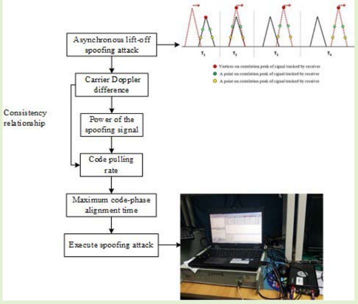
Asynchronous Lift-Off Spoofing on Satellite Navigation Receivers in the Signal Tracking Stage

Yangjun Gao, Zhiwei Lv, and Lundong Zhang

***Abstract*—As Global Navigation Satellite System (GNSS) spoofing techniques are highly stealthy and pose a tremendous risk to targets using GNSS technology, studies on GNSS spoofing techniques have been in the spotlight. If the accurate position and velocity of the target receiver can be obtained, the target receiver can be covertly spoofed during the signal tracking stage using synchronous lift-off spoofing. However, it is often difficult to accurately obtain the position and velocity of a target in real GNSS spoofing scenarios. To address this problem, To study the effects of spoofing signals' power (relative to the real signal), code pulling rate, carrier Doppler shift, initial code phase difference, and carrier phase difference on the efficacy of spoofing, the intrusion of receiver's signal tracking loop by spoofing signals is mathematically modeled. Based on the model, an asynchronous lift-off spoofing for GNSS receivers in the signal tracking stage is proposed. Theoretical analysis and experimental results show that the new method resulted in stable Doppler frequency variations, short fluctuations in carrier-to-noise ratio (C/N) and signal lock time, and gentle changes to the receiver's 3D Earth-Centered Earth Fixed (ECEF) coordinates, when the target's position and velocity were approximately known during the intrusion period. The proposed spoofing method is highly feasible and could expand the scope of applicability of lift-off spoofing.**


Asynchronous lift-off spoofing attack
Carrier Doppler difference
Power of the spoofing signal
Code pulling rate
Maximum code-phase alignment time
Execute spoofing attack
Consistency relationship
T_1
T_2
T_3
T_4
Vertices on correlation peak of signal tracked by receiver
A point on correlation peak of signal tracked by receiver
A point on correlation peak of signal tracked by receiver

***Index Terms*—Asynchronous, satellite navigation, lift-off spoofing, signal tracking stage, spoofing signal, *CLC number: TN972 Document code: A*.**

I. Introduction

As GLOBAL navigation satellite system (GNSS) technology has deeply penetrated many aspects of civilian and military field, satellite navigation signals have certain vulnerabilities [1], although there are many ways to detect spoofing [2], currently more effective anti-spoofing techniques include detection technology based on signal power, navigation message comparison technology, external speed information based spoofing detection technology and external location information based spoofing detection technology. Spoofed GNSS signals could cause disastrous outcomes providing erroneous positioning solutions. Therefore, spoofing have become a severe threat to GNSS technology [3]. Spoofing interference is implemented for the timing receiver in the infrastructure, and the timing synchronization error is introduced to destroy the system time synchronization, thereby paralyzing its communication and power systems [4]. Humphreys also provided some spoofing data sets for experiments [5]. For example, timing receivers are used to provide timing for synchronous phasor measurement units (PMUs). Tests have shown that GNSS spoofers may force PMUs to violate standards [6]. Ever since the U.S. Department of Transportation reported the threat of GNSS spoofing in 2001, spoofing have become a major military concern for many countries, and studies on GNSS interference techniques have been in the spotlight [7].

Spoofing are performed by generating signals that strongly resemble genuine GNSS signals, or by repeating real GNSS signals. Target receiver mistakes the spoofing signal for a real signal, and tracks this signal, thereby outputting either erroneous positioning solutions or no information [8]. Spoofing carry the greatest potential for damage among all GNSS interference techniques [9].

In an actual GNSS spoofing scenario, target receiver is usually infected during signal tracking stage [10]. "Jam-and-spoof" approach is an effective method for implementing spoofing, but it is easily recognized, and in such a case,

Manuscript received March 1, 2020; revised March 27, 2020; accepted March 27, 2020. Date of publication March 31, 2020; date of current version July 6, 2020. The associate editor coordinating the review of this article and approving it for publication was Dr. Shyqyri Haxha. *(Corresponding author: Zhiwei Lv.)*

The authors are with Information Engineering University, Zhengzhou 450001, China (e-mail: 951242669@qq.com; lvzhiwei@sina.com; zhangldxd@163.com).

Digital Object Identifier 10.1109/JSEN.2020.2984525

the target simply employs other ways to navigate [11]. However, one could surreptitiously perform a synchronous "lift-off" spoofing on a receiver during signal tracking stage, if one accurately knows the position and velocity of the target receiver. Lift-off spoofing prevent the receiver from losing lock, which allows to remain concealed [12]. Since lift-off spoofing has become an important direction for the development of spoofing techniques, it is of practical importance to study how covert spoofing could be executed on target receivers during tracking stage [13].

In summary, most spoofing may be categorized as intermediate spoofing [14], which are also known as lift-off spoofing [9]. Lift-off spoofing vary in terms of code pulling rates, carrier Doppler shift, and spoofing signal's power relative to the genuine signal, and this gives each approach a different set of strengths and weaknesses. Furthermore, one requires accurate information about the position and velocity of the targeted receiver's antenna phase center to successfully execute covert lift-off spoofing.

It is often difficult to obtain accurate information about a spoofing target in actual GNSS spoofing scenarios. To address this problem, we mathematically modeled the intrusion of receiver's signal tracking loop by a spoofing signal, to study the effects of spoofing signal's power (relative to the real signal), code pulling rate, carrier Doppler shift, initial code phase difference and carrier phase difference on the efficacy of spoofing. On this basis, an asynchronous lift-off spoofing for GNSS receivers during signal tracking stage is proposed. Theoretically and experimentally, when the target's position and velocity are approximately known during the intrusion period, new method outperforms the conventional synchronous lift-off spoofing as follows: (1) the variations in signal Doppler frequency are much more stable, (2) the fluctuations in carrier-to-noise ratio (C/N) are much shorter, (3) the signal lock time spans are shorter, and (4) the resulting changes in the receiver's 3D Earth-Centered Earth-Fixed (ECEF) coordinates are much more gentle.

II. Modeling Spoofing in the Signal Tracking Stage

When the receiver is tracking a genuine signal, the carrier frequency and code phase of the spoofing signal must match those of the genuine signal; otherwise, even very powerful spoofing signals cannot take over the receiver [15].

The following complex-number signal model represents a target receiver that is simultaneously receiving spoofing and genuine signals during the signal tracking stage:

$$\begin{aligned} r(nT_s) = & \sum_{h=J^a} \sqrt{P_h^a} D_h^a(nT_s - \tau_h^a) c_h^a(nT_s - \tau_h^a) e^{j\varphi_h^a + j2\pi f_h^a nT_s} \\ & + \sum_{m=J^s} \sqrt{P_m^s} D_m^s(nT_s - \tau_m^s) c_m^s(nT_s - \tau_m^s) \\ & \times e^{j\varphi_m^s + j2\pi f_m^s nT_s} + \eta(nT_s) \end{aligned} \tag{1}$$

Here, P is the received signal power; D is the navigation message; c is the pseudorandom noise (PRN) code sequence; T_s is the sampling interval; φ, f, and τ are the carrier phase, carrier Doppler frequency, and code phase, respectively; $\eta(nT_s)$ is additive Gaussian white noise with a zero average and variance of σ_n^2. The h and m subscripts indicate whether the signal being received is genuine or spoofing, whereas J^a and J^s are the real and spoofing signal sets respectively, where a and s subscripts indicate the received real signals and spoofing signals respectively. In GNSS, if each bit of the navigation message (D) is 20 ms long and the coherent integration time is constant, the effects of D on the calculations are then negligible. In civil GNSS codes, the ephemeris of D is repeated once every 30 s and updated once every 2 h, whereas the almanac is repeated once every 12.5 min and renewed every week. Once the almanac and ephemeris have been obtained, the next bit of data may be predicted [16].

The coherent integration of the l-th signal may be expressed as:

$$u_l\left[\tilde{f}_l, \tilde{\tau}_l, k\right] = \frac{1}{N} \sum_{n=(k-1)N+1}^{kN} r(nT_s) c_l(nT_s - \tilde{\tau}_l) e^{-j2\pi \tilde{f}_l nT_s} \tag{2}$$

In (2), $\tilde{f}_l$ and $\tilde{\tau}_l$ are the estimated delays in the carrier Doppler frequency and code phase, k is the index of the integration interval, and N is the coherent integration interval. Because the coherent integration time is usually 1 ms, which is much shorter than the data bit length of D (20 ms), the effects of D on the correlation may be excluded. Therefore, l-th real signal represents the real signal of the l-th channel, the correlation between the l-th real signal and the corresponding locally generated C/A code and carrier frequency is given by:

$$\begin{aligned} & \frac{1}{N} \sum_{n=(k-1)N+1}^{kN} \left(\sqrt{P_l^a} \left[c_l^a(nT_s - \tau_l^a) e^{j\varphi_l^a + j2\pi f_l^a nT_s} + \eta(nT_s) \right] \right. \\ & \quad \left. \times\ c_l(nT_s - \tilde{\tau}_l) e^{-j2\pi \tilde{f}_l nT_s} \right) \\ & = \frac{1}{N} \sum_{n=(k-1)N+1}^{kN} \left(\sqrt{P_l^a} c_l^a(nT_s - \tau_l^a) \right. \\ & \quad \left. \times\ c_l(nT_s - \tilde{\tau}_l) e^{j\Delta\varphi_{l,0}^{a,l} + j2\pi \Delta f_l^a nT_s} \right) + \bar{\eta}\left[nT_s\right] \end{aligned} \tag{3}$$

In (3), $\Delta\varphi_{l,0}^{a,l}$ is the difference between the carrier phases of the real and locally generated signals at $k = 0$, and $\Delta f_l^{a,l}$ is the difference in carrier frequency between the real and local signals.

When the receiver is in signal tracking phase, the local carrier frequency and code phase may be assumed to be identical to those of the real signal (i.e., $\Delta f_l^{a,l} \approx 0$, $\tau_l^a = \tilde{\tau}_l$). Equation (3) may then be simplified to:

$$\begin{aligned} u_l\left[k\right] \simeq & \sqrt{P_l^a} R(\Delta\tau_l^{a,l}) \sin c(\Delta f_l^{a,l} NT_s) \\ & \times e^{j\pi \Delta f_l^{a,l}[(2k-1)N-1]T_s + j\Delta\varphi_{l,0}^{a,l}} \\ & + \sqrt{P_l^s} R(\Delta\tau_l^{s,l}) \sin c(\Delta f_l^{s,l} NT_s) \\ & \times e^{j\pi \Delta f_l^{s,l}[(2k-1)N-1]T_s + j\Delta\varphi_{l,0}^{s,l}} + \bar{\eta}\left[k\right] \end{aligned} \tag{4}$$

In (4), $\Delta f_l^{s,l}$, $\Delta\varphi_{l,0}^{s,l}$, and $\Delta\tau_l^{s,l}$ are the carrier frequency difference, carrier phase difference, and code phase difference between the spoofing and local signal, respectively; $\Delta\tau_l^{a,l}$ is the code phase difference between the real signal and local signal; $R(\Delta\tau_l^{a,l})$ is the correlation between real and local signals with the same PRN but different code phases; $\Delta\tau_l^{s,l}$ is the code phase difference between the spoofing and local signal, and $R(\Delta\tau_l^{s,l})$ is the correlation between spoofing and local signals with the same PRN but different code phases.

The carrier frequency, carrier phase, and code phase of the genuine signal may be assumed to be aligned, i.e., $\Delta f_l^{a,l}$, $\Delta\tau_l^{a,l}$, and $\Delta\varphi_{l,0}^{a,l}$ are all close or equal to zero. Therefore, the correlation between the output signal (which contains the l-th real signal and l-th spoofing signal) and the output of the l-th local signal may be simplified to [16]:

$$u_l[k] = \sqrt{P_l^s} R(\Delta\tau_l^{a,s}) \sin c(\Delta f_l^{a,l} N T_s) \times e^{j\pi \Delta f_l^{a,s}[(2k-1)N-1]T_s + j\Delta\varphi_{l,0}^{a,s}} + \sqrt{P_l^a} + \bar{\eta}[k] \quad (5)$$

In (5), $\Delta f_l^{a,s}$, $\Delta\tau_l^{a,s}$, and $\Delta\varphi_l^{a,s}$ are the carrier frequency, code phase, and carrier phase differences between the genuine satellite and spoofing signal, respectively.

The quantitative requirements for a successful GNSS spoofing have been examined. Initially, the spoofing signal must be at least 2 dB more powerful than the real signal, so that the receiver seamlessly locks onto the spoofing signal; this deviation is also low enough not to be detected by power based spoofing countermeasures. Furthermore, spoofing signal's chip offsets should be less than 75 ns and 500 m to circumvent time and position based spoofing countermeasures [17]. Moreover, a target is successfully spoofed if each spoofing signal: (1) shifts 2 μs relative to the real signal, and (2) is at least 10 dB more powerful than the corresponding authentic signal [15]. Additionally, the spoofing signal simply has to be more powerful than the authentic signal after Doppler loses to take over the receiver's pseudo-noise (PN) code-tracking loop and spoofs a GNSS receiver that was originally tracking a genuine satellite signal. However, given a limited coherent accumulation time, one must find a balance between minimum spoofing-signal power and maximum synchronization time, which are contradictory requirements. For a typical GNSS receiver, the spoofing signal only needs to be 4 dB more powerful than the authentic signal, i.e., it takes a maximum of 50 min for spoofing GNSS signal to take over a GNSS receiver that was tracking a real signal [18]. The critical jamming-to-signal (J/S) ratio for a spoofing signal to disrupt a GNSS receiver that is constantly tracking a GNSS signal is 24 dB [19]. Concerning the covert spoofing: (1) The spoofer's power advantage must be no more than 12 dB, (2) the spoofing signal must have the same frequency as the real signal, and (3) a constant carrier-to-noise ratio (C/N) must be maintained throughout the spoofing [20]. Additionally, the maximum Doppler shift that can be tolerated by a target receiver that is constantly tracking a signal is approximately 50 Hz.

Spoofing methods have been proposed. Firstly, two intermediate spoofing strategies are reported. In the first strategy, the spoofing signal is locked to the carrier phase; in the second strategy, the code phase is kept consistent with the carrier phase. Although both strategies can drag the code phase away from the genuine signal, the first strategy disrupts the consistency between the carrier phase and code phase, which allows spoofing to be detected by carrier-code frequency consistency checks. The second strategy leads to oscillations in the output of phase-locked loop (PLL), which could also alert the receiver to the spoofing. Therefore, the spoofing strategy should be selected according to the receiver's characteristics [14]. In 2014, Ma *et al.* showed that, once the spoofing signal has been accepted by the receiver's navigation solver, the receiver is gradually pulled towards a predetermined region using forged ephemeris data and accumulated small errors over time; this allows the spoofing to elude detection by receiver autonomous integrity monitoring (RAIM) methods [21]. However, they did not quantitatively analyzed the effects of the J/S ratio on the receiver, nor did they check whether these effects could lead to anomalies in the receiver's output. Experiments from Wang *et al.* showed that the receiver positioning solutions can be scrambled by direct intrusion, where the spoofing signal's power is adjusted in a rational manner. However, they did not succeed in tricking the receiver to output a predetermined positioning solution. Using a jamming-assisted spoofing method, they successfully rendered the receiver output the preset positioning solution, thereby demonstrating the feasibility of GPS receiver spoofing [22]. In 2019, Peng *et al.* studied to what degree intermediate spoofing are affected by the relative powers, carrier frequencies, and code phases of the genuine and spoofing signals, when it is not possible to obtain accurate information about the target. However, they did not analyzed the mechanistic aspects of these effects in-depth [23].

The comparison table with all summarized parameters for different lift-off is provided below:

TABLE I
COMPARISON WITH ALL SUMMARIZED PARAMETERS FOR DIFFERENT LIFT-OFF SPOOFING

Spoofing method	Doppler frequency fixed	Consistent	Synchronous or asynchronous
A	Fixed	Inconsistent	Synchronous
B	Fixed	Inconsistent	Asynchronous
C	Fixed	consistent	Synchronous
D	Fixed	consistent	Asynchronous
E	Not fixed	Inconsistent	Synchronous
F	Not fixed	Inconsistent	Asynchronous
G	Not fixed	consistent	Synchronous
H	Not fixed	consistent	Asynchronous

III. NEW SPOOFING METHOD

In real spoofing scenario, the targeted GNSS receiver is not cooperative, which means that spoofers do not know the internal parameters of the target receiver and is very difficult to accurately obtain its antenna's position and velocity. Therefore, we proposed an effective and feasible method to perform a spoofing when the spoofer obtain the position and velocity of the target receiver's antenna approximately.

A. Overall Design

The method proposed here is an asynchronous lift-off spoofing. This method's procedures are described below. The red

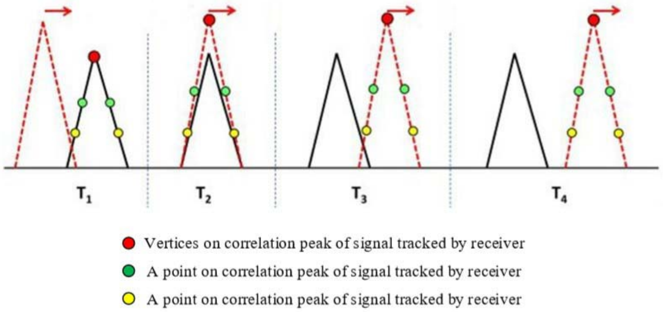

T₁
T₂
T₃
T₄
● Vertices on correlation peak of signal tracked by receiver
● A point on correlation peak of signal tracked by receiver
● A point on correlation peak of signal tracked by receiver

Fig. 1. Processes of an asynchronous lift-off spoofing.

dots in Fig. 1 indicate the vertices on correlation peak of signal tracked by receiver, and the green and yellow dots are both points on correlation peak of signal tracked by receiver. After the spoofer first obtains the approximate coordinates of the receiver's antenna phase center (Fig. 1), it produces a spoofing signal (red signal) that is more powerful than the genuine signal (black signal), and the spoofing signal gradually shifts towards the correlation peak of the genuine signal (T_1). At T_2, the spoofing and genuine signals are synchronous; the code phases of the spoofing and genuine signals are aligned (T_2). The spoofing signal then uses its advantage in power to take over the targeted GNSS receiver's pseudo-code loop, and it continues shifting until the code phases of genuine and spoofing signals disassociate from each other (T_3). Finally, the spoofing signal then continues to maintain the existing power (T_4).

In a realistic scenario, the key factors for determining the success of the spoofing are: the power of the spoofing signal, code pulling rate, carrier frequency difference between spoofing and genuine signals, consistency between Doppler shifts of spoofing and genuine signals, and code phase and carrier phase differences between spoofing and genuine signal. In the following, we thoroughly analyze the effects of the aforementioned factors on the spoofing process from a mechanistic perspective. We then propose an improved spoofing on this basis.

B. Power of the Spoofing Signal

In an asynchronous spoofing, it is important to control the power of the spoofing signal. If the power is too high, the spoofing may be detected by the receiver's power-based spoofing countermeasures, which reduces its effectiveness. If the power is too low, the spoofing signal does not succeed in taking over the receiver's tracking loop. The frequency difference, $\Delta f_l^{s,l}$, attenuates the coherent integration amplitude by $\sin c^2(\Delta f_l^{s,l} T_{coh})$, where $T_{coh} = NT_s$ is the coherent integration time. It has been demonstrated that the power of the spoofing signal's correlation peak must be greater than that of the genuine signal after Doppler losses, if the spoofing signal succeeds in taking over the receiver's tracking loop; this defines the spoofing signal's minimum power [18]. However, the spoofing signal's code pulling rate is often too large, which makes it less probable for the spoofing to succeed. By increasing the spoofing signal's power, the correlation between the spoofing and local signal could be stronger than the correlation peak between the local and genuine signal, even in the presence of a code phase difference between the PN codes of the spoofing and local signals. This allows the spoofing signal to take over the tracking loop, thereby increasing the spoofing 's probability of success. In practice, if the relationship between the spoofing signal's code Doppler and carrier Doppler is consistent, an increase in code pulling rate raises the carrier Doppler, thereby enhancing the spoofing signal's Doppler losses. Normally, the spoofing signal could not take over the code tracking loop if it becomes too weak. In this case, one must increase the spoofing signal's power to some extent to rise the spoofing probability of success.

C. Code Pulling Rate

A spoofing signal's code pulling rate is defined as the difference between the code rates of spoofing and genuine signals (typically a positive value). Based on the periodicity of the PN code, one may set a code pulling rate for the spoofing signal, which could compel the spoofing signal's code phase to be adjusted to that of the genuine signal after some time, allowing the spoofing signal to carry off the receiver's code tracking loop. However, when setting the code pulling rate, one should consider these: (1) The pull-in range of a typical GNSS receiver's tracking loop is 0.5 cps [24]. If one accounts for the code phase's measurement errors and dynamic stress errors, the relative offset of the spoofing signal's code phase within one coherent integration must not exceed 0.5 cps. Therefore, if the coherent integration time is 1 ms, the code pulling rate must be 500 cps or less. (2) Because the target receiver may use code Doppler and carrier Doppler consistency checks like the code carrier phase consistency (CCPC), the carrier Doppler must be taken into consideration when selecting the code pulling rate [14]. (3) If each interval of a PN code contains n chips, and υ is the spoofing signal's code pulling rate, the maximum alignment time between the code phases of genuine and spoofing signals is then $t_s = n/\upsilon$. Consequently, increasing the code pulling rate shortens the maximum alignment time. If one wishes to further decrease alignment time, the spoofing signal's power may increase to facilitate higher code pulling rates, as mentioned in Section IIIB. (4) The code pulling rate should not exceed the loop bandwidth of the delay lock loop (DLL), because this makes it difficult for the code loop to lock onto the spoofing signal.

D. Designing a Relationship Between the Code Doppler and Carrier Doppler

There are two methods by which a spoofing signal could take over a receive's tracking points after it is aligned with the correlation peak of the genuine signal. In the first method, the spoofing signal maintains the ratio between the carrier Doppler frequency ($f_{Doppler}^{carrier}$) and code Doppler frequency ($f_{Doppler}^{code}$). Because Doppler shifts are caused by the satellite-receiver relative motions, $f_{Doppler}^{carrier}$ and $f_{Doppler}^{code}$ should be related by $f_{Doppler}^{code} = f_{Doppler}^{carrier}/1540$ in L1 C/A navigation signals. Based on (5), the output of the correlation integral is [16]:

$$u_l\,[k] = \sqrt{P_l^s}\,R(-\frac{\Delta f_l^{a,s'}}{2f_l}(kNT_s)^2)\sin c(\Delta f_l^{a,l}NT_s)e^{j\,\Delta\varphi_l^{a,s}[k]} + \sqrt{P_l^a} + \bar{\eta}\,[k] \quad (6)$$

In (6), $\Delta f_l^{a,s'}$ is the change rate of the carrier frequency difference between the real satellite and spoofing signal. Because $\Delta f_l^{a,s} \neq 0$, the output amplitude of the correlation integral fluctuates, depending on the relative powers of the spoofing and real signal and the change rate of their carrier frequency difference; this could lead to the spoofing detection.

In the second method, a fixed carrier Doppler frequency is used in the spoofing signal; the Doppler frequencies of the spoofing and genuine signal are kept constant for a short period of time, whereas the spoofing signal's code phase is varied. In this case, the carrier frequencies of the spoofing and genuine signals are identical, i.e., $\Delta f_l^{a,s} \simeq 0$. However, their code phase difference, $\Delta\tau_l^{a,s}$, is not zero, i.e., $\Delta\tau_l^{a,s} \neq 0$. The output of the coherent integration may then be expressed as:

$$u_l[k] \simeq \sqrt{P_l^s}\,R(\Delta\tau_l^{a,s})\sin c(\Delta f_l^{a,l}NT_s)e^{j\,\Delta\varphi_{l,0}^{a,s}} + \sqrt{P_l^a} + \bar{\eta}[k] \quad (7)$$

Because the carrier phase difference between real and spoofing signals, $\Delta\varphi_{l,0}^{a,s}$, is invariant, the first term in (7) remains invariant, too. Therefore, the correlation amplitude does not fluctuate.

In this type of spoofing, the spoofing signal's Doppler shift is fixed at the correlation peak between the genuine and spoofing signal. Therefore, the targeted receiver is not likely to lose its lock, nor is it likely to detect the spoofing signal based on correlator fluctuations. However, the spoofing signal can still be detected by consistency checks between code velocity and Doppler shift.

Based on the takeover methods described above, one may surmise that the ideal takeover method would satisfy the consistency relationship between the code Doppler and carrier Doppler ($f_{Doppler}^{code} = f_{Doppler}^{carrier}/1540$) while ensuring that spoofing and genuine signals have the same carrier frequency. However, if the $f_{Doppler}^{carrier}$ of the spoofing signal must remain consistent with $f_{Doppler}^{code}$, while being identical to that of the genuine signal, the spoofing signal's code pulling rate will then be zero, which makes it impossible for the spoofing signal to take over the correlation peak. To resolve this, we proposed a novel and feasible takeover method.

The new takeover method maintains $f_{Doppler}^{code} = f_{Doppler}^{carrier}/1540$, while ensuring that the receiver's carrier frequency difference, $\Delta f_l^{a,s}$, is maximally stable during the takeover process. Let $\Delta f_l^{a,s'}$=0. Equation (6) may then be expressed as:

$$u_l\,[k] = \sqrt{P_l^s}\sin c(\Delta f_l^{a,l}NT_s)e^{j\,\Delta\varphi_{l,0}^{a,s}} + \sqrt{P_l^a} + \bar{\eta}\,[k] \quad (8)$$

Because $\Delta f_l^{a,l}$ and $\Delta\varphi_{l,0}^{a,s}$ are invariant, the output of $u_l\,[k]$ becomes a non-fluctuating fixed value. Therefore, the carrier frequency difference, $\Delta f_l^{a,s}$, should become a fixed value.

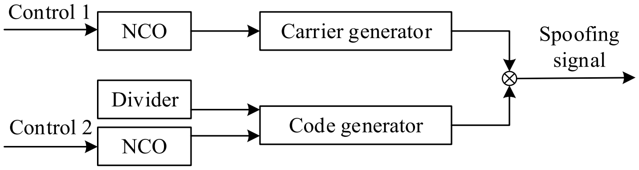


Fig. 2. Method for ensuring a fixed $\Delta f_l^{a,l}$ value while maintaining $f_{Doppler}^{code} = f_{Doppler}^{carrier}/1540$.

The method by which the spoofing signal is produced and controlled is illustrated below:

$D_l\,[k] = u_l^2\,[k]$ was used as a metric to highlight the changes in output $u_l\,[k]$

$$\begin{aligned} D_l\,[k] &= u_l^2\,[k] \\ &= (\sqrt{P_l^s}\sin c(\Delta f_l^{a,l}NT_s)e^{j\,\Delta\varphi_{l,0}^{a,s}} + \sqrt{P_l^a} + \bar{\eta}\,[k])^2 \\ &= P_l^a + P_l^s \sin c^2(\Delta f_l^{a,l}NT_s) + 2\sqrt{P_l^a P_l^s}\sin c \\ &\quad \times (\Delta f_l^{a,l}NT_s)\cos c(\Delta\varphi_l^{a,s}\,[k]) + \tilde{\eta}\,[k] \end{aligned} \quad (9)$$

In (9), $\tilde{\eta}\,[k]$ is the noise in $D_l\,[k]$.

Based on the findings of [23], the PLL and DLL locks of a target receiver depend on the carrier frequency difference between spoofing and genuine signals; the greater the value of $\Delta f_l^{a,s}$ is, the easier it is for the target receiver to lose its lock [23].

IV. Experimental Analysis

A. Calculation of Parameters

The spoofing's parameters described in Section III are calculated as follows:

If the maximum velocity offset that is acceptable for the target receiver is $\upsilon_{\max}$, the corresponding maximum carrier Doppler, $f_{\max}$, is:

$$f_{\max} = \frac{\upsilon_{\max}}{c} f_l \quad (10)$$

The carrier frequency difference between the spoofing and real signal, $\Delta f_l^{s,a}$, must then satisfy:

$$|\Delta f_l^{s,a}| \leq f_{\max} \quad (11)$$

Because the attenuation of the coherent integration amplitude due to $\Delta f_l^{s,a}$ is $\sin c^2(\Delta f_l^{s,a} T_{coh})$, the spoofing signal's power, P_l^s, should satisfy:

$$P_l^a < P_l^s \sin c^2(\pi\,\Delta f_l^{s,a} T_{coh}) < P_{\max} \quad (12)$$

where P_{max} is the power-based spoof detection threshold of the target receiver.

If $\Delta f_l^{s,a}$ satisfies (11) and (12), the code pulling rate, $\Delta C_l^{s,a}$, may then be derived from the ratio between the spoofing signal's carrier Doppler frequency and that of the PN code, as shown below:

$$\Delta C_l^{s,a} = \frac{\Delta f_l^{s,a}}{1540} \quad (13)$$

$\Delta C_l^{s,a}$ must be checked whether it is smaller than the loop bandwidth of the receiver's code loop, or not. Otherwise, $\Delta f_l^{s,a}$ must be reduced until $\Delta C_l^{s,a}$ is smaller than the

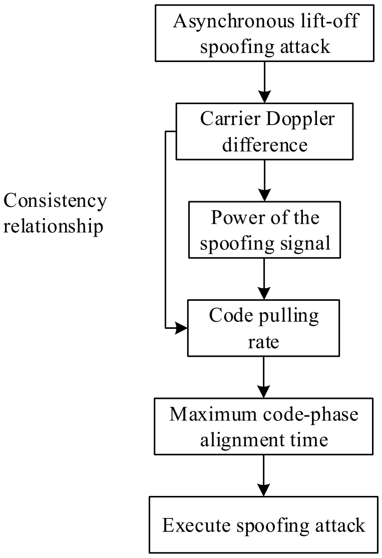

Asynchronous lift-off spoofing attack
Carrier Doppler difference
Consistency relationship
Power of the spoofing signal
Code pulling rate
Maximum code-phase alignment time
Execute spoofing attack

Fig. 3. Calculations of the proposed spoofing.

loop bandwidth. The spoofing signal's maximum synchronization time is then given by:

$$t_c = \frac{1023}{\Delta C_l^{s,a}} \tag{14}$$

In most cases, spoofing signal immediately controls the tracking loop once it has synchronized with the real signal and pulls the positioning solution away from the receiver's actual position. Although t_c might not be the actual length of time required to complete the synchronization process, it can still be used as a metric for the spoofing's speed.

The spoofing signal's parameters are calculated for the proposed spoofing as follows:

B. Experimental Environment

An experimental platform to simulate a realistic spoofing scenario was constructed, as shown in the figure below. This platform consisted of a GNSS signal simulator, host-computer control software, test receiver, and receiver antenna. The GNSS signal simulator was utilized to generate genuine and spoofing signals. The host computer has employed to control the code phase difference (m), carrier phase difference (m), code velocity (m/s), carrier-phase velocity (m/s), relative power gain (dB), and power increase/attenuation rate (dB/s), by writing the appropriate commands in its control software. The SV number, number of satellites and signal power of the genuine and spoofing signals were set using the host computer.

Here, a Septentrio PolaRx5 receiver was deployed as the target receiver, which had the ability to resist interference and detect spoofing to a certain extent, and would tolerate a maximum velocity offset of 10 m/s in the navigation message. This corresponded to a maximum carrier Doppler difference of 52.514 Hz between spoofing and real signal for GNSS L1 signals in formula 10, and a code pulling rate of 0.0341 Hz (i.e., 10 m/s) in formula 13. Furthermore, the spoofing signal's power advantage over the genuine signal should be set bigger than 0.392 dB in formula 12, and the maximum code-phase alignment time was 500 min in formula 14.

Fig. 4. Photograph of the experimental platform.

Two experiments were designed to compare new spoofing to a conventional one with a fixed Doppler frequency, in terms of spoofing efficacy. Experiment 1 was performed using the spoofing with a fixed Doppler frequency, whereas Experiment 2 was performed using new spoofing. These experiments were identical in all aspects except for the spoofing method.

1) Spoofing With a Fixed Doppler Frequency: The procedures of Experiment 1 are: (1) The PolaRx5 receiver was cold-started. (2) The signal simulator was used to produce 11 channels of real GPS L1 signal, which were transferred t the receiver through antenna cable. This process was allowed to continue for 5 min. (3) After 5 min, four spoofing signals with the same satellite PRN numbers as genuine signals were injected into the receiver. Each spoofing signal had an initial code phase difference and initial carrier phase difference of −300 m from the genuine signal. The spoofing signal's code velocity differed by 10 m/s from that of the real signal, whereas the spoofing signal's Doppler phase velocity relative to the real signal was maintained at 0 m/s, i.e., the carrier Doppler difference of spoofing and genuine signals was fixed. The spoofing signal's power was 0.4 dB greater than that of the genuine signal and the spoofing signal's code phase increased with a fixed gradient; this process continued for 5 min. The spoofing was then concluded.

Fig. 5 illustrates the changes in the Doppler frequency of two spoofing PRN29 and PRN30 satellite signals with respect to time. When the spoofing signal began to take over the receiver, The Doppler frequency fluctuated dramatically for 70 s during this period, which indicates that the spoofing signal's Doppler frequency was unstable during the transitional intrusion period. This anomaly might be detected by the receiver. Fig. 6 shows the change in the C/N of the spoofing PRN29 and PRN30 satellite signals with respect to time. When the spoofing signals took over the receiver, during this period, the C/N of the PRN29 signal changed by 18.25 dB/Hz, and it fluctuated for approximately 70 s. The C/N of the PRN30 signal changed by 19 dB/Hz, and it also fluctuated for approximately 70 s. The signal anomalies caused by long C/N fluctuation time might be detected by the receiver.

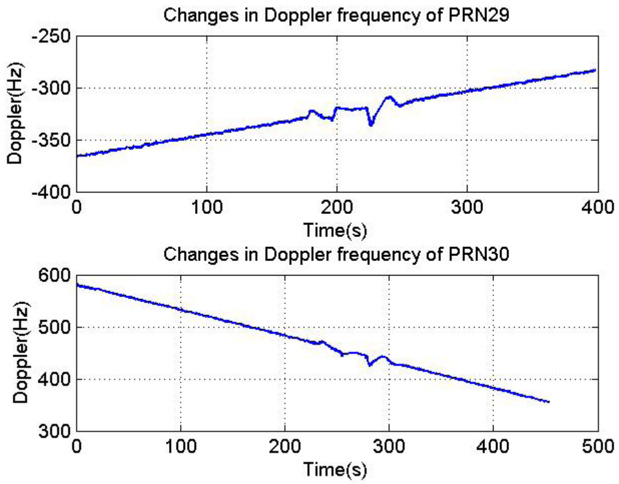


Fig. 5. Changes in satellite signals's Doppler frequency.

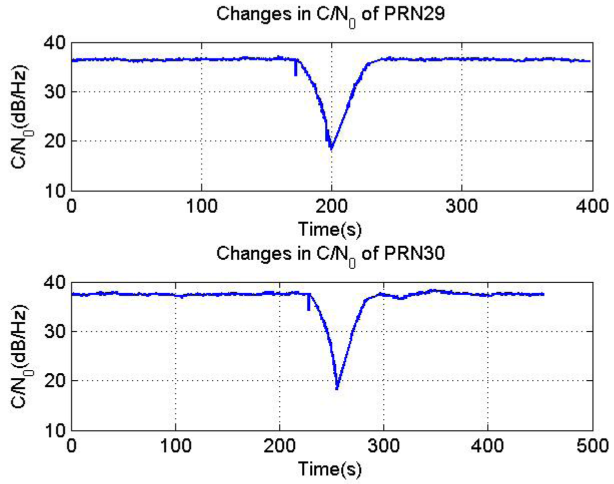


Fig. 6. Changes in satellite signals's carrier-to-noise ratio.

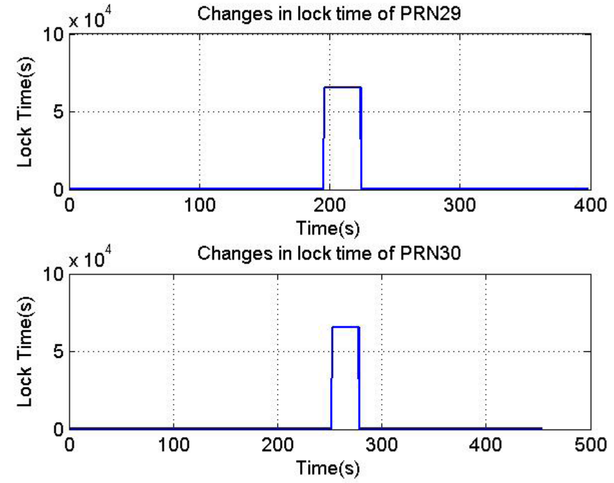


Fig. 7. Changes in the lock time of satellite signals.

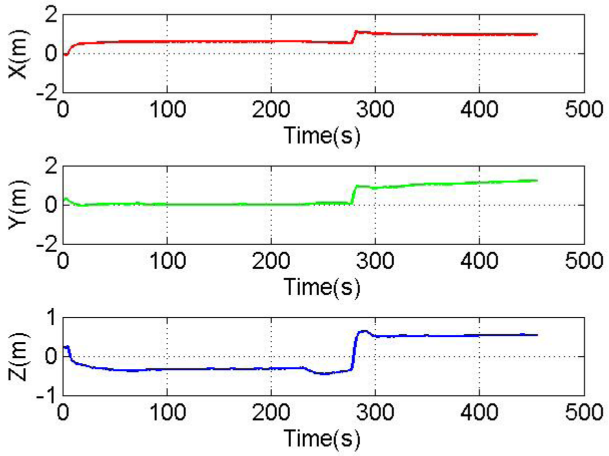


Fig. 8. Changes in the 3D ECEF coordinates of the GNSS receiver.

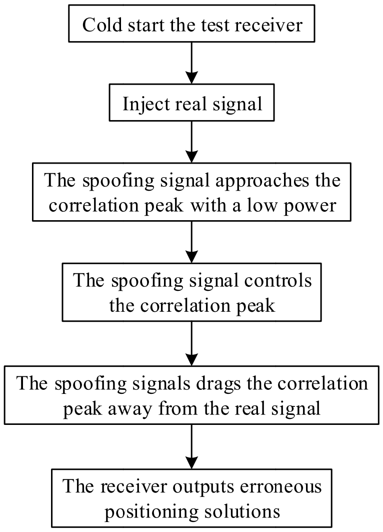
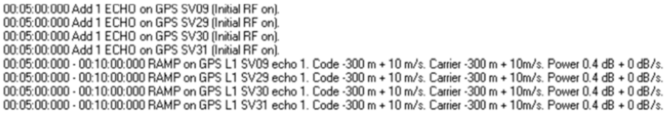

Cold start the test receiver
Inject real signal
The spoofing signal approaches the correlation peak with a low power
The spoofing signal controls the correlation peak
The spoofing signals drags the correlation peak away from the real signal
The receiver outputs erroneous positioning solutions

Fig. 9. Processes of the spoofing schemes.



```
00:05:00:000 Add 1 ECHO on GPS SV09 (Initial RF on).
00:05:00:000 Add 1 ECHO on GPS SV29 (Initial RF on).
00:05:00:000 Add 1 ECHO on GPS SV30 (Initial RF on).
00:05:00:000 Add 1 ECHO on GPS SV31 (Initial RF on).
00:05:00:000 - 00:10:00:000 RAMP on GPS L1 SV09 echo 1. Code -300 m + 10 m/s. Carrier -300 m + 10m/s. Power 0.4 dB + 0 dB/s.
00:05:00:000 - 00:10:00:000 RAMP on GPS L1 SV29 echo 1. Code -300 m + 10 m/s. Carrier -300 m + 10m/s. Power 0.4 dB + 0 dB/s.
00:05:00:000 - 00:10:00:000 RAMP on GPS L1 SV30 echo 1. Code -300 m + 10 m/s. Carrier -300 m + 10m/s. Power 0.4 dB + 0 dB/s.
00:05:00:000 - 00:10:00:000 RAMP on GPS L1 SV31 echo 1. Code -300 m + 10 m/s. Carrier -300 m + 10m/s. Power 0.4 dB + 0 dB/s.
```

Fig. 10. Commands used in Experiment 2.

Fig. 7 illustrates the changes in the spoofing PRN29 and PRN30 satellite signals' lock time with respect to time. When the spoofing signal begins to take over the receiver, During this period, the lock time increased rapidly for a short time, and then met its original value. Therefore, the spoofing signal's lock time fluctuated during the intrusion period. The duration of this fluctuation was 28.4s and 25.9s for the PRN29 and PRN30 signals, respectively. Fig. 8 shows the changes in the receiver's 3D ECEF coordinates with respect to time. From time = 0s to time = 80s, the receiver got a genuine signal and gradually converged to a positioning solution. From time = 80s to time = 277s, the receiver had a stable positioning solution. From time = 277s to time = 300s, the spoofing signal took over the receiver and gradually pulled its positioning solution away from its actual position. The changes in the receiver's position were abrupt during this period. Although the receiver was successfully spoofed, a sudden change in the position solution could have alerted the receiver to the spoofing.

2) New Asynchronous Lift-Off Spoofing: This experiment procedures are: (1) The PolaRx5 receiver was cold-started.

TABLE II
COMPARISON OF EXPERIMENTAL PARAMETERS

Parameter	Experiment 1	Experiment 2 [a]
Code velocity	10m/s	10m/s
Doppler phase velocity	0m/s	10m/s
Power advantage	0.4dB	0.4dB
Initial code phase difference	-300m	-300m
Initial phase difference	-300m	-300m
duration	5min	5min

(2) After the receiver was cold started, we used the signal simulator to produce 11 genuine GNSS L1 signals and attached the antenna to the receiver. This process was allowed to continue for 5 min. (3) After 5 min, four spoofing signals with satellite PRN numbers that were the same as those of the genuine signals were injected into the receiver. The initial code phase difference and initial carrier phase difference between the spoofing and genuine signal were −300 m. The spoofing signal's code velocity differed by 10 m/s from the real signal, whereas the spoofing signal's Doppler phase velocity relative to the real signal was maintained at 10 m/s. The spoofing signal's power was 0.4 dB greater than that of the genuine signal, and the spoofing signal's code phase increased with a fixed gradient; this process continued for 5 min. Subsequently, we concluded the spoofing. The processes of the aforementioned spoofing schemes may be expressed as follows:

The commands we used in Experiment 2 are shown below:

In these commands, "ECHO" initiates the spoofing signal's transmission; "RAMP" defines the initial code phase difference, initial carrier phase difference, initial power gain, and spoofing signal's code velocity relative to the genuine signal, spoofing signal's carrier velocity and power gain/attenuation rate, as well as the command's time of initiation and duration. The comparison table for experiment on Section IV is provided below:

In the following, we analyze the changes in the signal Doppler frequency, C/N, signal lock time, and 3D ECEF coordinates of the test receiver during Experiment 2.

Fig. 11 shows the changes in the Doppler frequency of the spoofing PRN29 and PRN30 satellite signals with respect to time. It is shown that the Doppler frequency varied in a stable manner as a whole, albeit with slight fluctuations when the spoofing signal began to take over the receiver, despite this, these changes were insignificant. Compared to Experiment 1, the spoofing signal's Doppler frequency was much more stable during the transitional intrusion period, and the receiver might not have detected this anomaly. Fig. 12 illustrates the C/N variations of the spoofing PRN29 and PRN30 signals with respect to time. It is shown that the C/Ns of these signals were relatively stable, although fluctuations occurred in one or two instances during the intrusion period, these fluctuations were very short, and the C/Ns immediately returned to their normal value. Compared to the C/N anomaly in Experiment 1, the C/N anomaly in Experiment 2 is more likely to be identified by the receiver as random signal noise rather than a spoofing.

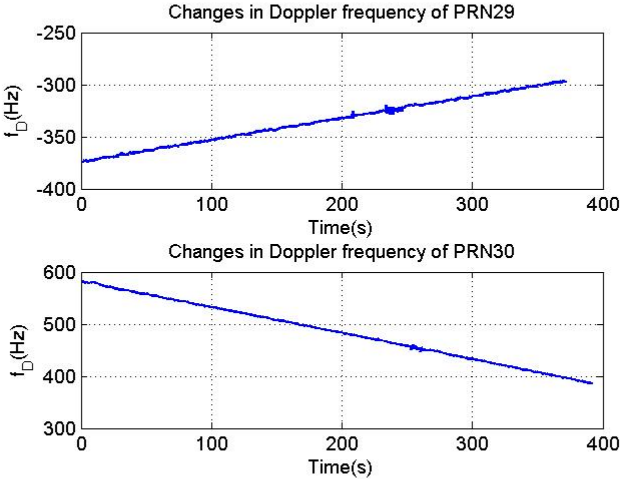


Fig. 11. Changes in satellite signals's Doppler frequency.

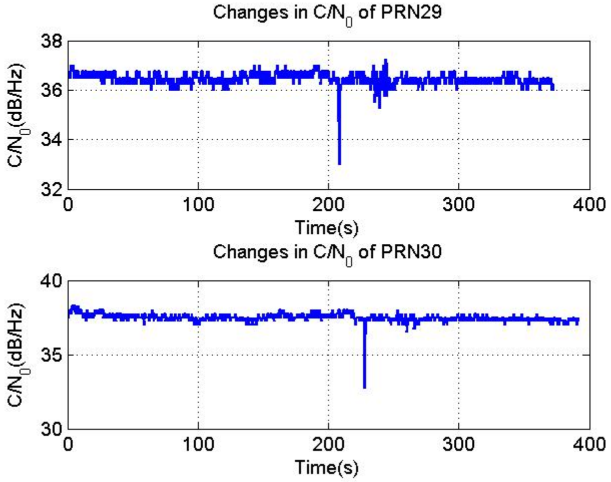


Fig. 12. Changes in satellite signals's carrier-to-noise ratio.

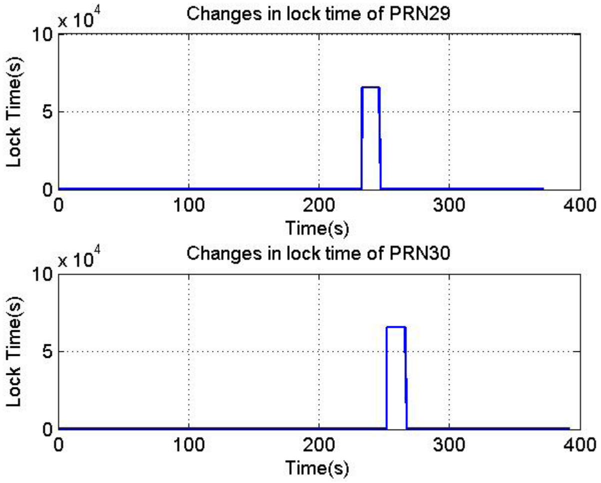


Fig. 13. Changes in the lock time of satellite signals.

Fig. 13 illustrates how the receiver lock time of spoofing PRN29 and PRN30 signals changed with time. A signal's lock time refers to the period where the signal's carrier phase

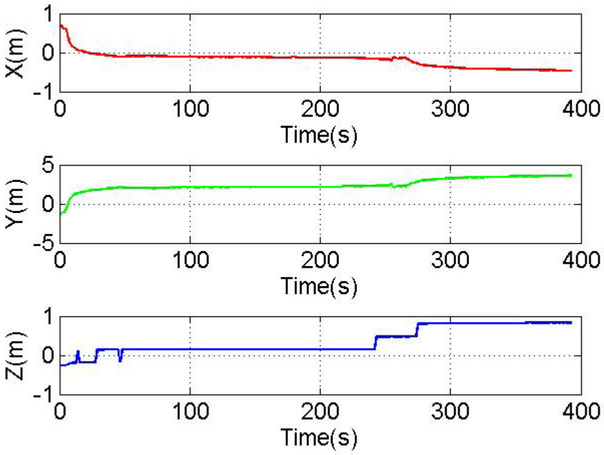


Fig. 14. Changes in the 3D ECEF coordinates of the receiver.

changes continuously. Lock time resets when the PLL begins to lock in a signal or loses lock. When the spoofing signal began to take over the receiver, lock time increased rapidly for a certain amount of time before meeting its original value. Therefore, the spoofing signal's lock time fluctuated during the intrusion period. In Experiment 2, the fluctuations in the lock time of spoofing PRN29 and PRN30 signals were 13.7s and 14.7s long, respectively. Compared to Experiment 1, these fluctuations were shorter by 14.7s and 11.2s, respectively. Shorter fluctuations help to keep the spoofing hidden. Fig. 14 illustrates how the 3D ECEF coordinates of the receiver changed with time. From time = 0s to time = 50s, the receiver got a genuine signal and gradually converged to a positioning solution. From time = 50s to time = 244s, the receiver had a stable positioning solution. The spoofing signal began to take over the receiver from time = 244s to 340s. Compared to Experiment 1, where the receiver's positioning solution changed rapidly with time, the receiver's positioning solution change was much more gradual here. This improves the spoofing's stealthiness. Moreover, the changes in the positioning solution indicate that the receiver was successfully taken over.

Based on the experimental results, during the intrusion period, our new method produced more stable variations in signal Doppler frequency, shorter fluctuations in C/N, shorter fluctuations in signal lock time, and more gentle changes in the receiver's 3D ECEF coordinates, compared to the conventional fixed-Doppler frequency spoofing. Therefore, our method could make spoofing much stealthier, which makes it harder for the target receiver to detect spoofing.

Theoretical analysis and experimental results show that the new method can not only ensure the reasonableness of the carrier Doppler frequency difference between spoofing signals and authentic signals, but also satisfy the consistency relationship between pseudorange code Doppler and carrier Doppler. The verification of the designed experimental platform shows that under the condition that only the approximate position and velocity information of the target is obtained during the intrusion of the spoofing signal, compared with the fixed carrier Doppler frequency signal spoofing method, the newly designed signal spoofing method can make the Doppler frequency change of the target receiver signal more stable, the signal carrier-to-noise ratio change can be reduced by 75.1% on average, the carrier-to-noise ratio change time can be shortened by 98.8%, and the signal lock-out time can be shortened by 47.6% on average, and the three-dimensional coordinate changes of the receiver are more gentle, which improves the concealment, applicability and timeliness of spoofing.

V. Conclusion

GNSS aiming at the fact that it is difficult to obtain the target's precise position and speed in actual spoofing scenarios, and traditional signal spoofing methods is hard to play a role, a mathematical model for spoofing signals into the receiver loop is established, the influence mechanism of the power, the pseudorange code traction rate, the carrier Doppler, the initial code phase difference, and the initial carrier phase difference of spoofing signal on the effect of the spoofing interference is analyzed, and a new asynchronous traction signal spoofing method for receiver tracking phase is proposed. Theoretical analysis and experimental results show that the new method can not only ensure the reasonableness of the carrier Doppler frequency difference between spoofing signals and authentic signals, but also satisfy the consistency relationship between pseudorange code Doppler and carrier Doppler.

Theoretical analysis and experiments show, when the target's position and velocity are approximately known during the intrusion period, our method outperforms the conventional fixed-Doppler frequency spoofing as follows: (1) the changes in the signal Doppler frequency are much more stable, (2) the fluctuations in C/N are much shorter, (3) the fluctuations in signal lock time are shorter, and (4) the resulting changes in the receiver's 3D ECEF coordinates are much more gentle. Our findings are academically and practically important, because the proposed spoofing is highly feasible and could expand the scope of applicability of lift-off spoofing.

References

[1] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016.

[2] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[3] T. E. Humphreys *et al.*, "Assessing the Spoofing Threat," *GPS World*, vol. 20, no. 1, p. 28, 2009.

[4] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013, doi: 10.1109/TSG.2012.2227342.

[5] T. E. Humphreys. The University of Texas at Austin. (Mar. 2016). *Texbat Data Sets 7 And 8* [Online]. Available: http://radionavlab.ae.utexas.edu/datastore/texbat/texbat_ds7_and_ds8.pdf

[6] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov. 2015, doi: 10.1109/TSG.2014.2346088.

[7] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3535–3548, Jul. 2019.

[8] C. J. Wullems, "A spoofing detection method for civilian l1 GPS and the E1-B galileo safety of life service," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, no. 4, pp. 2849–2864, Oct. 2012.

[9] T. E. Humphreys *et al.*, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer C/ION GNSS," in *Proc. Radionavigat. Lab. Conf.*, Savannah, Georgia, Sep. 2008, pp. 55–56.

[10] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2250–2267, Oct. 2013.

[11] X. Fan, L. Du, and D. Duan, "Synchrophasor data correction under GPS spoofing attack: A state estimation-based approach," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4538–4546, Sep. 2018.

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

[13] J. Lee, A. F. Taha, N. Gatsis, and D. Akopian, "Tuning-free, low memory robust estimator to mitigate GPS spoofing attacks," *IEEE Control Syst. Lett.*, vol. 4, no. 1, pp. 145–150, Jan. 2020.

[14] Y. Gao, H. Li, M. Lu, and Z. Feng, "Intermediate spoofing strategies and countermeasures," *Tsinghua Sci. Technol.*, vol. 18, no. 6, pp. 599–605, Dec. 2013.

[15] L. W. Zhao *et al.*, "A novel spoofing detection method in satellite navigation tracking phase," *J. Astronaut.*, vol. 36, no. 10, pp. 1172–1177, 2015.

[16] Y. F. Hu, "Research on GNSS spoofing technology," Ph.D. dissertation, Wuhan, China, Naval Univ. Eng., 2014.

[17] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur. (CCS)*, 2011, pp. 75–86.

[18] L. Huang, Z. C. Li, and F. X. Wang, "Spoofing pattern research on GNSS receivers," *J. Astronaut.*, vol. 33, no. 7, pp. 884–890, 2012.

[19] H. L. Lu, J. Y. Di, and W. Wang, "The spoofing threat and anti-spoofing measurements analysis for satellite navigation receiver," in *Proc. China Satell. Navigat. Conf.*, 2013, pp. 141–145.

[20] 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.

[21] K. Ma, X. Sun, and Y. P. Nie, "Research on key technologies of GPS generated spoofing," *Aerosp. Electr. Warfare*, vol. 30, no. 6, pp. 24–26, 2014.

[22] H. Y. Wang *et al.*, "Experiment study of spoofing jamming on GPS receiver," *Fire Control Command Control*, vol. 41, no. 7, 2016.

[23] C. Peng *et al.*, "Research of intermediate spoofing without precise target information," *Proc. China Satell. Navigat. Conf.*, 2019, pp. 615–624.

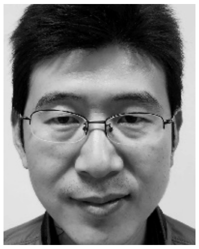
[24] Y. Hu, S. Bian, and B. Li, "A novel array-based spoofing and jamming suppression method for GNSS receiver," *IEEE Sensors J.*, vol. 18, no. 7, pp. 1952–2958, Sep. 2018.

Yangjun Gao received the B.S. degree in navigation engineering from Information Engineering University, Zhengzhou, Henan, China, in 2017, where he is currently pursuing the M.S. degree.

He has published several articles on satellite navigation data processing and satellite navigation spoofing technology. His current research focuses mainly on satellite navigation data processing and satellite navigation spoofing technology.

Zhiwei Lv received the Ph.D. degree in space geodetic survey and navigation from Information Engineering University, Zhengzhou, Henan, China, in 2010.

He is currently a Professor with Information Engineering University. He has published several articles on satellite navigation data processing and space geodetic survey. His current research focuses mainly on satellite navigation data processing and space geodetic survey.



Lundong Zhang received the Ph.D. degree from the National University of Defense Technology, China, in 2012.

He is currently a Lecturer with Information Engineering University, Zhengzhou, Henan, China. He has published several articles on indoor navigation and pedestrian. His current research focuses mainly on indoor navigation and pedestrian.