase difference and the carrier phase difference between an authentic signal and a spoofing signal, as well as the spoofing-signal ratio. Therefore, the lower limit of the spoofing-signal ratio is determined by the other two parameters. The phase discriminator spacing will affect the calculation of the correlation R. In the following sections, the formula for the lower limit of the spoofing-signal ratio for different phase discriminator spacings is discussed.

3.1 Phase discriminator spacing of target receiver = 0.5 chip

Assume that the spoofing signal enters the code loop traction range at t_0. After the spoofing signal enters the code loop, the code loop attains an equilibrium state at t_1. Assume that at t_0 and t_1, the code phase difference between an authentic signal and a spoofing signal is τ_0 and stabilizes. The definition of the code loop equilibrium state is that the early correlation of the code loop is equal to the late correlation, i.e., $E = L$. In the deduction in Reference [15], an initial conclusion is obtained: at t_1, the phase difference between the spoofing signal and the local code is $\tau_S(t_1)$; the code phase difference between an authentic signal and the local code is $\tau_R(t_1)$; and once $\tau_R(t_1) < d$ and $\tau_S(t_1) > d$, spoofing will fail. Assume that the receiver local replicate code aligns with an authentic signal at t_0, i.e., $\tau_R(t_0) = 0$. At this moment, the following expressions hold:

$$\begin{cases} E(t_1) = L(t_1) \\ \tau_S(t_1) + \tau_R(t_1) = \tau_0 \end{cases} \tag{8}$$

where $E(t_1)$ and $L(t_1)$ represent the lead correlation and lag correlation at t_1; τ_0 represents the code phase difference between a spoofing signal and an authentic signal at t_0 and t_1. The correlation function $R(\tau)$ of the PN codes can be expressed in Formula (9) as follows:

$$\begin{cases} R_E(\tau) = 0, & R_L(\tau) = A(1+d+\tau), & -1-d \le \tau < -d \\ R_E(\tau) = A(1-d+\tau), & R_L(\tau) = A(1-d-\tau), & -d \le \tau < d \\ R_E(\tau) = A(1+d-\tau), & R_L(\tau) = 0, & d \le \tau \le 1+d \\ R_E(\tau) = 0, & R_L(\tau) = 0, & \text{other} \end{cases} \tag{9}$$

where d represents the phase discriminator spacing; τ represents the code phase difference between the signal and the local replicate code.

According to Formula (7), for E and L, as well as Formula (9) for the correlation function $R(\tau)$, when $\tau_R(t_1) < d$ and $\tau_S(t_1) > d$ is substituted into Formula (8), the solution for $\tau_R(t_1)$ and $\tau_S(t_1)$ is as follows:

$$\begin{cases} \tau_R(t_1) = (\pm \sqrt{(\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4)\eta^2 \\ \quad +4d\eta\alpha\tau_0 + 8d\eta\alpha - 4\eta\alpha\tau_0 - 8\eta d^2\alpha + 4d^2 - 8d + 4} \\ -2d\eta\alpha + 2d + d\eta^2 - \eta^2\tau_0 + \eta^2 + \eta\alpha\tau_0 - 2)/(-\eta^2 + 2\eta\alpha) \end{cases} \tag{10}$$

where $\alpha = \cos(\phi - \phi')$ represents the cosine of the carrier phase difference between an authentic signal and a spoofing signal. The sign "±" in Formula (10) should be "+" when $-\eta^2 + 2\eta\alpha$ is greater than 0, and it should be "−" when $-\eta^2 + 2\eta\alpha$ is less than 0. Once the spoofing-signal ratio η of the spoofing signal is in the range for which a solution for $\tau_S(t_1)$ and $\tau_R(t_1)$ in Formula (10) exists, $\tau_R(t_1) < d$ and $\tau_S(t_1) > d$, this spoofing-signal ratio will cause spoofing failure. The solution space S for this condition is calculated, and the complementary set $\overline{S}$ is calculated to obtain the spoofing-signal ratio required for successful spoofing.

The necessary condition for the $\tau_R(t_1)$ solution is that the radical in Formula (10) is greater than or equal to 0.

$$\begin{aligned} &(\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4)\eta^2 \\ &\quad +4d\eta\alpha\tau_0 + 8d\eta\alpha - 4\eta\alpha\tau_0 - 8\eta d^2\alpha + 4d^2 - 8d + 4 \ge 0 \end{aligned} \tag{11}$$

To solve inequation (11), first, the solutions for the following equation are obtained:

$$\begin{aligned} &(\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4)\eta^2 \\ &\quad +4d\eta\alpha\tau_0 + 8d\eta\alpha - 4\eta\alpha\tau_0 - 8\eta d^2\alpha + 4d^2 - 8d + 4 = 0 \end{aligned}$$

The solutions are

$$\begin{cases} \eta_1 = \dfrac{2\alpha(\tau_0 - 2d + 2d^2 - d\tau_0) - 4\sqrt{3d\tau_0 - 2d - \tau_0 + 2d\alpha^2 - 3d^2\tau_0 + d^3\tau_0 + \alpha^2\tau_0 + 2d^3 - d^4 - \alpha^2 - 2d^3\alpha^2 + d^4\alpha^2 - 3d\alpha^2\tau_0 + 3d^2\alpha^2\tau_0 - d^3\alpha^2\tau_0 + 1}}{\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4} \\ \eta_2 = \dfrac{2\alpha(\tau_0 - 2d + 2d^2 - d\tau_0) + 4\sqrt{3d\tau_0 - 2d - \tau_0 + 2d\alpha^2 - 3d^2\tau_0 + d^3\tau_0 + \alpha^2\tau_0 + 2d^3 - d^4 - \alpha^2 - 2d^3\alpha^2 + d^4\alpha^2 - 3d\alpha^2\tau_0 + 3d^2\alpha^2\tau_0 - d^3\alpha^2\tau_0 + 1}}{\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4} \end{cases} \tag{12}$$

Second, the coefficient of η^2 in Formula (11) is considered:

$$A = \alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4 \tag{13}$$

When $A < 0$, the solution space of inequation (11) is

$$S_1 = [\ \min(\eta_1, \eta_2),\ \max(\eta_1, \eta_2)] \tag{14}$$

When $A > 0$, the solution space of inequation (11) is

$$S_1 = [-\infty,\ \min(\eta_1, \eta_2)] \cup [\ \max(\eta_1, \eta_2), \infty] \tag{15}$$

To ensure that $\tau_R(t_1) < d$, inequation (16) holds.

$$\begin{aligned} &\pm\sqrt{(\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4)\eta^2} - 2d\eta\alpha \\ &\quad +4d\eta\alpha\tau_0 + 8d\eta\alpha - 4\eta\alpha\tau_0 - 8\eta d^2\alpha + 4d^2 - 8d + 4 \\ &\quad \frac{+2d + d\eta^2 - \eta^2\tau_0 + \eta^2 + \eta\alpha\tau_0 - 2}{-\eta^2 + 2\eta\alpha} < d \end{aligned} \tag{16}$$

Similarly, the solution for the equation

$$\begin{aligned} &\pm\sqrt{(\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4)\eta^2} \\ &\quad +4d\eta\alpha\tau_0 + 8d\eta\alpha - 4\eta\alpha\tau_0 - 8\eta d^2\alpha + 4d^2 - 8d \\ &\sqrt{\frac{+4 - 2d\eta\alpha + 2d + d\eta^2 - \eta^2\tau_0 + \eta^2 + \eta\alpha\tau_0 - 2}{-\eta^2 + 2\eta\alpha}} = d \end{aligned} \tag{17}$$

is

$$\begin{cases} \eta_3 = \dfrac{2d\alpha - \alpha - \sqrt{4d^2\alpha^2 - 4d^2 - 4d\alpha^2 + 4d + \alpha^2}}{2d - \tau_0 + 1} \\ \eta_4 = \dfrac{2d\alpha - \alpha + \sqrt{4d^2\alpha^2 - 4d^2 - 4d\alpha^2 + 4d + \alpha^2}}{2d - \tau_0 + 1} \end{cases} \tag{18}$$

When $\tau_0 > 1 + d$, the spoofing signal cannot enter the phase discriminator traction range, so $\tau_0 \le 1 + d$. Therefore, the coefficient of η^2 in inequation (16) is expressed as follows:

$$A' = 2d - \tau_0 + 1 > 0 \tag{19}$$

The solution space for inequation (16) is expressed as follows:

$$S_2 = [\ \min(\eta_3, \eta_4),\ \max(\eta_3, \eta_4)] \tag{20}$$

The spoofing-signal ratio η that leads to spoofing failure should be in $S_1 \cap S_2$; the complementary set $S = \overline{S_1 \cap S_2}$ is the spoofing-signal ratio η range for successful spoofing. Based on Formulae (14), (15), and (20),
when $A = \alpha^2\tau_0^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4 < 0$,

$$S = \overline{S_1 \cap S_2} = (-\infty,\ \max(\ \min(\eta_1, \eta_2),\ \min(\eta_3, \eta_4)\ ]\cup[\ \min(\ \max(\eta_1, \eta_2),\ \max(\eta_3, \eta_4)), +\infty) \tag{21}$$

and when
$A = \alpha^2\tau_0^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4 > 0,$

$$S = \overline{S_1 \cap S_2} = (-\infty,\ \min(\eta_3, \eta_4)]\cup[\ \min(\eta_1, \eta_2),\ \max(\eta_1, \eta_2)]\ \cup[\ \max(\eta_3, \eta_4), +\infty) \tag{22}$$

Formulae (21) and (22) and $\eta > 1$ are combined to obtain the lower limit of the spoofing-signal ratio required for successful spoofing.

$$\begin{cases} \inf(\eta) = \min(\ \max(\eta_1, \eta_2),\ \max(\eta_3, \eta_4)), \\ if\ \alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4 < 0 \\ \inf(\eta) = \max(\ \min(\eta_1, \eta_2),\ \min(\eta_3, \eta_4)), \\ if\ \alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4 > 0 \end{cases} \tag{23}$$

When $d = 0.5$ and no carrier phase difference between authentic signals and spoofing signals is observed, i.e., $\alpha = \cos(\phi - \phi') = \cos 0 = 1$, Formula (23) is simplified as follows:

$$\inf\{\eta\} = \frac{1}{2 - \tau_0} \tag{24}$$

This result matches the conclusion in Reference [15].

3.2 Phase discriminator spacing of target receiver < 0.5 chip

When the phase discriminator spacing of the target receiver is under 0.5 chip, the spoofing failure condition is $\tau_R(t_1) < d$ and $1 - d < \tau_S(t_1)$ (Reference [15]). Similar to the deduction in Section 3.1, Formula (8) for E and L and the correlation function $R(\tau)$ for $\tau_R(t_1) < d$ and $1 - d < \tau_S(t_1)$ (Formula (25) are substituted into Formula (8):

$$\begin{cases} R_E(\tau) = 0, & R_L(\tau) = A(1 + d + \tau), & -1 - d \le \tau < d - 1 \\ R_E(\tau) = A(1 - d + \tau), & R_L(\tau) = A(1 + d + \tau), & d - 1 \le \tau < -d \\ R_E(\tau) = A(1 - d + \tau), & R_L(\tau) = A(1 - d - \tau), & -d \le \tau \le d \\ R_E(\tau) = A(1 + d - \tau), & R_L(\tau) = A(1 - d - \tau), & d < \tau \le 1 - d \\ R_E(\tau) = A(1 + d - \tau), & R_L(\tau) = 0, & 1 - d < \tau \le 1 + d \\ R_E(\tau) = 0, & R_L(\tau) = 0, & \text{other} \end{cases} \tag{25}$$

The solution for $\tau_R(t_1)$ is as follows:

$$\begin{cases} \tau_R(t_1) = (\pm \sqrt{\begin{array}{l} (\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4)\eta^2 \\ +4d\eta\alpha\tau_0 + 8d\eta\alpha - 4\eta\alpha\tau_0 - 8\eta d^2\alpha \\ +4d^2 - 8d + 4 - 2d\eta\alpha + 2d + d\eta^2 - \eta^2\tau_0 \\ +\eta^2 + \eta\alpha\tau_0 - 2)/(-\eta^2 + 2\eta\alpha)\tau_S(t_1) = \tau_0 - \tau_R(t_1) \end{array}} \end{cases} \tag{26}$$

Similar to the solution in Section 3.1 for $\tau_R(t_1)$, at this moment, the formula for the lower limit of the spoofing-signal ratio is similar to Formula (23).

Similarly, when no carrier phase difference between an authentic signal and a spoofing signal is observed, i.e., $\alpha = \cos(\phi - \phi') = \cos 0 = 1$, the formula for the lower limit of the spoofing-signal ratio is simplified as follows:

$$\inf\{\eta\} = \frac{2d}{2d - \tau_0 + 1} \tag{27}$$

This result matches the conclusion in Reference [15].

3.3 Phase discriminator spacing of target receiver > 0.5 chip

When the phase discriminator spacing of the target receiver exceeds 0.5 chip, the spoofing failure condition is $\tau_R(t_1) < 1 - d$ and $d < \tau_S(t_1)$ (Reference [15]). Similar to the deduction in Section 3.1, Formula (7) for E and L and the correlation function $R(\tau)$ for $\tau_R(t_1) < 1 - d$, $d < \tau_S(t_1)$ (Formula (28)) are substituted into Formula (8):

$$\begin{cases} R_E(\tau) = 0, & R_L(\tau) = A_s(1 + d + \tau), & -1 - d \le \tau < -d \\ R_E(\tau) = 0, & R_L(\tau) = A_s(1 - d - \tau), & -d \le \tau < d - 1 \\ R_E(\tau) = A_s(1 - d + \tau), & R_L(\tau) = A_s(1 - d - \tau), & d - 1 \le \tau \le 1 - d \\ R_E(\tau) = A_s(1 - d + \tau), & R_L(\tau) = 0, & 1 - d < \tau \le d \\ R_E(\tau) = A_s(1 + d - \tau), & R_L(\tau) = 0, & d < \tau \le 1 + d \\ R_E(\tau) = 0, & R_L(\tau) = 0, & \text{other} \end{cases} \tag{28}$$

The solution for $\tau_R(t_1)$ is as follows:

$$\begin{cases} \tau_R(t_1) = (\pm \sqrt{\begin{array}{l} (\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4)\eta^2 \\ +4d\eta\alpha\tau_0 + 8d\eta\alpha - 4\eta\alpha\tau_0 - 8\eta d^2\alpha + 4d^2 - 8d \\ +4 - 2d\eta\alpha + 2d + d\eta^2 - \eta^2\tau_0 + \eta^2 \\ +\eta\alpha\tau_0 - 2)/(-\eta^2 + 2\eta\alpha)\tau_S(t_1) = \tau_0 - \tau_R(t_1) \end{array}} \end{cases} \tag{29}$$

This finding is similar to the solution for $\tau_R(t_1)$ in Section 3.1. However, the condition changes to $\tau_R(t_1) < 1 - d$ and $d < \tau_S(t_1)$. Therefore, the solutions for inequation (30) are required.

$$\pm \sqrt{\begin{array}{l} (\alpha^2\tau_0{}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4)\eta^2 \\ +4d\eta\alpha\tau_0 + 8d\eta\alpha - 4\eta\alpha\tau_0 - 8\eta d^2\alpha \\ +4d^2 - 8d + 4 - 2d\eta\alpha + 2d + d\eta^2 - \eta^2\tau_0 + \eta^2 \\ \dfrac{+\eta\alpha\tau_0 - 2}{-\eta^2 + 2\eta\alpha} \end{array}} < 1 - d \tag{30}$$

The solutions are

$$\begin{cases} \eta_3 = \dfrac{2 - 2d}{2 - \tau_0} \\ \eta_4 = \dfrac{2d - 2}{2 - \tau_0} \end{cases} \tag{31}$$

Because the phase discriminator spacing $d > 1$ is meaningless, $d < 1$ and $\tau_0 \le 1 + d < 2$. Therefore, $\eta_3 > \eta_4$ and Formula (23) is rearranged as follows:

$$\begin{cases} \inf(\eta) = \min\left(\max(\eta_1, \eta_2), \eta_3\right), \\ \text{if} \alpha^2 {\tau_0}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4 < 0 \\ \inf(\eta) = \max\left(\min(\eta_1, \eta_2), \eta_4\right), \\ \text{if} \alpha^2 {\tau_0}^2 - 4\alpha^2\tau_0 + 4\alpha^2 + 4d^2 - 4d\tau_0 + 4\tau_0 - 4 > 0 \end{cases} \tag{32}$$

Similarly, when no carrier phase difference is observed between an authentic signal and a spoofing signal, i.e., $\alpha = \cos(\phi - \phi') = \cos 0 = 1$, the formula for the lower limit of the spoofing-signal ratio is simplified as follows:

$$\inf\{\eta\} = \frac{2-2d}{2-\tau_0} \tag{33}$$

This finding matches the conclusion in Reference [15].

Based on the initial conclusions in Reference [15], when the carrier phases of authentic and spoofing signals are misaligned, the lower limit of the spoofing-signal ratio required for successful spoofing is deduced. When the carrier phases of authentic and spoofing signals are aligned, the formula for the lower limit matches the conclusion in Reference [15]. In the next section, the validity of these conclusions is verified via testing.

4 Test verification

In this section, the formula for calculating the spoofing-signal ratio, which was derived in the previous sections will be verified in testing. GPS signal is the most popular and matured navigation system, so we select GPS signal and GPS receiver as the testing signal and device. The test includes two parts. The first part is a test using a GNSS signal generator, which will be repeated 100 times. The lower limit of the spoofing-signal ratio in each test will be recorded. Then the highest value in the statistic of these 100 results will be compared with the theoretical result. In the second part, a GPS receiver collects and stores authentic signal with a length of 1 h. Then randomly select 100 starting points to generate 100 testing data with the length of 1 ms each. The spoofing-signal ratio lower limits of these 100 testing samples are obtained. The highest value of them will be compared with the theoretical result. Below are the detailed introduction of the two parts of the test, as well as the analysis of the results of the testing.

4.1 Verification via a signal generated by a signal simulation source

The GNSS signal simulation source can accurately control the navigation signal SNR, the spoofing-signal ratio of an authentic signal to a spoofing signal, the carrier phase difference, and the code phase difference between the two signals. Therefore, the signal simulation source is employed to generate the data required in the test. In each test, the simulation source generates two signals: an authentic signal and a spoofing signal. The two signals have identical frequencies. The carrier phase difference between the two signals is set to 0.1, 0.2, 0.3, 0.4, and 0.5 (unit, radian). The code phase difference between the two signals increases from 0~1+d chip (d represents the receiver phase discriminator spacing); the increase step size is 0.01 chip. To verify the results for different phase discriminator spacings, Matlab software receiver is employed. The phase discriminator spacing is set to 0.3 (< 0.5), 0.5 (equal to 0.5), and 0.7 (above 0.5) chip. The test procedure is as follows:

1. The simulation source generates an authentic signal; the software receiver exports stable and accurate positioning results.
2. The power difference between the spoofing signal and authentic signal, the carrier phase difference, and the

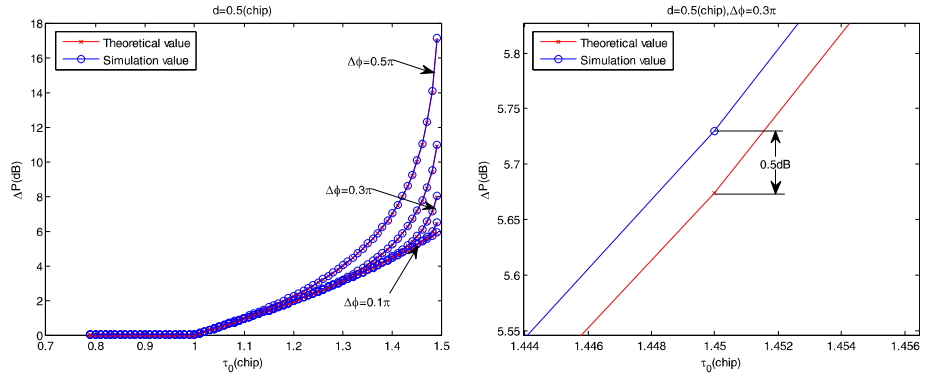

Fig. 4 Theoretical value versus simulation data when phase discriminator spacing = 0.5 chip. **a** Overall diagram. **b** Zoomed-in diagram

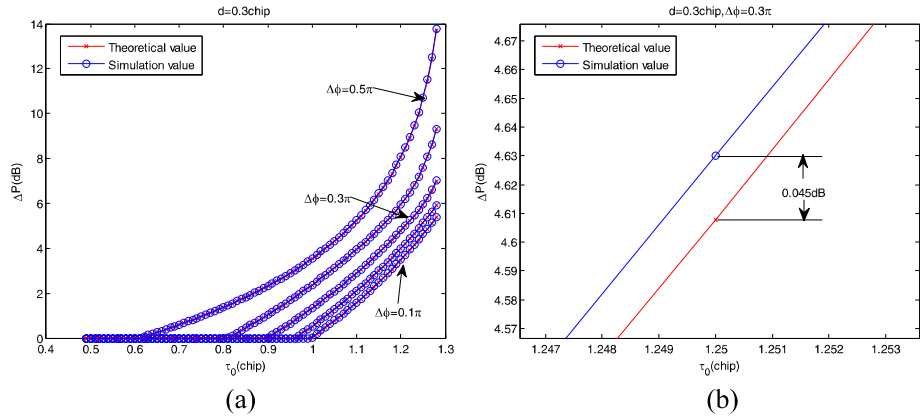

Fig. 5 Theoretical value versus simulation data when phase discriminator spacing = 0.3 chip

code phase difference between the two signals are configured to generate the spoofing signal.

3. The code phase difference between the authentic signal and spoofing signal is gradually adjusted to separate the two signals. The spoofing signal is evaluated to determine if it can seize control from a receiver. The criterion for successful control seizure is as follows: the distance between the code phase of the authentic signal and the code phase of the receiver local replicate signal exceeds 1 + d; the distance between the code phase of the spoofing signal and the code phase of the receiver local replicate signal is less than 1+d. If spoofing is successful, go to step 4. Otherwise, increase the power of the spoofing signal, and repeat step 3.
4. Record the power difference between the spoofing signal and the authentic signal. Increase the code phase difference between the two signals by 0.01 chip; reset the power difference to 0, and repeat step 2 until the code phase difference is equal to 1+d. Go to step 5.
5. Increase the carrier phase difference between the two signals by 0.1 rad; reset the code phase difference to 0, and repeat step 2 until the carrier phase difference is equal to 0.6 rad. Go to step 6.
6. Repeat the above test for 100 times. Record and study the highest value of the power difference lower limits in these 100 tests. Convert the spoofing-signal ratio calculated by Formulae (24) and (33) to the power difference and compare it with the recorded power difference to verify the validity of the formula.

4.2 Verification via an authentic navigation signal

To prove the validity and practicality of Formulae (24) and (33), an authentic GPS navigation signal collected by the receiver is employed for verification. The sampling rate is set to 14 MHz, and the intermediate frequency is set to 3 MHz. One-hour-long authentic navigation signal of a GPS satellite is collected and recorded. Randomly selects 100 data with 1-ms length each in the recorded authentic navigation signal. The data are processed via Matlab software to

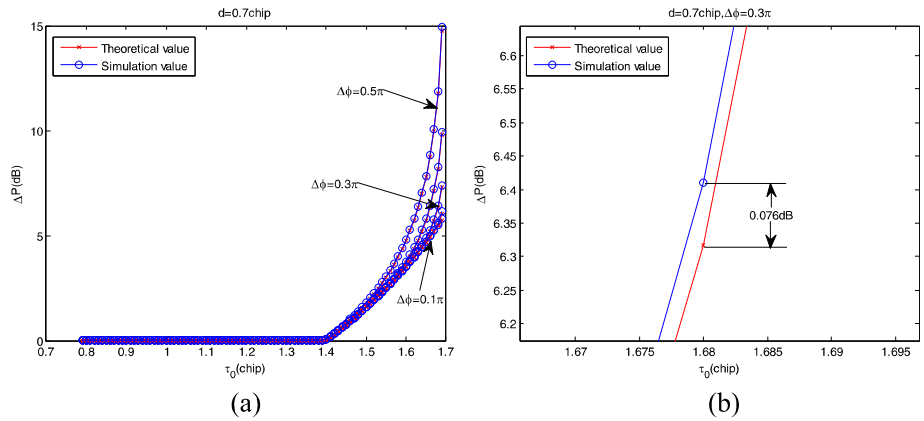

Fig. 6 Theoretical value versus simulation data when phase discriminator spacing = 0.7 chip. **a** Overall diagram. **b** Zoomed-in diagram

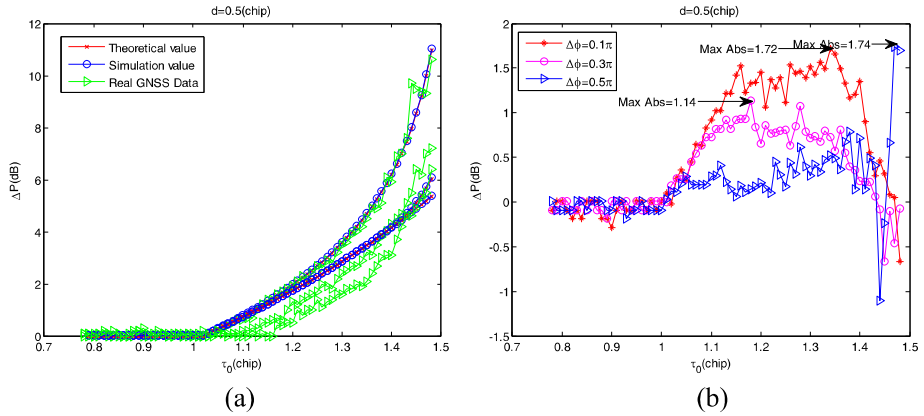

Fig. 7 Theoretical value, simulation data, and authentic signal alignment results when phase discriminator spacing = 0.5 chip. **a** Overall diagram. **b** Zoomed-in diagram

extract information including the carrier phase, code phase, navigation message, and Doppler shift. The carrier, pseudo code, and navigation message in the signal are separated, and the carrier phase and code phase are altered and recombined with the noise to recreate the spoofing signal, for which the signal-to-noise ratio is set to 10 dB. Similar to the test procedure in Section 4.1, the carrier phase difference between the authentic signal and the spoofing signal is set to 0.1, 0.2, 0.3, 0.4, and 0.5 (unit, radians). The code phase difference between the two signals gradually increases from 0~1+d chip (d represents the receiver phase discriminator spacing); the step size of this increase is 0.01 chip. The phase discriminator spacing of Matlab software receiver is set to 0.3 (< 0.5), 0.5 (= 0.5), and 0.7 chip (> 0.5). The minimum power required for successful spoofing is recorded, and the highest value of the power difference lower limits in these 100 tests is studied and is compared with the results calculated by Formulae (24) and (33).

5 Results and discussion

5.1 The result of the signal simulation source

The test results obtained by using the GNSS signal generator are shown in Figs. 4, 5 and 6.

Figures 4, 5 and 6 show the results of the theoretical value versus the simulation value when the phase discriminator spacing is 0.5 chip, 0.3 chip, and 0.7 chip. In the three zoomed-in diagrams, the error between the theoretical value and the simulation value is always under 0.1 dB in the three scenarios. The theoretical results are close to the simulation results, thereby demonstrating the validity of Formulae (24) and (33).

5.2 The result of the authentic navigation signal

The test results obtained by using the authentic navigation signal are shown in Figs. 7, 8 and 9.

Figures 7, 8 and 9 show the theoretical value, the simulation data, and the authentic signal alignment results when the discriminator spacing is equal to 0.5 chip, 0.3 chip, and 0.7 chip. These three figures show

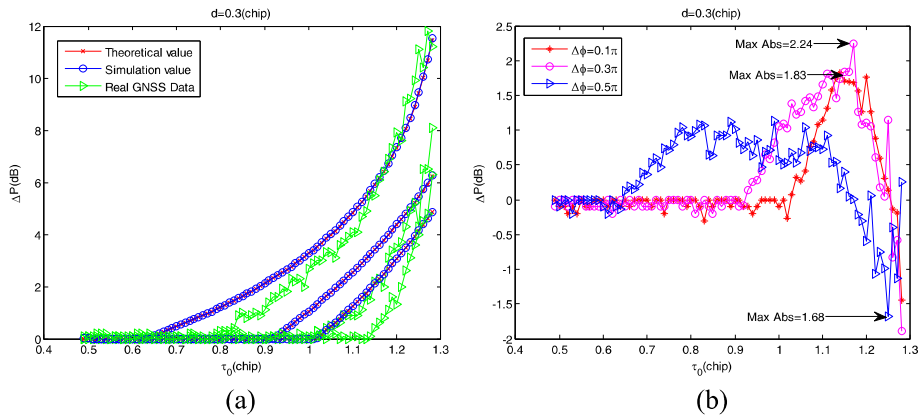

Fig. 8 Theoretical value, simulation data, and authentic signal alignment results when phase discriminator spacing = 0.3 chip. **a** Overall diagram. **b** Zoomed-in diagram

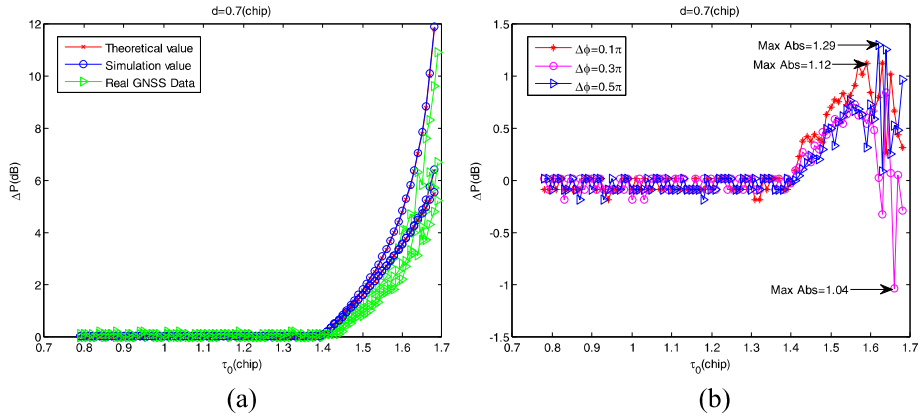

Fig. 9 Theoretical value, simulation data, and authentic signal alignment results when phase discriminator spacing = 0.7 chip. **a** Overall diagram. **b** Zoomed-in diagram

theoretical values minus real values measured by GPS. After adding noise, the difference between the theoretical value and the measured data increases, but the maximum values in these three cases do not exceed 2 dB and trend toward convergence. Using Formulae (24) and (33) to calculate the results of the lower limit of the spoofing-signal ratio provides strong guidance in actual attack scenarios. In addition, the influence of noise can change the lower limit of the spoofing-signal ratio, inducing it not only to grow in one direction but also to fluctuate around the theoretical value. This is because noise affects not only the spoofing signal but also the authentic signal. Under certain conditions, noise may make the control loop capture the spoofing signal more easier than capture the authentic signal.

From the results of these theoretical calculations, the simulation results and the measured results, all of the corresponding values τ_0 when the lower limit of the spoofing-signal ratio changes from zero to non-zero are the same. When the discriminator spacing is less than or equal to 0.5 chip, the critical point falls in the vicinity of 1 chip. When the discriminator spacing is greater than 0.5 chip and the critical point is in the vicinity of 2× spacing, the critical point has no effect on the carrier phase difference between two signals. Therefore, while the spoofer estimates the position of the target sufficiently accurately and the code phase of the spoofing signal and the authentic signal is sufficiently close, the spoofer can successfully capture control of the target machine when the power of the spoofing signal is slightly greater than that of the authentic signal.

In these experiments, our discussions are limited to situations with carrier phase differences less than or equal to 90°. This is because when the carrier phase difference between the spoofing and authentic signals is within the range (90°, 180°), these two signals are no longer in superposition and weaken each other. In this scenario, the conclusions of Chapter 3 are no longer accurate, and the lower limit of the spoofing-signal ratio calculated from Formulae (24) and (33) is no longer applicable.

6 Conclusions

A receiver-spoofer is a highly covert and hazardous GNSS navigation spoofing attack method. In this paper, the influencing parameters of spoofing are analyzed, and the results indicate that the spoofing-signal ratio is a critical parameter in a spoofing attack. The lower limits of the spoofing-signal ratio required for successful spoofing under various receiver phase discriminator spacings, carrier phase differences, and code phase differences between authentic signals and spoofing signals are obtained via detailed deduction. Verification via a signal simulation source and an authentic navigation signal proves that the formula for the lower limit is accurate and valid. This finding provides a basis for the future study of anti-spoofing technologies.

Based on this study, parameters such as the frequency difference between authentic signals and spoofing signals and SNR will be investigated to identify a more effective method for spoofing-signal detection and elimination.

Abbreviation

BDS: Beidou Navigation System; CSNC: China Satellite Navigation Conference; GNSS: Global navigation satellite system; GPS: Global positioning system; LSP: Leadership Scholarship Program; NCO: Numeric control oscillator; NRSCC: National Remote Sensing Center of China; SNR: Signal-to-noise ratio

Acknowledgements

The authors would like to thank the reviewers for the very helpful comments.

Funding

This work was supported by the National Natural Science Foundation of China (Grant No. 61571255).

Availability of data and materials

The datasets supporting the conclusions of this article are private, and it came from the Department of Electrical Engineering, Tsinghua University, Beijing, China.

Authors' contributions

Dr. Zhou is the project leader of the ground simulation system for Beidou Navigation System (BDS). Shecompleted the derivation of the main formula and the writing of the main contents of the paper. Dr. Li hasfinished the test verification in this paper. Prof. Lu has given his ideas in Sec. 2. All authors read and approved the final manuscript.

Authors' information

Meng Zhou was born in 1980. She joined Beijing Satellites Navigation Center and has been an engineer since December 2006. Then, she is a PhD candidate in the Department of Electronic Engineering, Tsinghua University, Beijing, China. She has been the project leader of the ground simulation system for Beidou Navigation System (BDS). Her research interests include simulation of satellite navigation system and anti-spoofing technology of satellite navigation system. Hong Li was born in 1981. He received the BS degree (with honors) from Sichuan University, Chengdu, China, in 2004, and the PhD degree (with honors) from Tsinghua University, Beijing, China, in 2009. Then, he joined the Department of Electronic Engineering of Tsinghua University and has been an associate professor since August 2014. He leads the research of GNSS security in the GNSS lab of the department, including spoofing, anti-spoofing, performance evaluation of signals, and the associated signal processing techniques. He has received the Academic Young Talent of Tsinghua University for young faculties, innovation foundation for Young Talents of National Remote Sensing Center of China (NRSCC), Leadership Scholarship Program (LSP) of Committee of 100, several excellent paper awards for young scholars of China Satellite Navigation Conference (CSNC), outstanding PhD graduate award, excellent doctoral dissertation award, and top 10 outstanding graduate students of Tsinghua University. Mingquan Lu was born in 1965. He received the MS degree in Electronic Engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 1993. He joined the Department of Electronic Engineering of Tsinghua University, Beijing, China, in 2003 and is currently a professor and the director of the Institute of Information System. His research interests include signal processing, simulation of satellite navigation system, local area navigation system, and software-defined receiver.

Competing interests

No conflict of interest exists in the submission of this manuscript, and the manuscript is approved by all authors for publication. I would like to declare on behalf of my co-authors that the work described was original research that has not been published previously, and not under consideration for publication elsewhere, in whole or in part. All the authors listed have approved the manuscript that is enclosed.

Publisher's Note

Received: 6 December 2017 Accepted: 30 January 2018
Published online: 17 February 2018

References

1. JS Warner, RG Johnston, A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. J. Secur. Adm (2003)
2. P Papadimitratos, A Jovanovic, *Protection and fundamental vulnerability of GNSS* (IWSSC, Toulouse, 2008)
3. T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O. Hanlon and P. M. Kintner, Assessing the spoofing threat: development of a portable GPS civilian spoofer, in *Institute of Navigation GNSS (ION GNSS 2008)*, pp. 2314–25,(Savanna, GA, 2008).
4. Shepard D, Humphreys T, Characterization of receiver response to a spoofing attack. *Proceedings of. ION GNSS 2011*, pp.2608–18, (Portland, OR, 2011).
5. T. Humphreys, P. Kintner, Jr., M. Psiaki, B. Ledvina, and B. O'Hanlon, *Assessing the spoofing threat* (GPS World, 20(28),2009).
6. D. P. Shepard, T. E. Humphreys, and A. A. Fansler, Going up against time: the power grid's vulnerability to GPS spoofing attacks. GPS World. Vol.22, pp.34–38, (2012).
7. D. Shepard, J. Bhatti, and T. Humphreys, *Drone hack: spoofing attack demonstration on a civilian unmanned aerial vehicle*, GPS World, Vol.23, pp. 30–.33. (2012).
8. J. A. Bhatti, T. E. Humphreys, Covert control of surface vessels via unpredictable civil GPS signals, available online at http://radionavlab.ae.utexas.edu/publications/375-covert-control-of-surface-vessels-via-counterfeit-civil-gps-signals, 2014.
9. A Jafarnia-Jahromi, A Broumandan, J Nielsen, G Lachapelle, Pre-despreading authenticity verification for GPS L1 C/a signals. Navigation **61**(1), 1–11 (2014)
10. P. Levin, D. De Lorenzo, P. Enge, and S. Lo, *Authenticating a signal based on an unknown component thereof*, (U.S. Patent No. 7,969,354B2, 2011).
11. BW O'Hanlon, ML Psiaki, JA Bhatti, DP Shepard, TE Humphreys, Real-time GPS spoofing detection via correlation of encrypted signals. Navigation **60**(4), 267–78 (2013)
12. C. Tanil, S. Khanafseh, and B. Pervan, GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory, in *Proc. ION GNSS+*, (Tampa, FL, 2015).
13. M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, GNSS spoofing detection using high-frequency antenna motion and carrier-phase data, in *Proc. of the International Technical Meeting of the Satellite Division of the Institute of Navigation Conference ION GNSS+*, (Nashville, TN, 2013), pp. 2949–91.
14. A Alaqeeli, J Starzyk, F Van Grass, in *Proceedings of the 2003 International Symposium on Circuits and Systems, Vol.4*. Real-time acquisition and tracking for GPS receivers (2003)
15. Meng Zhou, Ying Liu, Lin Xie, Hong Li, Mingquan Lu, Peng Liu, Performance Analysis of Spoofing-signal Ratio for Receiver-Spoofer. In *Proceedings of the 2017 International Technical Meeting of The Institute of Navigation*(ION GNSS 2011), (Monterey, California, 2017), pp. 898–911.