remote sensing

MDPI

Article

Spoofing Traction Strategy Based on the Generation of Traction Code

Ning Ji [1,2,3,*], Yongnan Rao [1,2,3], Xue Wang [4], Decai Zou [1,2,3], Xiaofei Chen [1,2,3] and Yao Guo [1,2,3]

[1] National Time Service Center, Chinese Academy of Sciences, Xi'an 710600, China
[2] Key Laboratory of Precision Navigation, Positioning and Timing Technology, Chinese Academy of Sciences, Xi'an 710600, China
[3] University of Chinese Academy of Sciences, Beijing 101408, China
[4] Institute of Information Sensing, Xidian University, Xi'an 710600, China
* Correspondence: jining18@mails.ucas.ac.cn

Abstract: Traction spoofing is an important component of Global Navigation Satellite System (GNSS) intermediate attacks, and the traction scheme directly determines the concealment of spoofing. However, spoofing via conventional traction strategies can be easily detected using Time of Arrival (TOA) and power detection. Based on a BPSK-modulated signal, a novel traction strategy using traction code is proposed to suppress part of the authentication signal and form an ideal correlation peak. This strategy was modeled and simulated to verify its theoretical feasibility. Effective spoofing data were generated based on the signal generation software to verify the spoofing effect with the reception of the software receiver. It can be inferred that no significant distortion occurred throughout the traction process, and the value range of the traction speed was expanded. The received results in different scenarios demonstrated that the observations' Root-Mean-Square Error (RMSE) percentage change in the proposed strategy is significantly better than those of conventional strategies. A Ratio Test was also performed, verifying that the strategy can bypass Signal Quality Monitoring (SQM) detection. Meanwhile, the proposed strategy remained effective when the C/N_0 increased to 60 dBHz. In summary, the proposed strategy exhibits destructiveness, concealment, and adaptability on the battlefield.

Keywords: covert spoofing attack; GNSS; signal suppression; traction code; traction spoofing

Citation: Ji, N.; Rao, Y.; Wang, X.; Zou, D.; Chen, X.; Guo, Y. Spoofing Traction Strategy Based on the Generation of Traction Code. *Remote Sens.* **2023**, *15*, 500. https://doi.org/10.3390/rs15020500

Academic Editors: Krzysztof Naus and Mieczysław Bakuła

Received: 27 November 2022
Revised: 6 January 2023
Accepted: 9 January 2023
Published: 14 January 2023

1. Introduction

Recently, information and navigation warfare have become important trends in modern warfare. Several military weapons, equipment, and carriers that use GNSS to provide Positioning, Navigation and Timing services pose a threat to national security, such as unauthorized Unmanned Aerial Vehicles and military-guided weapons. In the face of such threats, conventional jamming methods, such as seizing radio control and suppression jamming, may cause the target to fall, resulting in secondary damage. Therefore, spoof jamming has gradually become a popular topic in GNSS jamming.

The spoofing signal has the same structure as the authentication signal. It can invade an enemy receiver that has no corresponding defensive measures without destroying the tracking loop or even being detected. Subsequently, it can change or control the positioning and timing results. Hence, it is an ideal means of controlling various military weapons, equipment, and carriers [1]. GNSS deception is predicted to play a significant role in modern warfare [2].

Traction spoofing is an important part of intermediate and sophisticated navigation spoofing. Among the five detection means of the receiver [3], TOA detection [4], power detection [5,6], and Angle Of Arrival (AOA) detection are all important methods for detecting traction spoofing. However, as there is no space for AOA detection to be overcome in the software, this is not the objective of this study. Power detection identifies spoofing

by the monitoring signal power changes. As shown in Figure 1, TOA detection includes change detection of observations [7] and distortion detection of correlation values [8,9]. The observation objects can include the code frequency, carrier frequency, and other information.

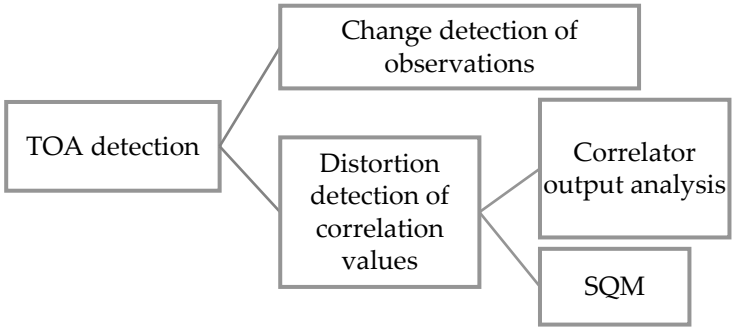


Figure 1. Classification of TOA detection of satellite signals.

Therefore, to address possible security threats, designing a traction strategy to bypass the spoofing detection means of the receiver and stably invading the target tracking loop is an important issue in traction spoofing.

2. Materials and Methods

2.1. Conventional GNSS Traction Spoofing

The conventional traction process of spoofing can be divided into three steps:

Step 1: Signal reception. The receiving module of the spoofer receives a genuine signal, detects the location and speed of the target, and estimates the genuine signal's key parameters.

Step 2: Determine the traction scheme. The parameters of the spoofing signal are set such that the correlation peak of the spoofing signal arriving at the target receiver aligns gradually with the actual peak. In a conventional traction strategy, the correlation peak envelope of the composite signal is distorted, as shown in Figure 2.

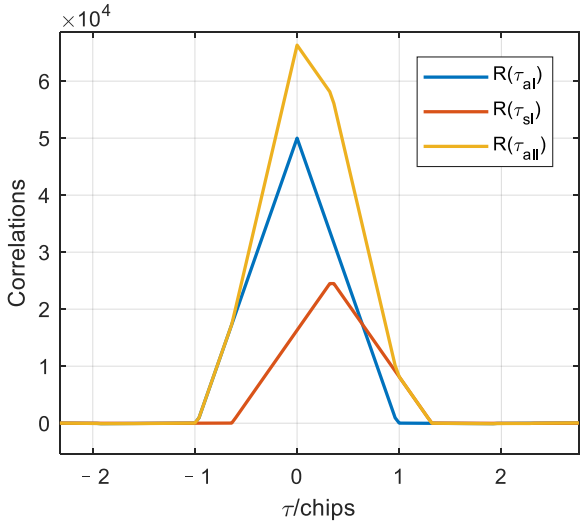


Figure 2. Demonstration of correlation peak distortion of conventional traction strategy.

Step 3: Traction spoofing. The spoofing signal is generated to dominate the tracking loop and gradually enlarge the code phase difference to generate a pseudo-distance error, which eventually controls the target.

The correlation result between the local and authentication signals is defined as $R_{al}(\tau)$, and thatbetween the local and superimposed signals is defined as $R_{all}(\tau)$. If the correla-

tion function between the spoofing signal and local replica is $R_{sl}(\tau)$, then the distortion correlation peak envelope of the composite signal is as illustrated in Figure 2.

In the first step, the detection of the antenna position and speed of the spoofing target, power level, channel conditions, and other information is not within the scope of this study, assuming that the spoofer has obtained specific information. The content discussed in this study is the setting and generation module of the spoofing signal.

The discussion in this paper is based on a Binary Phase Shift Keying (BPSK) signal system. First, we can model the genuine signal as:

$$s_a(t) = \sqrt{P_a(t)} \cdot D_a(t) \cdot C_a(t) \cdot \cos(2\pi(f_0 + f_{d\_a})t + \theta_a), \quad (1)$$

Similarly, the spoofing signal can be expressed as

$$s_s(t) = \sqrt{P_s(t)} \cdot D_s(t) \cdot C_s(t) \cdot \cos(2\pi(f_0 + f_{d\_a} + f_{as})t + \theta_a + \theta_{as}), \quad (2)$$

where the subscripts a and s represent the genuine and spoofing signals, respectively. In addition, P, D, C, f_d and θ denote the satellite signal power, navigation message, pseudo code, Doppler shift, and initial carrier phase, respectively.

The traction modes in the latter two steps can be divided into synchronous and asynchronous traction according to the accuracy of the parameter estimation [10].

(1) Synchronous traction

The diagram of synchronous traction is shown in Figure 3.

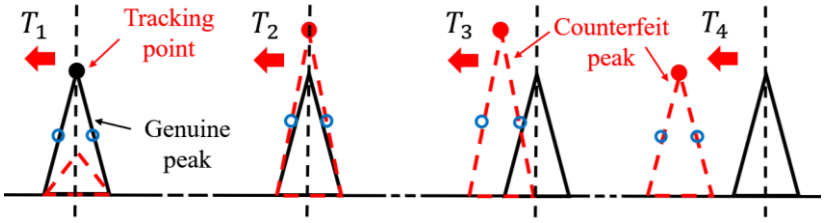


Figure 3. Diagram of synchronous traction.

T1: At the beginning of traction, the spoofing code phase (Doppler) is aligned with the genuine code phase (Doppler).

T2: Increase the power of spoofing signals.

T3: Drag the correlation peak away from the original tracking point.

T4: Keep the power consistent with the genuine signal.

This method requires high measurement accuracy in the first step and is difficult to achieve in an actual scenario.

(2) Asynchronous traction

A diagram of asynchronous traction is shown in Figure 4. Unlike synchronous traction, asynchronous traction does not require a spoofer to determine the exact parameters of an authentication signal. This traction mode directly generates a higher power correlation peak to control the loop, which is more suitable for application in actual scenarios.

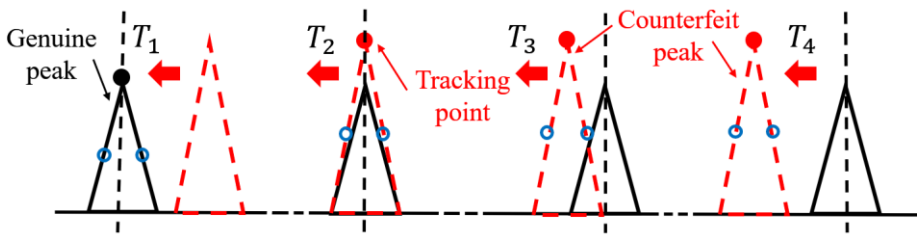


Figure 4. Diagram of asynchronous traction.

Control of the distance velocity of the correlated peaks is defined as the traction code rate v_{drag}. In the third step of the spoofing traction process, according to whether the spoofing signal maintains the code and carrier phase consistency, conventional traction strategies can be divided into two types [11]:

Strategy 1 Adjust the code phase only

The code and carrier phase consistencies are broken, and only the code rate is altered.

$$f_{drag} = 0, \tag{3}$$

Strategy 2 Maintain code-carrier coherence

If the spoofing signal maintains code-carrier coherence, we obtain

$$f_{drag} = v_{drag} \cdot \frac{f_0}{R_0} \tag{4}$$

where f_0 and R_0 represent the nominal carrier frequency and code rate, respectively.

The deception process of the spoofer is illustratedin Figure 5. The first light-grey area is the setting module of the spoofing signal, and the lower light-grey area is the generation module of the spoofing signal.

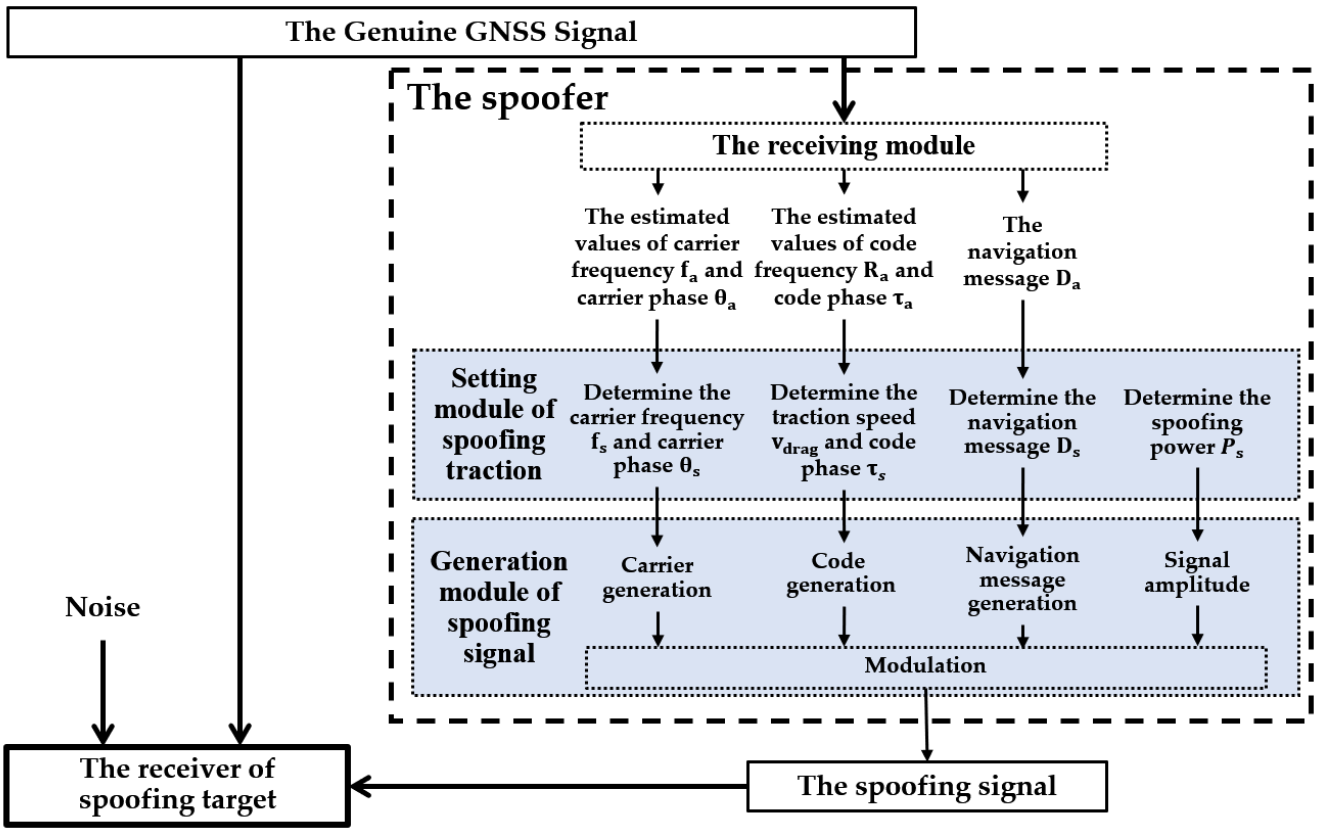


Figure 5. Schematic diagram of the deception process of the traction spoofer.

In conventional traction strategies, although the Pseudo-Random Noise (PRN) code $C_s(t)$ used forspoofing is the same as the genuine signal, there is a designed phase difference τ_{as}:

$$C_s(t) = C_a(t + \tau_{as}), \tag{5}$$

where

$$\tau_{as}(t) = \tau_s(t) - \tau_a(t) = v_{drag} \cdot t \tag{6}$$

After determining the traction speed v_{drag}, the phase difference τ_{as} can be obtained from Equation (6). Then $C_s(t)$ can be obtained from Equation (5).

The distortion in Figure 2 is often the root cause of TOA and power detection; hence, traction strategies that can avoid correlation peak superposition are considered. In this case, replacing the code of the original system may be a novel idea, as discussed in the next section.

2.2. Proposed Spoofing Traction Strategy

In this section, the theory and implementation of an improved spoofing traction strategy are introduced.

2.2.1. Signal Model

To ignore the noise, there is

$$R_{all}(\tau) = R_{al}(\tau) + R_{sl}(\tau) \tag{7}$$

A correlation function diagram for the proposed strategy is shown in Figure 6. The objective of the proposed traction strategy is to make R_{all} replace R_{al} to affect the decision making of the receiver. The code-phase relationship between R_{all} and R_{al} is determined using the traction speed v_{drag}. The ideal correlation peaks can be modeled as:

$$R(\tau) = A_R(1 - |\tau|), |\tau| \leq 1 \tag{8}$$

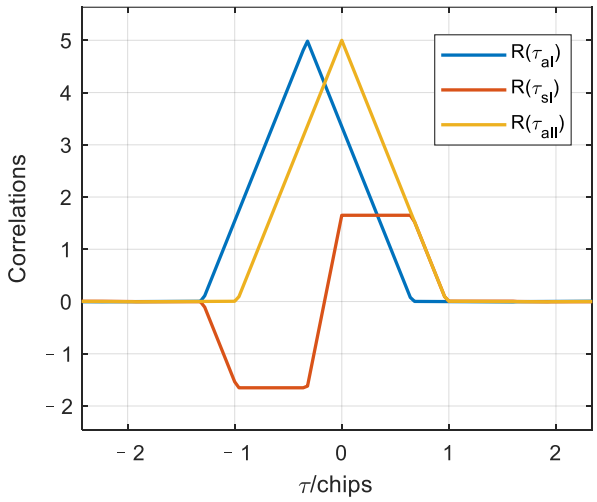


Figure 6. Diagram of correlation function of covert spoofing traction.

In addition, we intend to obtain

$$\tau_{al} = v_{drag}t, \tag{9}$$

which gives

$$R_{all}(\tau) = R\left(\tau + v_{drag}t - \tau_{al}\right) = R(\tau) \tag{10}$$

The code used to replace the pseudo code of the original system may be called the traction code. From the expected R_{sl} and the correlation theorem of the Fourier transform, the formula for the traction code sequence can be derived as

$$C_s(t) = \mathcal{F}^{-1}\left\{\frac{\mathcal{F}[R_{sl}(\tau)]}{\mathcal{F}^*[C_l(t)]}\right\} = C_l(t) - C_a(t) = C_a(t + \tau_{al}) - C_a(t) \tag{11}$$

where $C_l(t)$ denotes the desired local replica of the PRN code. The calculation method for the pseudocode sequence can be found in the Interface Control Document. It can be seen

from Equation (11) that the traction code sequence $C_s(t)$ is actually equal to the difference between $C_l(t)$ and the PRN code sequence $C_a(t)$ of the genuine signal. In other words, the desired phase-shifted PRN code is formed by superimposing a traction code on top of the genuine PRN code.

In an actual scenario, the power level of the genuine signal must be accurately estimated to determine the amplitude of the traction code. Additionally, the estimation belongs to the first step of the traction process, which is not within the scope of this study.

$C_l(t)$ and $C_a(t)$ are the same set of conventional PRN codes with a code phase difference τ_{al}, whereas $C_s(t)$ is not. This is discussed in Section 2.2.2.

2.2.2. Generation of Traction Code

The generation of traction codes is the core innovation in the proposed traction strategy. The code embedded in the signal-generation software completes the generation of the spoofing code described above. Figure 7 presents the generation steps of the traction code, where T_{coh} is the coherent integration time, which is equals to 1 ms.

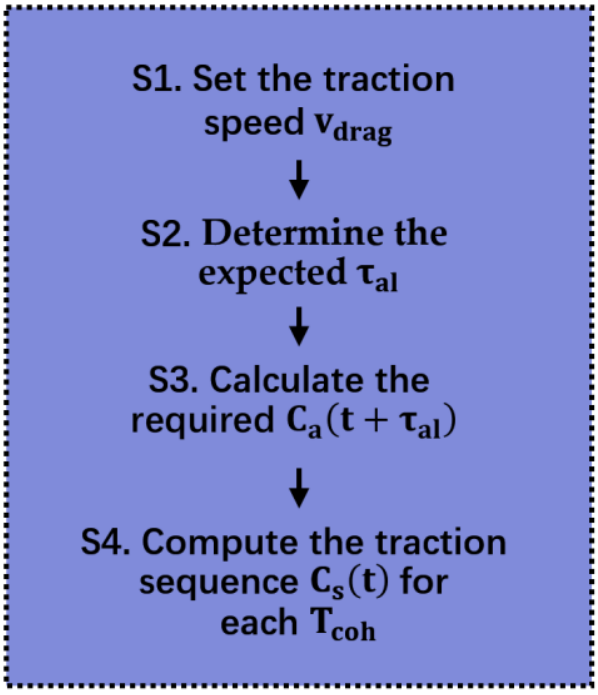


Figure 7. Process diagram of the generation of traction code.

In S1, the selection of the traction speed v_{drag} follows certain principles, which is discussed later. In S2, τ_{al} can be calculated using Equation (9). In S4, $C_s(t)$ can be calculated using Equation (11).

Consider the BeiDou Navigation Satellite System No. 33 satellite as an example to generate a spoofed traction code. We generate data for 20 s, and traction was selected to start at 1 s and end at 16 s. Three time points are randomly selected to observe the changes in the pseudo-code layer in the initial, intermediate, and final stages of traction. Figure 8 shows the transition process of the traction code sequence. It can be observed that the traction code changes with the advancement of the traction process and has no fixed form; conventional PRN codes have values of ± 1, whereas traction codes have values of 0 and ± 2; hence, it is not a PRN code in the conventional sense.

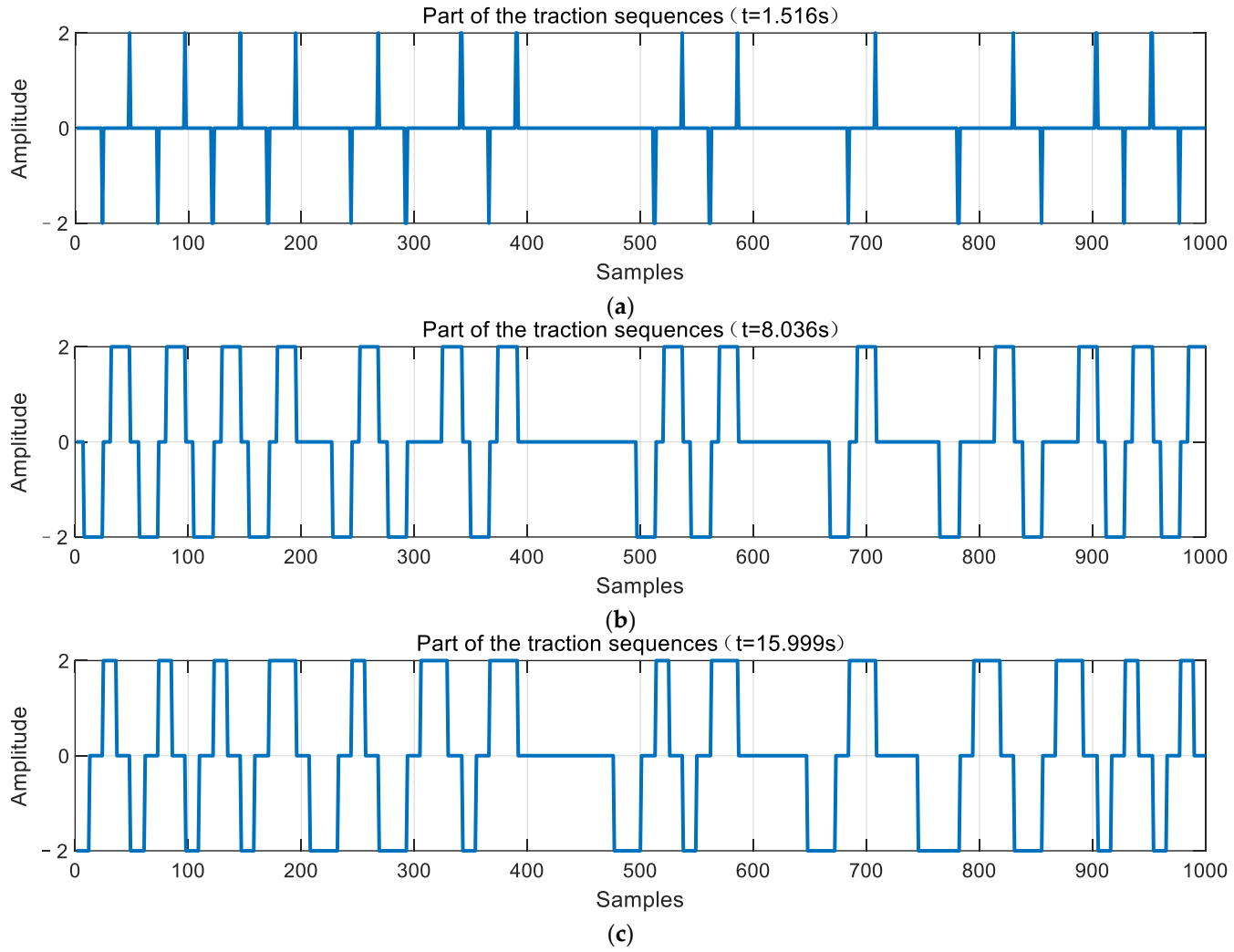


Figure 8. Transition process of traction code sequence. (**a**) Initial form of traction code; (**b**) Intermediate form of traction code; (**c**) Final form of traction code.

Figure 9 shows the transition process of the PRN code sequence received by the spoofing target. Under the assumption of the proposed strategy, the received code sequence is always in the form of an authentication PRN code, and there is a significant phase shift caused by the code Doppler change v_r based on the real value.

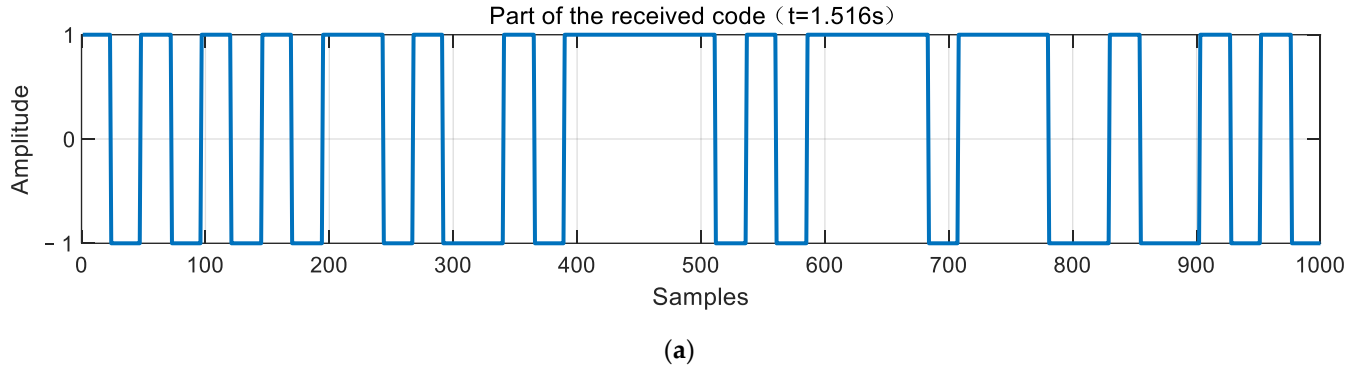
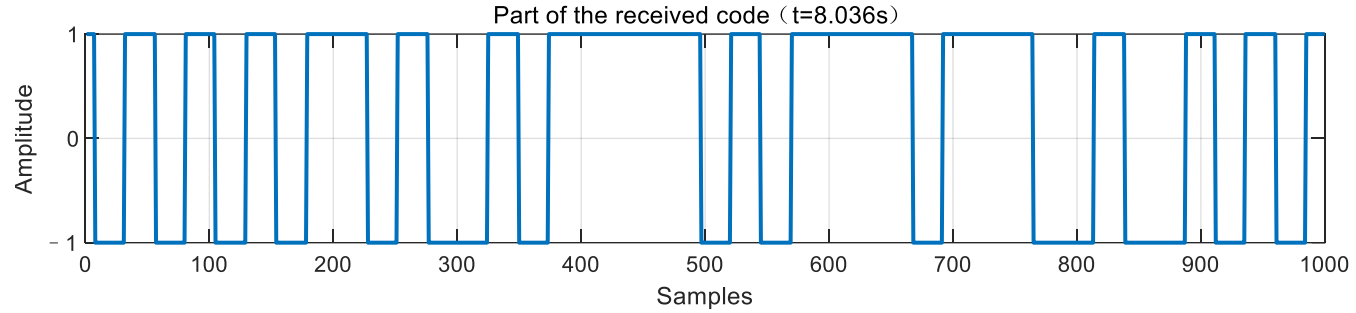
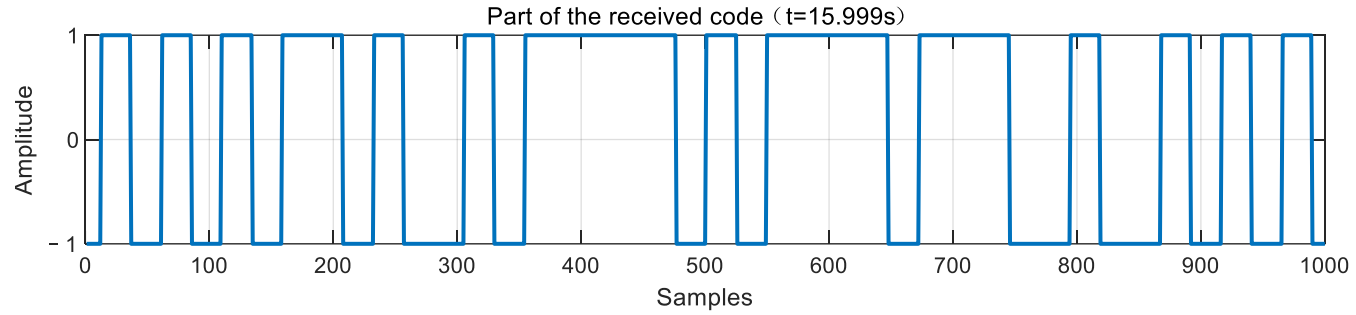


Figure 9. *Cont.*



(**b**)



(**c**)

Figure 9. Transition process of the received PRN code. (**a**) Initial form of received PRN code; (**b**) Intermediate form of the received PRN code; (**c**) Final form of the received PRN code.

Figure 10 shows a diagram of the deception process of the proposed traction strategy. In the dark-blue area, there is a procedure for generating the spoofing traction code, which is also a key step that differs from the other traction processes.

2.3. Methods of Simulation and Experiment

2.3.1. Theoretical Model of Received Signal

According to the signal model in Section 2.1, the composite signal r(t) is demodulated by the local receiver as follows:

$$i_P(t) = r(t)C_a(t+\tau_{al})\cdot\cos(2\pi(f_0+f_{d\_a}+f_{al})t+\theta_a+\theta_{al}) = i_{P_a}(t)+i_{P_s}(t), \quad (12)$$

where τ_{al} is the code phase difference between the genuine and local signals, and the same is true for parameters f_{al}, θ_{al}, τ_{sl}, f_{sl}, θ_{sl} and other parameters.

Coherent integration of $i_{P_a}(t)$ is performed to obtain the prompt correlation values:

$$I_{P_a} = \frac{\sqrt{P_a}}{2}R(\tau_{al})T_{coh}\mathrm{sin\,c}(f_{al}T_{coh})\cos\left(2\pi f_{al}\left(t_1+\frac{T_{coh}}{2}\right)+\theta_{al}\right) \quad (13)$$

$i_{P_s}(t)$ are integrated and dumped to produce the prompt correlation results of spoofing signals:

$$I_{P_s} = \frac{\sqrt{P_{sp}}}{2}R(\tau_{sl})T_{coh}\mathrm{sin\,c}(f_{sl}T_{coh})\cos\left(2\pi f_{sl}\left(t_1+\frac{T_{coh}}{2}\right)+\theta_{sl}\right) \quad (14)$$

Given τ_{al} and τ_{sl}, we can obtain $R(\tau_{al})$ and $R(\tau_{sl})$ according to Equation (8).

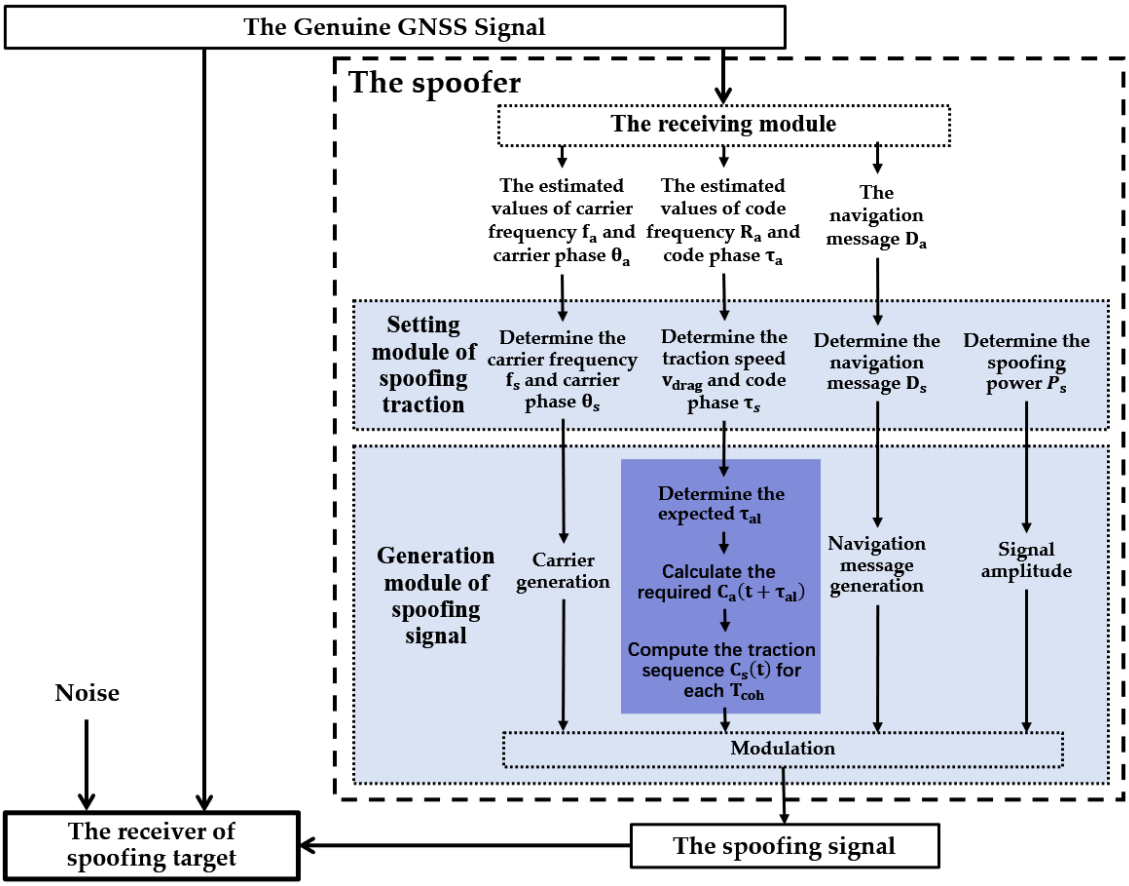


Figure 10. Schematic diagram of the spoofer applying the proposed traction strategy.

Strategy 1

Assuming that the amplitude ratio between the spoofing and genuine signals is $h = \sqrt{\frac{P_s}{P_a}}$, the correlation results can be simplified as

$$I_P(t) = \frac{\sqrt{P_a}}{2} T_{coh}(R(\tau_{al}) + hR(\tau_{sl})) \tag{15}$$

The same is true for I_E and I_L.

Define v_{drag} as the traction speed, then

$$\tau_{as}(t) = \tau_s(t) - \tau_a(t) = v_{drag} \cdot t \tag{16}$$

Then $R(\tau_{al})$, $R(\tau_{sl})$, the early and late correlation results can be derived.

When the carrier loop is in a steady state, the received signal power is not transferred from the in-phase components to quadrature components. The phase discriminator of the code tracking loop processes the early and late correlation results, and the output is

$$\delta_{cp} = \frac{I_E - I_L}{I_E + I_L} = \frac{R^+(\tau_{al}) - R^-(\tau_{al}) + hR^+(\tau_{sl}) - hR^-(\tau_{sl})}{R^+(\tau_{al}) + R^-(\tau_{al}) + hR^+(\tau_{sl}) + hR^-(\tau_{sl})} \tag{17}$$

where $R^+(\tau) = R(\tau + d)$, $R^-(\tau) = R(\tau - d)$.

Local code Doppler cd_l is obtained after the filter of the code loop processing δ_{cp}:

$$cd_l(n) = k_{c2}\delta_{cp}(n) + \sum_{i=1}^{n} k_{c1}\delta_{cp}(i) \tag{18}$$

Strategy 2

If the spoofing signal maintains the code-carrier coherence, the frequency change in the spoofing signal directly influences the local carrier generation, and the received signal power is transferred to the quadrature components. The prompt correlation amplitude is expressed as follows:

$$P = |I_P(n) + jQ_P(n)| = \left| \frac{\sqrt{P_a}}{2} R(\tau_{al}) T_{coh} \sin c(f_{al} T_{coh}) e^{j\phi_{al}} + \frac{\sqrt{P_{sp}}}{2} R(\tau_{sl}) T_{coh} \sin c(f_{sl} T_{coh}) e^{j\phi_{sl}} \right| \tag{19}$$

The output of the phase discriminator of the code tracking loop can be expressed as:

$$\delta_{cp} = \frac{E - L}{E + L} \tag{20}$$

where the forms of the early and late correlation amplitudes are the same as those of the prompt correlation amplitude; only the function $R(\tau)$ is replaced by $R^+(\tau)$ or $R^-(\tau)$.

The output of the phase discriminator of the carrier loop is typically calculated using a two-quadrant arctangent function:

$$\phi_e(n) = \arctan\left(\frac{Q_p(n)}{I_p(n)}\right) = \arctan\left(\frac{\sin\phi_{al} + h\frac{R(\tau_{sl})\sin c(f_{sl}T_{coh})}{R(\tau_{al})\sin c(f_{al}T_{coh})}\sin\phi_{sl}}{\cos\phi_{al} + h\frac{R(\tau_{sl})\sin c(f_{sl}T_{coh})}{R(\tau_{al})\sin c(f_{al}T_{coh})}\cos\phi_{sl}}\right) \tag{21}$$

Local carrier Doppler fd_l is obtained after the filter of carrier loop processing $\phi_e(n)$:

$$fd_l(n) = k_{f2}\phi_e(n) + \sum_{i=1}^{n} k_{f1}\phi_e(i) \tag{22}$$

Proposed Strategy Spoofing traction strategy based on the generation of traction code

The correlation results can be stable throughout the traction process, and the prompt correlation result P is always

$$P(n) = \frac{\sqrt{P_a}}{2} T_{coh} R\left(v_{drag} t - \tau_{al}\right) \tag{23}$$

Similarly, the forms of the early and late correlation results are the same as those of the prompt correlation results. Only functions $R(\tau)$ are replaced by $R^-(\tau)$ and $R^+(\tau)$.

The ideal output of the phase discriminator of the code loop can be obtained:

$$\delta_{cp} = \frac{I_E - I_L}{I_E + I_L} = \frac{R^-\left(v_{drag}t - \tau_{al}\right) - R^+\left(v_{drag}t - \tau_{al}\right)}{R^-\left(v_{drag}t - \tau_{al}\right) + R^+\left(v_{drag}t - \tau_{al}\right)} \tag{24}$$

2.3.2. Simulation and Conditions

Considering synchronous traction with a more hidden spoofing effect as an example, simulations were performed for three traction strategies according to the theoretical model of the received signal in Section 2.3.1. Because the simulation does not require mass data processing at a high sampling rate, it can quickly test traction success under a certain strategy. For the 20-s data, the simulation of Strategy 1 took less than 1 s, and the simulation of Strategy 2 took less than 2 s.

Spoofing was selected to enter at 1 s. Traction duration was determined by v_{drag} and the tracking-loop structure. Because the carrier loop is only related to the prompt correlation value, when τ_{al} and τ_{as} are 1 chip, the two peaks have exited each other's prompt tracking point, whereas the code loop needs to wait for the other correlation peak

to exit the early or late tracking point. If the traction duration of the carrier loop is defined as t_f and that of the code loop is defined as t_c, then

$$t_f = \frac{1}{v_{drag}}, \tag{25}$$

$$t_c = \frac{1+d}{v_{drag}}, \tag{26}$$

In other words, according to the structural characteristics of the carrier and code loops, the traction duration should be at least t_c.

The maximum spoofing power of conventional spoofing signals is equal to the genuine signal power. The correlator spacing at the receiver was set as the typical value for satellite navigation receiver applications, i.e., D = 2d = 1. The spoofing signal has the same initial carrier and code phases as the genuine signal when added.

$$\theta_{sl} = \theta_{al} = \theta_{as} = 0 \tag{27}$$

The first set of simulations (Nos. 1, 3, and 5) was used to directly compare the theoretical deception effects of the strategies.

The Simulation conditions are presented in Table 1. When implementing a traction strategy to successfully implement spoofing traction, the selection of traction speed v_{drag} follows certain principles. According to the code loop structure, the code phase offset within each coherence integration should not exceed 0.5 chips [12], that is the traction speed v_{drag} should not be too fast. However, owing to the loose requirements, spoofing may fail even if the conditions are met.

Table 1. Simulation conditions.

No.	Spoofer						Channel	Receiver
	Strategy	Traction Duration (s)		Data Length (s)	v_{drag} (cps)	h_{max}	Nosie Padding	D (Chips)
		Start Time	End Time					
1	1	1	$1 + t_c$	20	0.1	1	Disabled	1
2					$\lvert v_{drag} \rvert \leq 500$ cps			
3	2				0.1			
4					$\lvert v_{drag} \rvert \leq 500$ cps			
5	3				0.1			
6					$\lvert v_{drag} \rvert \leq 500$ cps			

When the traction strategy is determined, the range of traction speed that can make traction successful is determined. Therefore, the theoretical value range of the traction speeds of the three strategies can be determined via another set of traversal simulations (Nos. 2, 4, and 6).

2.3.3. Spoofing Experiment and Scenario

To verify the applicability of the proposed strategy in actual environments, effective intermediate-frequency spoofing data were generated based on the signal generation software, and noise was added to the composite signal. We then used a software receiver to examine the effects of the different spoofing traction strategies. No. 33 satellite signal was selected. The intermediate frequency was $f_{IF} = 10$ MHz, sampling rate was $f_s = 50$ MHz, and carrier-to-noise ratio was $C/N_0 = 50$ dBHz. Three traction strategies were simulated under these conditions.

However, to simulate the change in the signal strength caused by different noise environments and satellite altitude angle changes, C/N_0 was set to 30 dBHz, 40 dBHz and

50 dBHz, respectively. Owing to the particularity of spoofing, we expected the received results to be stably close to those of the genuine signal. Therefore, RMSE statistics were conducted on the results of the three traction strategies to observe the performance of the proposed strategy under different C/N_0. These statistics were compared with the genuine results.

A spoofing scenario of 60 dBHz C/N_0 was used to simulate the power enhancement in special scenarios, such as the battlefield. To simulate narrow correlators and pulse-aperture correlators, spoofing scenarios with narrow correlation intervals (D = 0.2 chips) were added.

The designed spoofing scenarios are presented in Table 2.

Table 2. Overview of the spoofing scenarios.

No.	Spoofer						Channel	Receiver
	Strategy	Traction Duration (s)		Traction Duration (s)	v_{drag} (cps)	h_{max}	C/N_0 (dBHz)	D (Chips)
		Start Time	End Time					
1	1	1	$1 + t_c$	1	0.1	1	30	1
2							40	1
3							50	1
4								0.2
5							60	1
6	2						30	1
7							40	1
8							50	1
9								0.2
10							60	1
11	3						30	1
12							40	1
13							50	1
14								0.2
15							60	1

2.3.4. Data Processing

Whether in the simulation or experiment, the local code phase is not directly known, and it must be obtained using the following formula:

$$\tau_l(n) = \tau_0 + T_{coh} \cdot \sum_{i=1}^{n} cd_l(i), \tag{28}$$

where τ_0 is the initial code phase obtained from acquisition. The phase difference diagram can be obtained by subtracting τ_l from τ_a and τ_s, respectively.

Once we obtain the tracking results, we must determine whether the spoofing traction was successful. For spoofing, whose frequency is locked to the genuine signal, we want τ_{sl} to be 0 to demonstrate that the code loop traction is successful, and for spoofing that maintains the code-carrier coherence, we also want f_{sl} to be 0 to demonstrate that the carrier loop traction is successful. These results can be expressed using the following formulas:

$$T_1 = sgn\{\log|\tau_{sl}|\} \tag{29}$$

$$T_2 = sgn\{\log(|\tau_{sl}| + |f_{sl}|)\} \tag{30}$$

If T_1 (or T_2) is less than 0, traction succeeds; otherwise, traction fails.

Given the maximum traction speed v_{drag_max} for a given strategy, the shortest time required for deceptive traction can be calculated using the following formula:

$$t_{c\_min} = \frac{1+d}{v_{drag\_max}} \tag{31}$$

Because there are several detection methods included in TOA and power detection, this study attempts to use a simple statistical analysis method and the SQM method as examples to verify the detection quantity. If we perform a statistical analysis on observation X, the RMSE statistic is:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(X_i - X_{0_i})^2}, \tag{32}$$

where X_{0_i} are the fitting values of the genuine signal observations. To reflect the influence of the spoofing signals of each strategy on the RMSE, the RMSE values are calculated as follows:

$$Percentage_{\Delta i} = \frac{RMSE_i - RMSE_0}{RMSE_0} \times 100\% \tag{33}$$

where $RMSE_0$ represents the RMSE statistic of the genuine signal observations.

In the SQM technique, we used a Ratio Test metric to identify correlation distortions. The Ratio Test metric is:

$$R_{SQM+} = \frac{E+L}{2P}, \tag{34}$$

where E, L, and P denote early, late, and prompt correlator outputs over the in-phase branch, respectively.

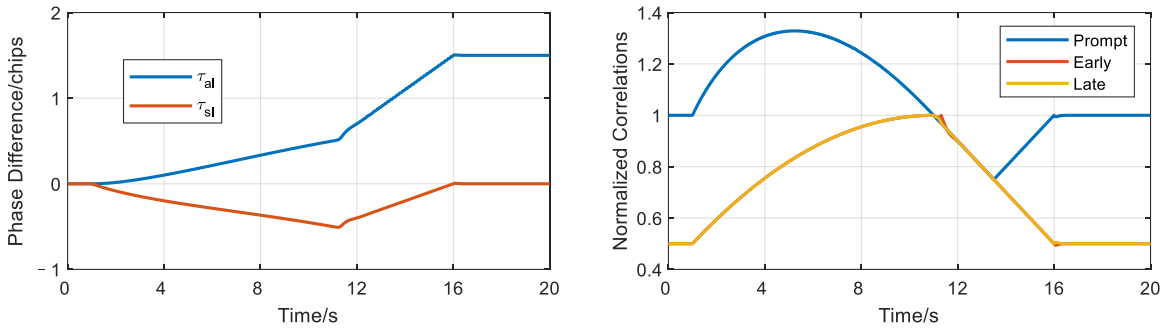
To observe fluctuations, we uniformly subtracted the ideal value of metric 1/2 from the metric when plotting.

3. Results

3.1. Simulation Results

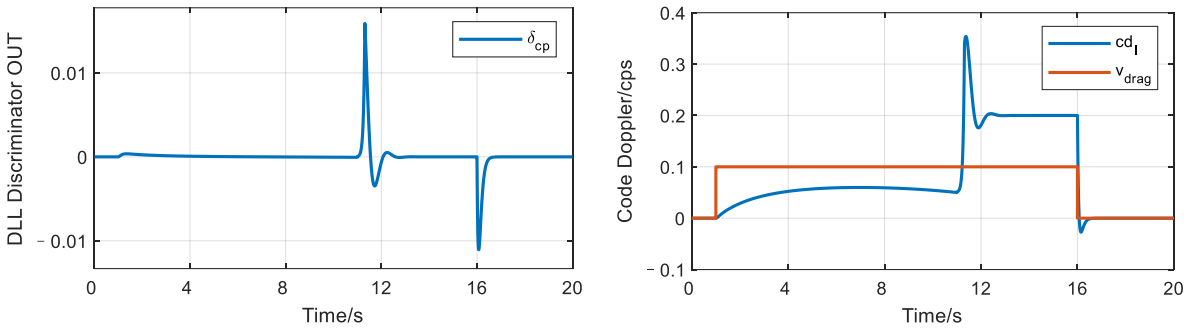
The results of the spoofing simulation designed in Section 2.3.2 are listed in this section.

The simulation results for the three traction strategies are shown in Figures 11–13. Figures 11a, 12a and 13a present the code phase difference diagrams, and we expect τ_{sl} (local spoofing) to always be on the x-axis. Figures 11b, 12b and 13b present the correlator output diagrams, and we expect these values to be stable. Figures 11c, 12c and 13c and Figures 11e, 12e and 13e are discriminator output diagrams, and we expect δ_{cp} and ϕ_e to always be on the x-axis. Figure 11d,f, Figure 12d,f and Figure 13d,f are the filter output diagrams, and we expect the local code Doppler cd_l and local carrier Doppler fd_l to follow v_{drag} and f_{drag}, respectively.



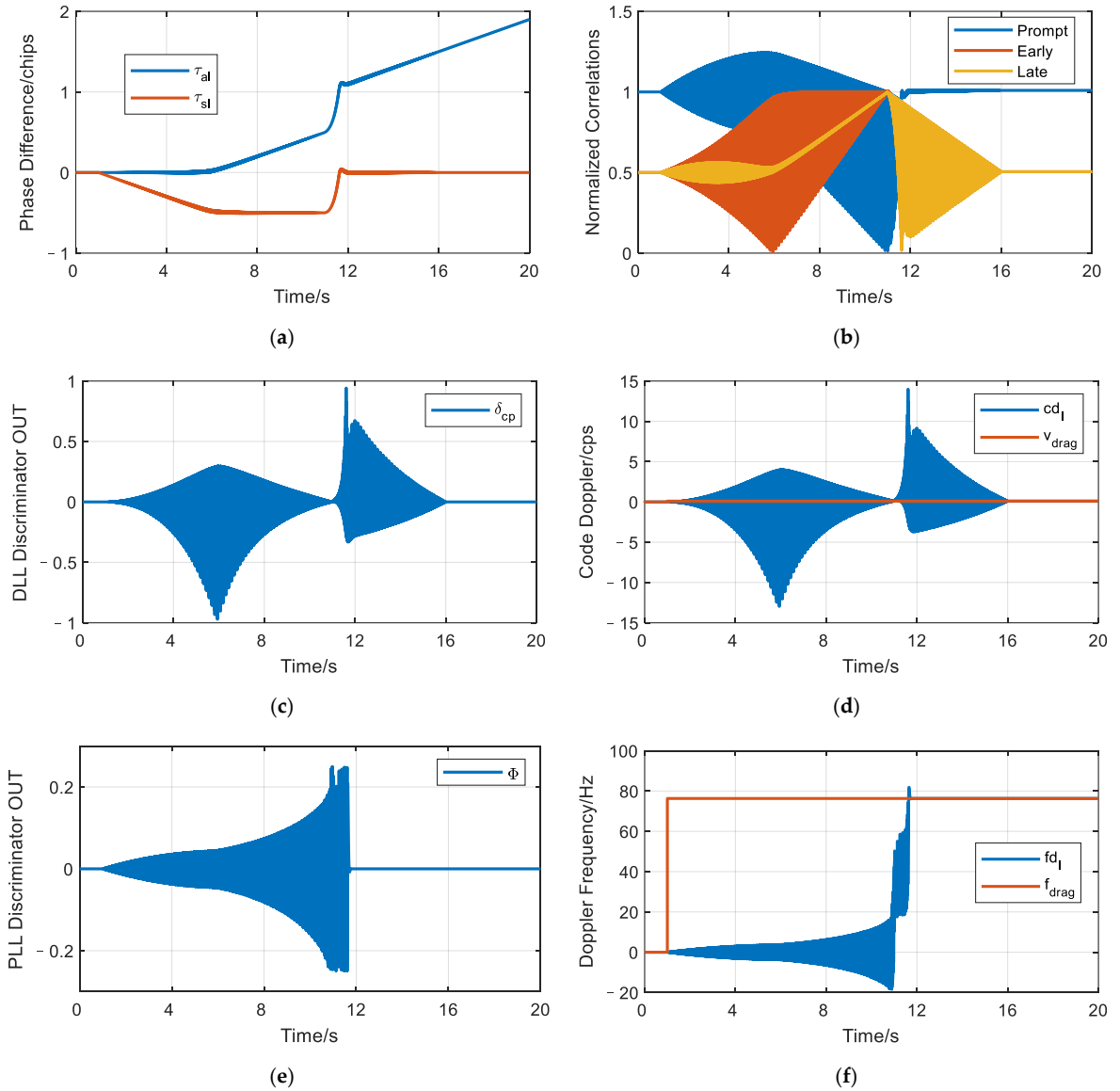
(**a**) (**b**)

Figure 11. *Cont.*



(**c**) (**d**)

Figure 11. Theoretical simulation results of strategy 1. (**a**) Code phase differences; (**b**) Outputs of correlators; (**c**) Output of phase discriminator of the code loop; (**d**) Filter output of the code loop.



(**a**) (**b**)

(**c**) (**d**)

(**e**) (**f**)

Figure 12. Theoretical simulation results of strategy 2. (**a**) Code phase differences; (**b**) Outputs of correlators; (**c**) Output of phase discriminator of the code loop; (**d**) Output of filter of the code loop; (**e**) Output of phase discriminator of the carrier loop; (**f**) Output of filter of the carrier loop.

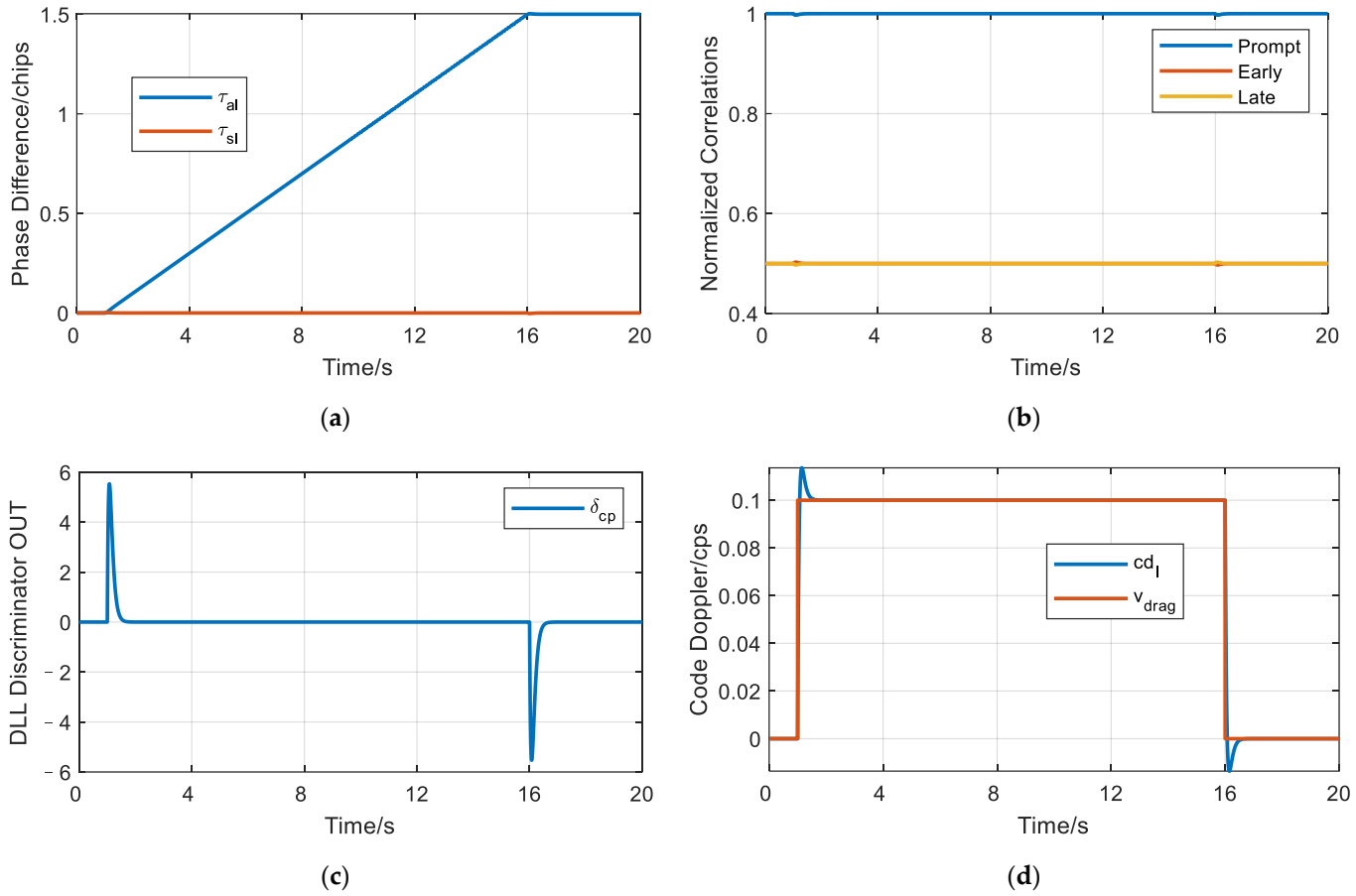


Figure 13. Theoretical simulation results of the proposed traction strategy. (**a**) Code phase difference; (**b**) Outputs of correlators; (**c**) Outputs of phase discriminator of code tracking loop; (**d**) Outputs of filter of code tracking loop.

Via a traversal simulation, the theoretical value ranges of the traction speeds of the three strategies are presented in Table 3.

Table 3. Value ranges of v_{drag} for three strategies.

Traction Strategy	Theoretical Value Ranges of v_{drag}	t_{c_min}
Strategy 1	$\lvert v_{drag} \rvert \leq 2.79$ cps	0.538 s
Strategy 2	$\lvert v_{drag} \rvert \leq 0.104$ cps	14.423 s
Proposed strategy	$\lvert v_{drag} \rvert \leq 27.89$ cps	0.054 s

3.2. Experimental Results

The results of the spoofing experiment designed in Section 2.3.3 are listed in this section.

Unlike the simulation results in Section 3.1, effective intermediate frequency spoofing data with noise were generated based on the signal generation software. The obtained results of the three spoofing traction strategies Under the C/N_0 50 dBHz condition are shown in Figures 14–16. Code-phase difference diagrams were plotted accordingly.

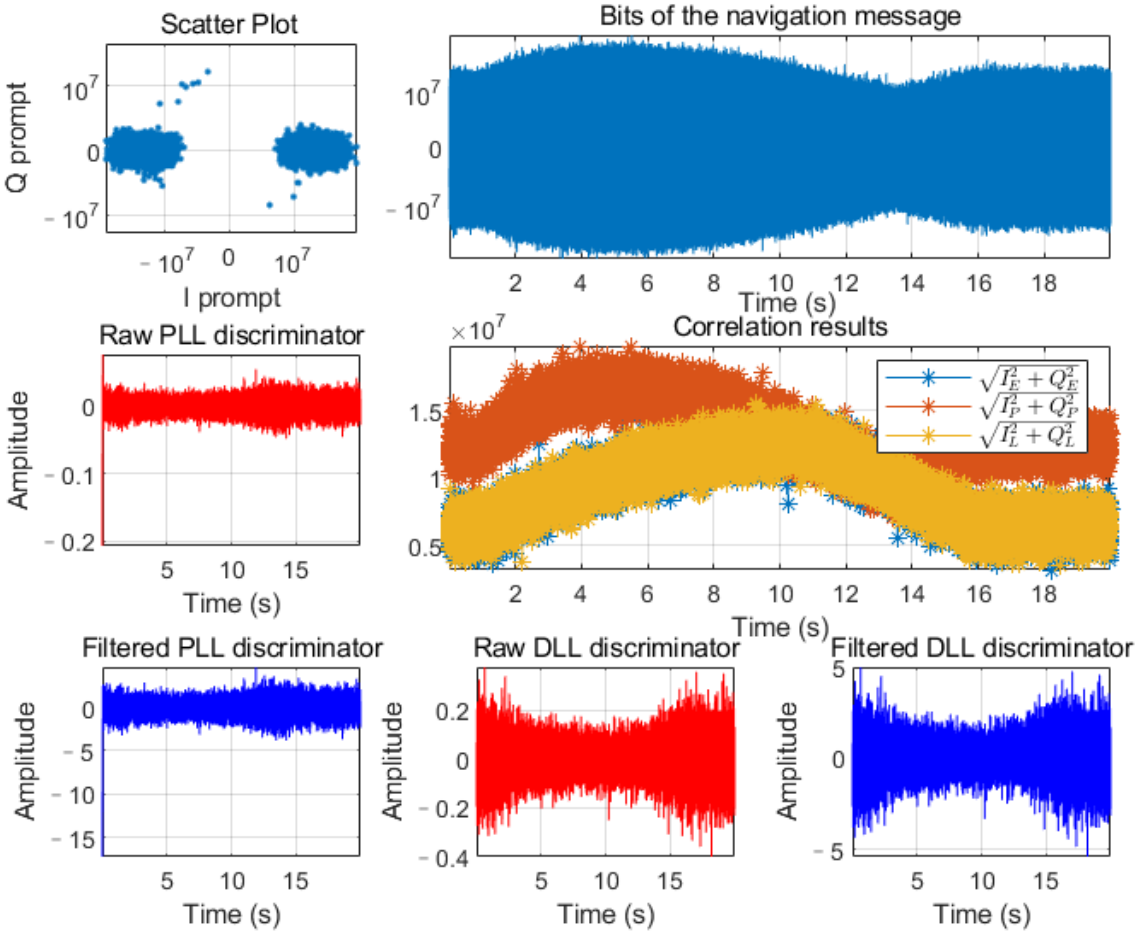
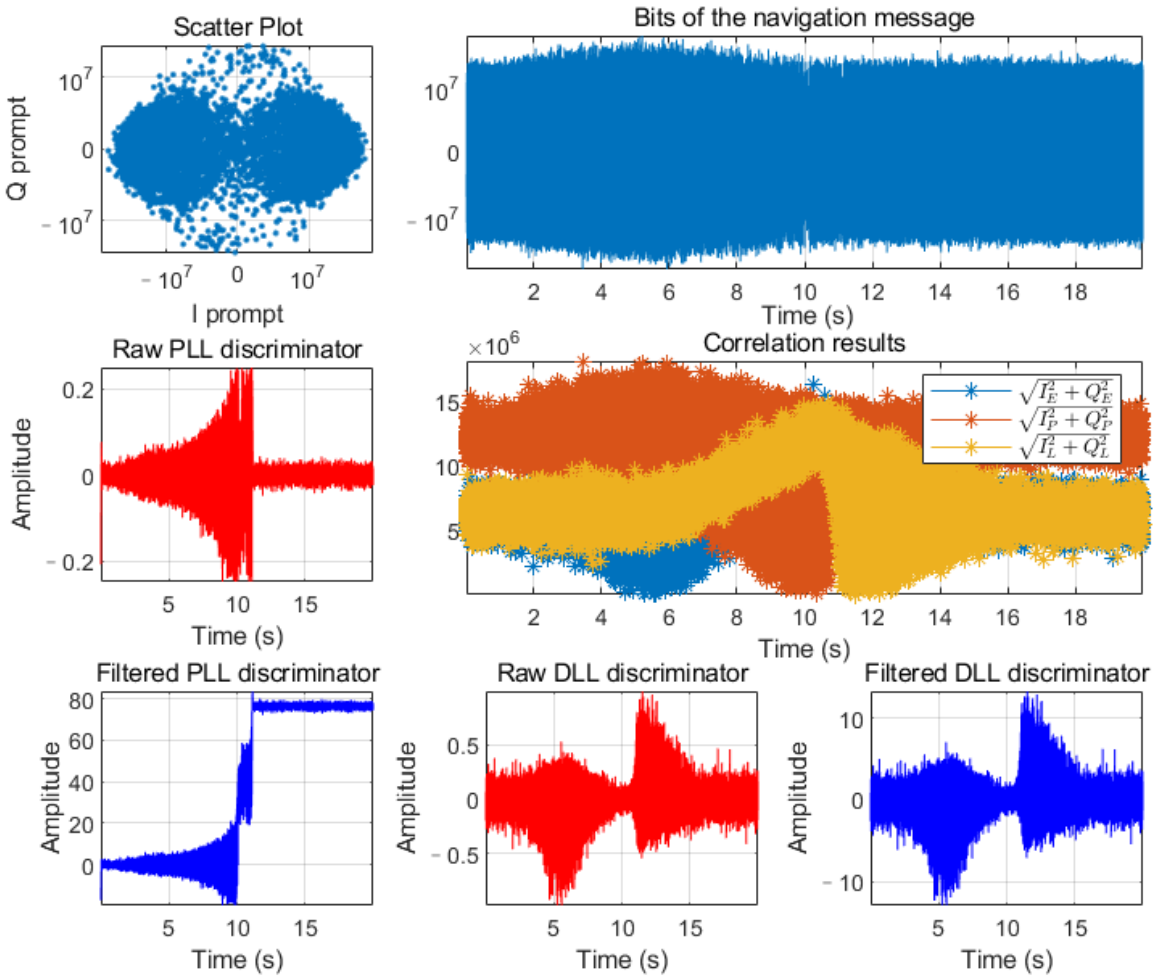


Figure 14. Results of the conventional Strategy 1 ($C/N_0 = 50$ dBHz, $D = 1$). (**a**) Obtained results of software receiver; (**b**) Code phase difference.



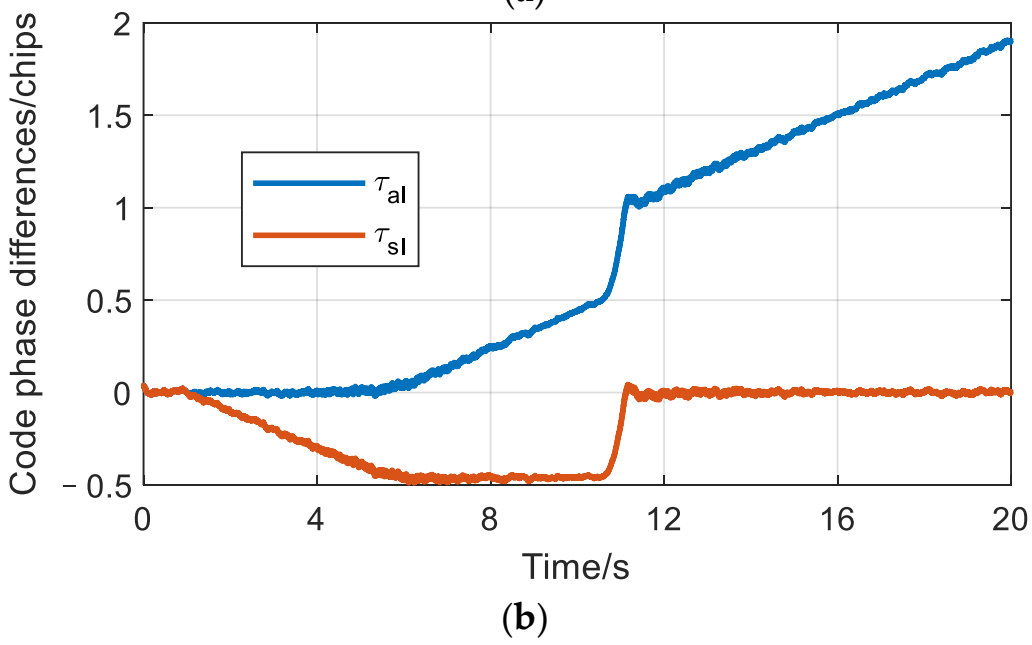


Figure 15. Results of the conventional Strategy 2($C/N_0 = 50$ dBHz, $D = 1$). (**a**) Obtained results of the software receiver; (**b**) Code phase difference.

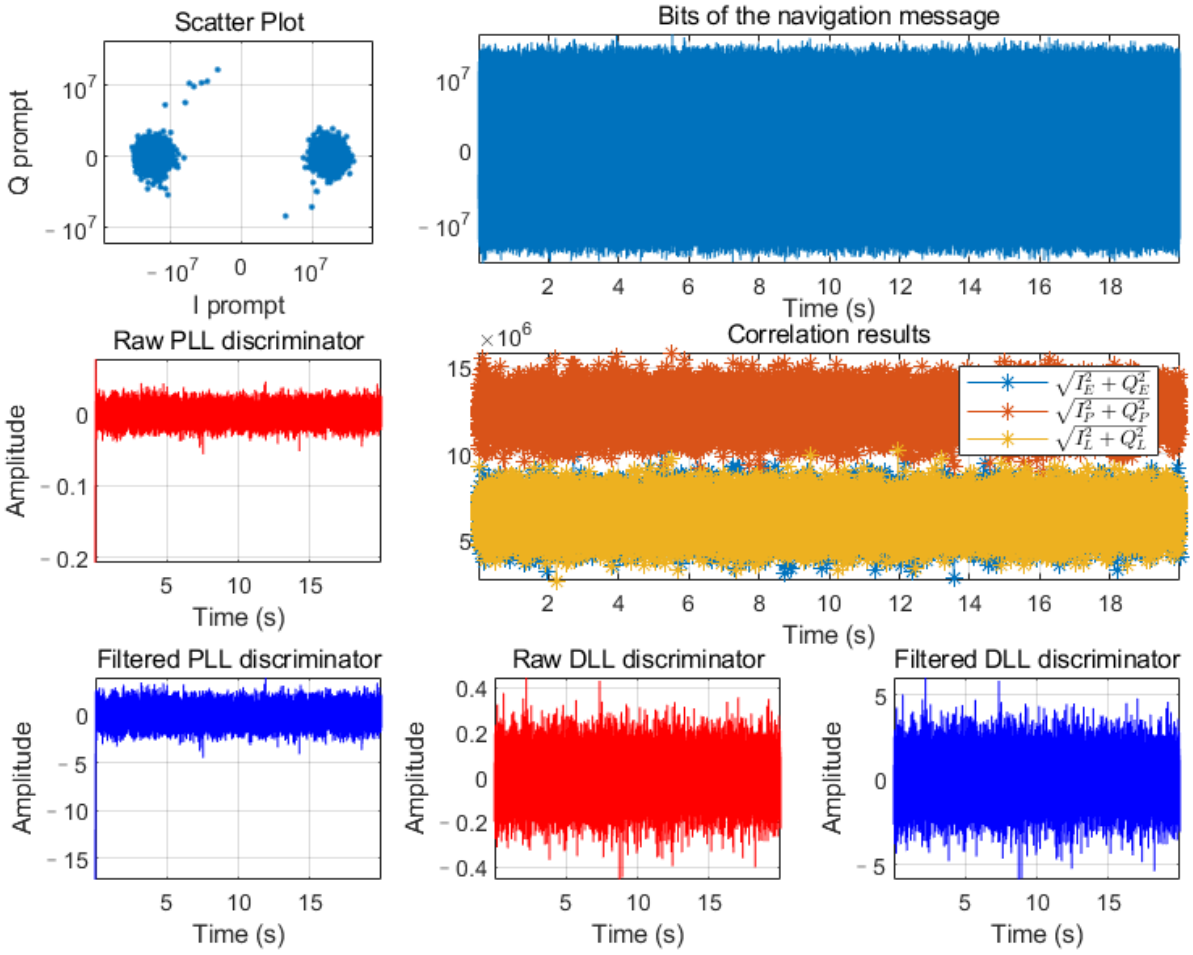


Figure 16. Results of the proposed strategy (C/N_0 = 50 dBHz, D = 1). (**a**) Obtained results of software receiver; (**b**) Code phase difference.

In Figures 17–19, the results of the proposed traction strategy are given under C/N_0 of 60 dBHz, 40 dBHz, and 30 dBHz, respectively.

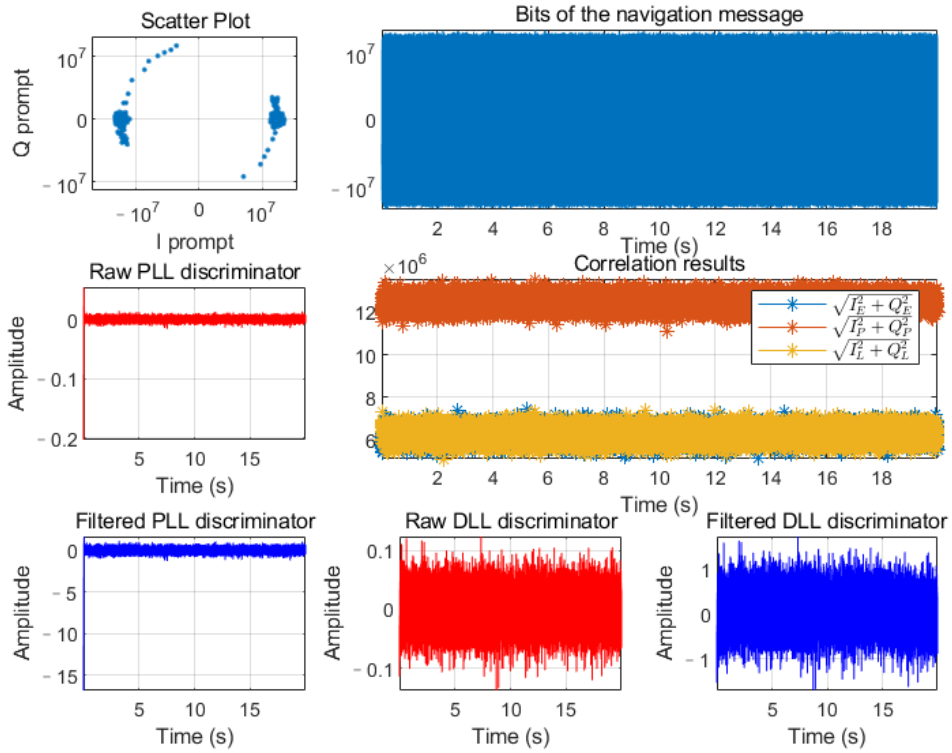


Figure 17. Tracking results of the proposed strategy (C/N_0 = 60 dBHz, D = 1).

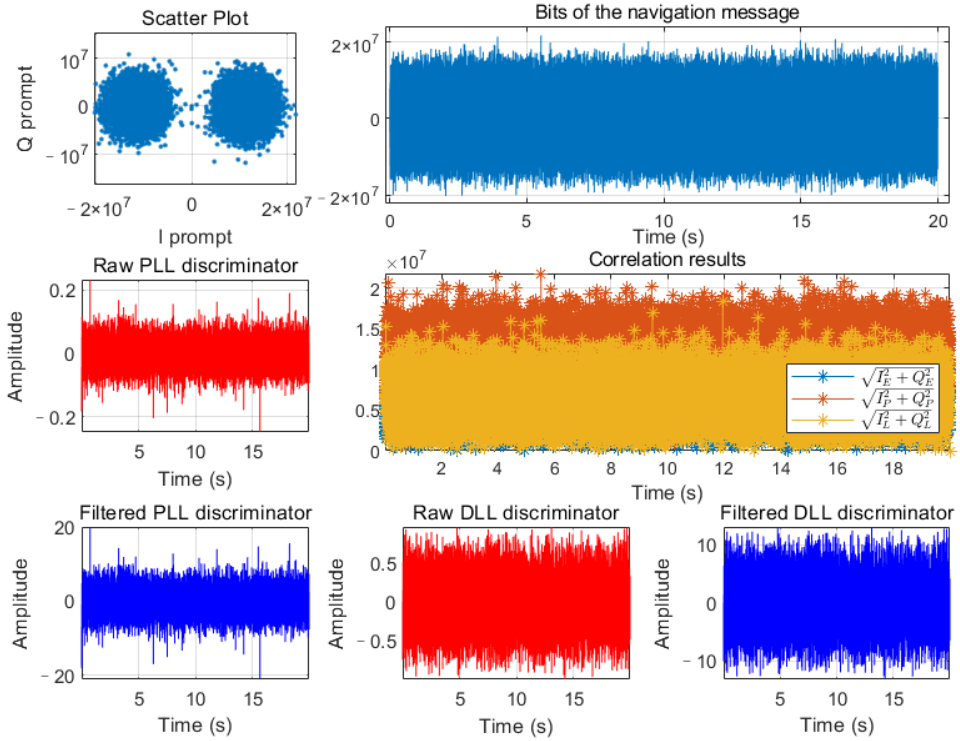
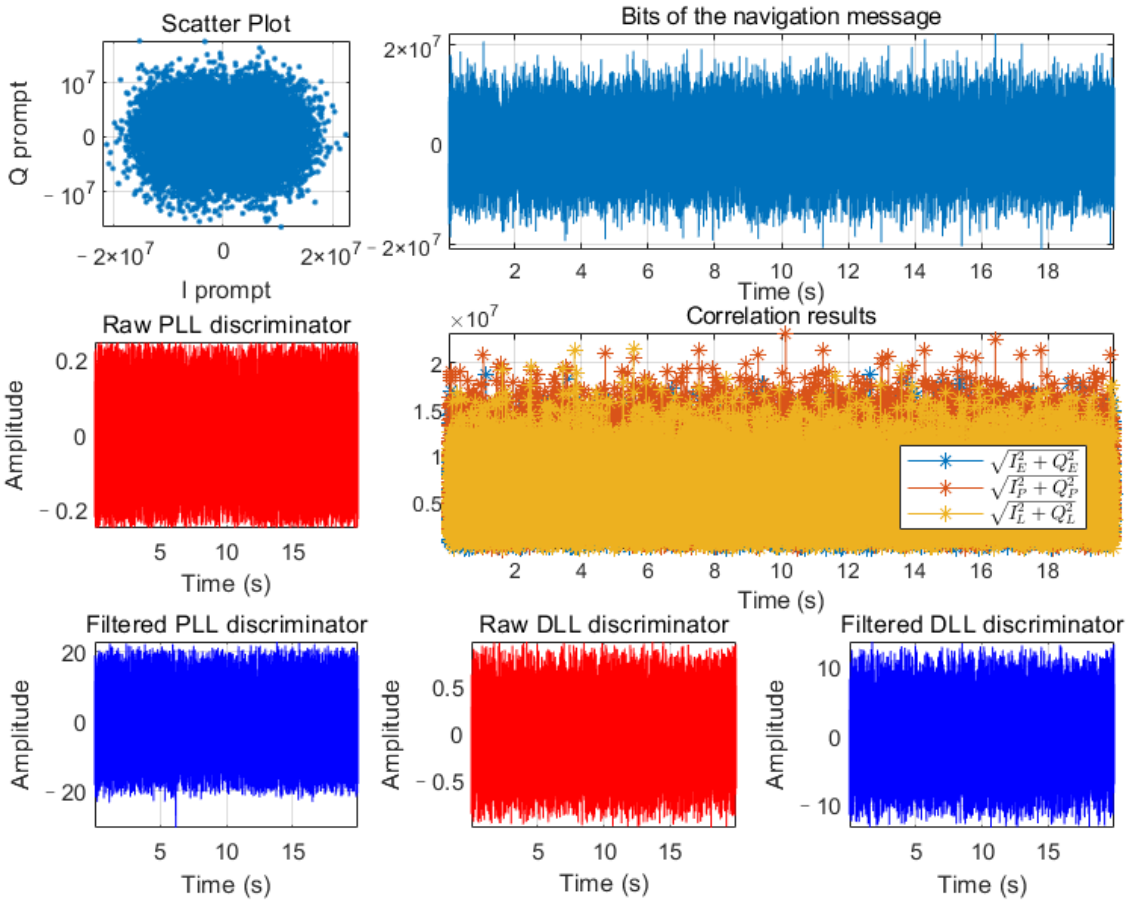
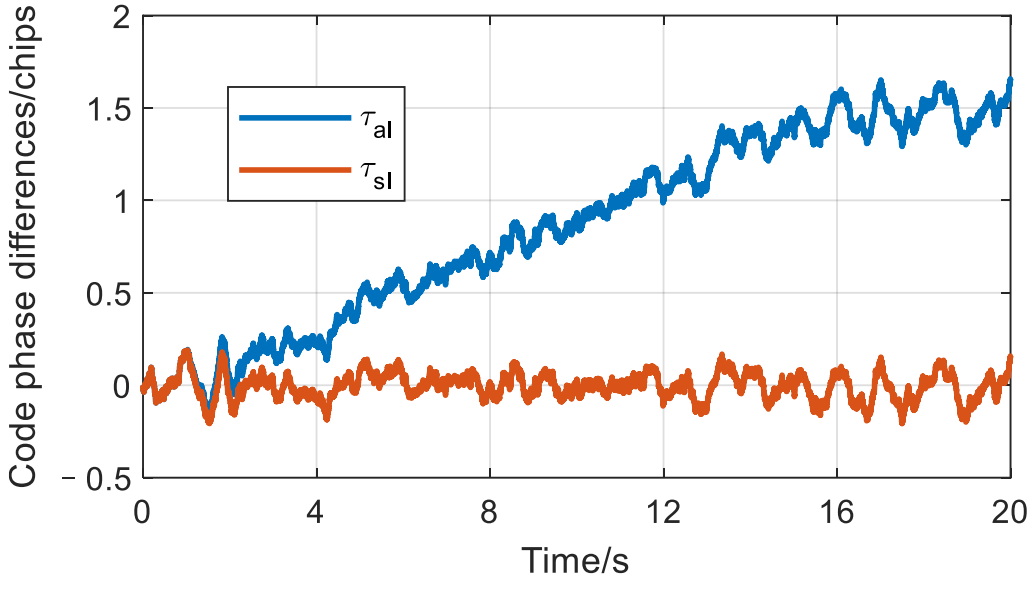


Figure 18. Tracking results of the proposed strategy (C/N_0 = 40 dBHz, D = 1).



(**a**)



(**b**)

Figure 19. Results of the proposed strategy (C/N_0 = 30 dBHz, D = 1). (**a**) Obtained results of software receiver; (**b**) Code phase difference.

Under a C/N_0 of 50 dBHz, the results obtained when the receiver is equipped with a narrow correlator are presented in Figure 20.

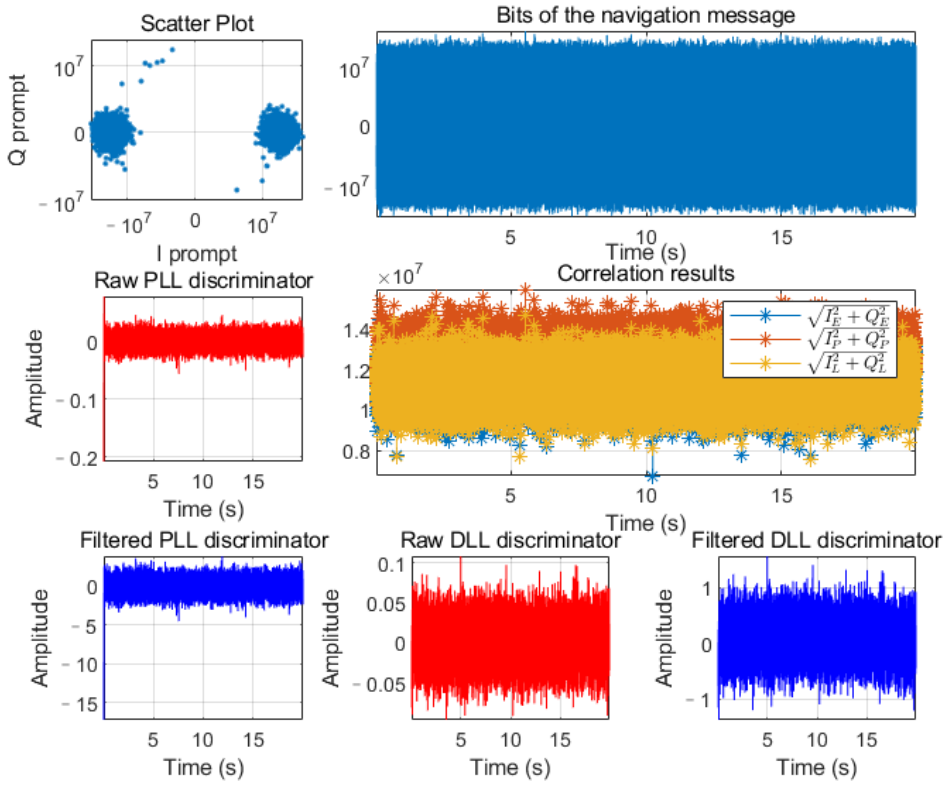


Figure 20. Tracking results of the proposed strategy (C/N_0 = 50 dBHz, D = 0.2).

3.3. Stability Testes

The RMSE statistics were calculated for the observations of genuine signals and the three traction strategies. The statistical results are presented in Tables 4–8.

Table 4. Comparison of RMSE for different strategies and the genuine signal (C/N_0 = 30 dBHz, D = 1).

RMSE	Genuine Signal	Strategy 1		Strategy 2		Proposed Strategy	
Code Doppler/cps	5.0126	4.8096	−4.05%	4.9474	−1.30%	5.0325	0.40%
Carrier Doppler/Hz	9.2118	8.1530	−11.49%	49.6585	439.07%	8.9270	−3.09%
Baseband signal power/dBHzm	11.7478	11.3715	−3.20%	11.7659	0.15%	11.4168	−2.82%

Table 5. Comparison of RMSE for different strategies and the genuine signal (C/N_0 = 40 dBHz, D = 1).

RMSE	Genuine Signal	Strategy 1		Strategy 2		Proposed Strategy	
Code Doppler/cps	3.8620	3.0380	−21.34%	3.8313	−0.79%	3.8527	−0.24%
Carrier Doppler/Hz	3.1576	3.0254	−4.19%	51.8225	1541.20%	3.1742	0.53%
Baseband signal power/dBHzm	4.7131	5.8102	23.28%	7.4685	58.46%	4.7356	0.48%

Table 6. Comparison of RMSE of different strategies and the genuine signal (C/N_0 = 50 dBHz, D = 1).

RMSE	Genuine Signal	Strategy 1		Strategy 2		Proposed Strategy	
Code Doppler/cps	1.3314	1.0161	−23.68%	2.3446	76.10%	1.3378	0.48%
Carrier Doppler/Hz	1.0219	0.9858	−3.53%	51.8179	4970.74%	1.0255	0.35%
Baseband signal power/dBHzm	1.4258	3.7214	161.00%	6.4803	354.50%	1.4225	−0.23%

Table 7. Comparison of RMSE for different strategies and the genuine signal (C/N_0 = 60 dBHz, D = 1).

RMSE	Genuine Signal	Strategy 1		Strategy 2		Proposed Strategy	
Code Doppler/cps	0.4255	0.3392	−20.28%	2.0826	389.45%	0.4327	1.69%
Carrier Doppler/Hz	0.4713	0.4657	−1.19%	51.7133	10,872.48%	0.4739	0.55%
Baseband signal power/dBHzm	0.4440	3.4613	679.57%	6.4441	1351.37%	0.4493	1.19%

Table 8. Comparison of RMSE for different strategies and the genuine signal (C/N_0 = 50 dBHz, D = 0.2).

RMSE	Genuine Signal	Strategy 1		Strategy 2		Proposed Strategy	
Code Doppler/cps	0.3338	0.2986	−10.55%	0.5735	71.81%	0.3453	3.45%
Carrier Doppler /Hz	1.0176	0.9403	−7.60%	1.7632	73.27%	1.0222	0.45%
Baseband signal power /dBm	1.4194	3.5533	150.34%	2.4744	74.33%	1.4155	−0.27%

Figures 21–24 presents the SQM metric in the same four cases.

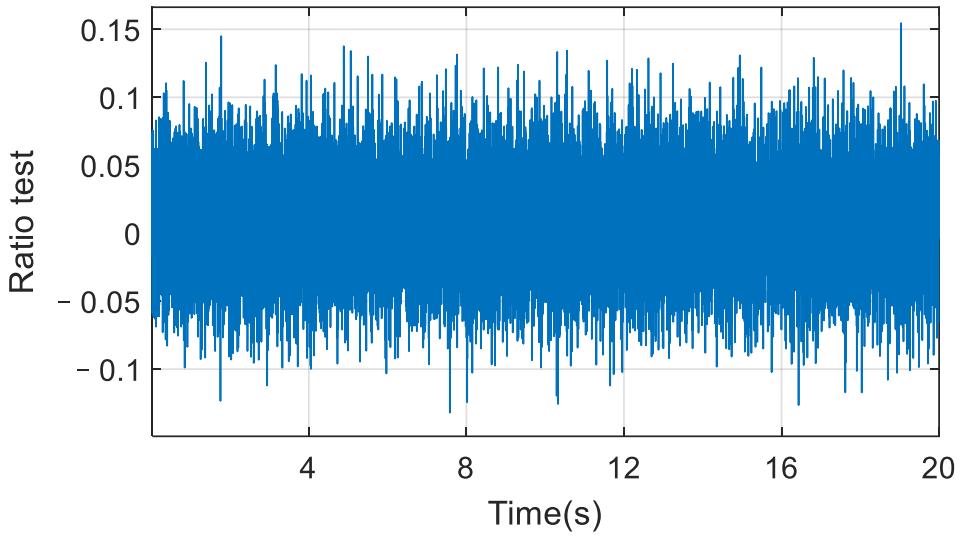


Figure 21. Ratio Test metric behavior of the genuine signal.

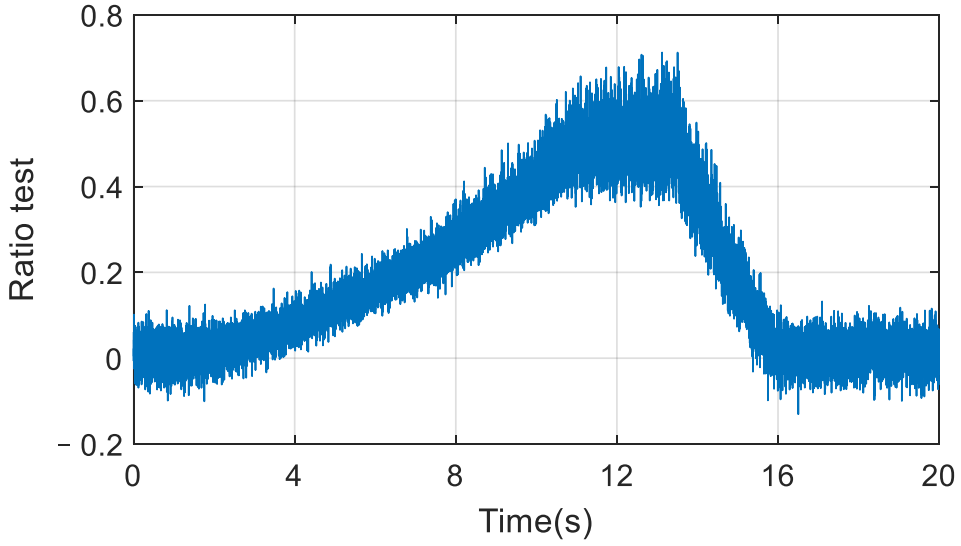


Figure 22. Ratio Test metric behavior under traction Strategy 1.

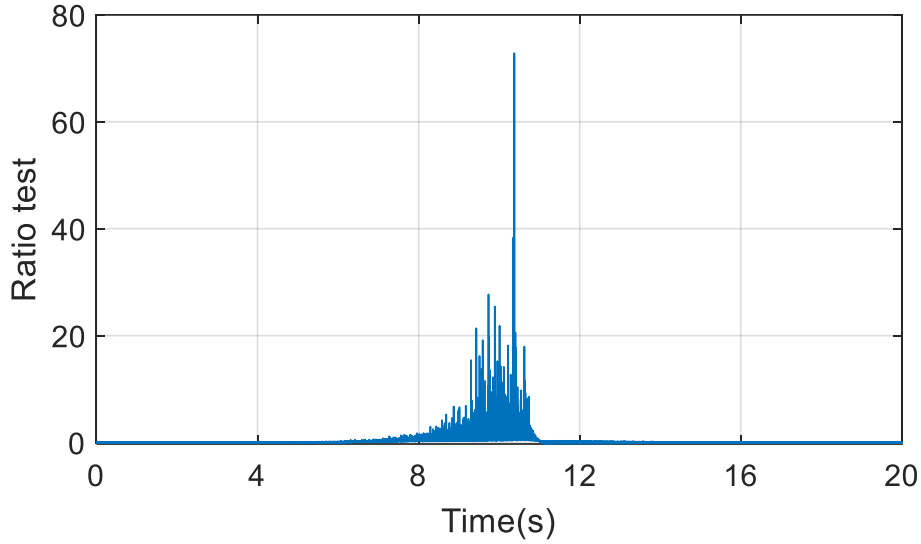


Figure 23. Ratio Test metric behavior under traction Strategy 2.

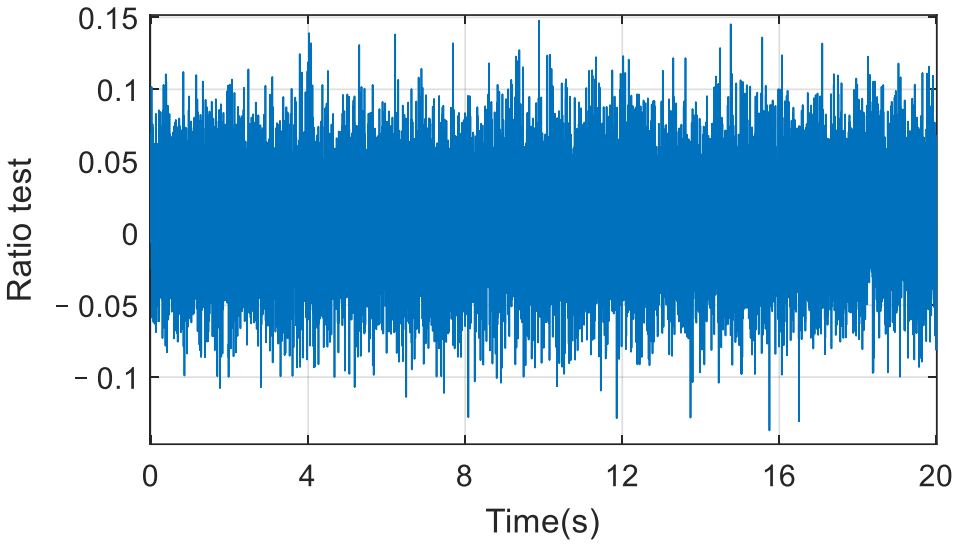


Figure 24. Ratio Test metric behavior under the proposed Strategy.

4. Discussion

4.1. Discussion on Simulation Results

This section discusses the results obtained in Section 3.1.

First, the advantages and theoretical feasibility of the proposed strategy compared to the conventional traction strategy are discussed.

The simulation results for the three strategies are presented in Figures 11–13. All τ_{sl} in Figures 11a, 12a and 13a finally approach 0, indicating successful code-loop traction of the three strategies. According to Figure 12f, the local Doppler fd_l is finally equal to the spoofing Doppler f_{drag}, and the carrier-loop traction of Strategy 2 is successful.

As can be observed in Figure 11a,c and Figure 12a,c, the code phase, code rate, and carrier frequency of the local loop cannot be followed up in real time, and there is a long loop adjustment process. Successful traction requires P_s to be at least equal to P_a within a certain period of time, which directly leads to considerable distortion when the correlation peaks are superimposed. The power will inevitably increase significantly, and distortion of the correlation peak and fluctuation of observations will be inevitable, as illustrated in Figures 11b and 12b. Therefore, conventional traction strategies are at risk of being detected

by power and TOA detection. Based on this limitation, a novel traction strategy for covert spoofing against TOA and power detection is proposed.

Therefore, because the conventional traction method risks being detected by power and TOA detection, we expect that the proposed strategy can circumvent these problems.

Figure 13 shows that the simulation results of the proposed method differ from those of the previous two methods. The conventional traction idea is a correlation peak superposition, and the spoofing signal slightly increases the spoofing signal power to take advantage. However, the proposed traction strategy essentially suppresses part of the genuine signals while realizing the generation of an ideal composite correlation peak.

The outputs of the correlators fluctuated slightly only when spoofing was added or when the traction speed returned to 0. This is because the adjustment process of the tracking loop causes τ_{al} to lag behind the changes in v_{drag} for a short period at the beginning and end of the traction. Most of the time, we have

$$v_{drag} t \approx \tau_{al} \tag{35}$$

Then we have

$$I_P(n) \approx \frac{\sqrt{P_a}}{2} T_{coh} R(0), \tag{36}$$

$$\delta_{cp} = \frac{I_E - I_L}{I_E + I_L} \approx \frac{R^-(0) - R^+(0)}{R^-(0) + R^+(0)} = 0 \tag{37}$$

Therefore, the proposed strategy is theoretically feasible. Compared to conventional strategies, it has a more ideal spoofing effect.

The second part is the comparison of two conventional strategies.

Compared with Strategy 1, it can be determined that Strategy 2 leads to the deterioration of the stability of the carrier loop, and the change in the phase discriminator output is more complicated owing to the influence of the carrier.

The third part is the discussion on traction speed and traction duration.

From Table 3, it can be observed that the value range of the traction speed is extended under the proposed strategy. Because the selection of v_{drag} directly affects the adjustment time of the loop traction, these two indicators must be weighed. In actual navigation wars, it is usually necessary to quickly seize the control of the tracking loop, and the traction time should not be too long, i.e., the traction speed should not be too slow. Compared to conventional traction strategies, the proposed strategy can more covertly and promptly control of the tracking loop.

4.2. Discussion on Experimental Results

This section discusses the experimental results obtained in Sections 3.2 and 3.3.

First, the results of these strategies are discussed to clarify the feasibility of the proposed strategy.

All τ_{sl} values in Figures 14a, 15a and 16a finally approach 0, indicating successful code loop traction of the three strategies. According to Figure 15a, the output of filter fd_l is finally equal to the spoofing Doppler f_{drag}, and the carrier loop traction of Strategy 2 is successful.

However, as shown in Figures 14a and 15a, each received observation has a different degree of distortion under the two conventional strategies. By comparing Figures 14–16 with Figures 11–13, it can be observed that the experimental results are consistent with the simulation results, which confirms the correctness of the simulations.

From Figure 15, it can be seen that the received observations of the proposed strategy are stable without distortion, and the code phase of the tracking loop follows the preset code phase of spoofing, which verifies the feasibility of the proposed strategy under noise.

The second part presents the analysis of the proposed strategy under different spoofing scenarios.

In Tables 4–8, it can be observed that the observations' RMSE percentage change in the proposed strategy is significantly better than those of Strategies 1 and 2, and the observations' RMSE percentage change in Strategy 2 is the worst. Based on these data, we can infer that in all designed spoofing scenarios, the implementation of the proposed strategy has no significant effect on the statistical value of the signal.

As shown in Figure 20 and Table 8, the obtained results of the narrow correlator are similar to those of the wide correlator. The proposed strategy can also address narrow pulse-aperture correlators.

Because the 30 dBHz C/N_0 is already a very weak GNSS signal, there will be some difficulties in estimating the genuine signal in the first step. In Table 4, significant changes in the observations are easily lost in the noise;therefore, the meaning of the obtained results is relatively limited. As shown in Figure 19a, the received results are very poor, which also means that there will be some difficulties in the acquisition and extraction of navigation messages. However, as can be seen from Figure 19b, the phase is successfully pulled, so the proposed spoofing traction strategy also exhibits good performance under the condition of a poor C/N_0.

In conventional Strategy 1, the statistics of code Doppler and carrier Doppler are small because this strategy directly superimposes spoofing signals of the same format, and the effect of correlation peak superposition is equivalent to power enhancement, thus reducing the output of the phase discriminator to a certain extent.

In special scenarios, such as a battlefield, the GNSS of the defense side may be enhanced to improve the service accuracy and reduce the possibility of spoofing. Figure 17 and Table 7 demonstrate that the proposed strategy performs well in the case of a power-enhanced signal.

The third part presents the performance analysis of the proposed strategy in the context of the SQM technique.

From Figures 21–24, it can be observed that the Ratio Test metric values of the genuine signal are in the range ± 0.15, while the metric values of Strategies 1 and 2 are far beyond this range. As expected, the metric values of the proposed strategy are within a safe range. The threshold value can be easily derived according to the theory presented in [13], given a determinate false detection probability. A threshold is built around the shape of the metric function, and can be used to detect the presence of distortions in real time. These results demonstrate that this strategy can bypass the SQM detection.

4.3. Limitations and Prospects

The proposed strategy has certain limitations. First, the proposed traction strategy is only for BPSK modulation and is suitable for the BeiDou Navigation Satellite System B1I and Global Positioning System L1C/A. Second, the proposed traction strategy is actually a variant of conventional Strategy 1. If the code-carrier coherence is detected, the proposed strategy may be detected when the traction speed is high. Finally, the scope of this study is limited to the generation of spoofing signals and the spoofing effect for a single satellite; multi-satellite positioning and timing spoofing have not been analyzed.

However, the traction concept of the proposed strategy is worth investigating. According to this idea, the traction code can be derived provided the nominal correlation function is given. Therefore, the applicability of the proposed strategy to other modulated signals should be investigated further. In the case of a high traction rate, necessary improvements can be made to maintain the code-carrier coherence and avoid detection. After the traction is completed, the influence of the proposed strategy on the subsequent message demodulation and positioning also needs to be analyzed.

5. Conclusions

The correlation peak superposition of conventional strategies rendersthe observations of the receiver unstable. The receiver only needs to perform mathematical statistics on the observations of the receiver to detect spoofing, such as TOA and power detection. We

assumed that we can design spoofing that can form an optimal correlation peak at the receiver to avoid the instability of the received results.

From the analysis of the desired ideal correlation peak, we determined that pseudo-code used in modulation could be replaced by a traction code, and this traction code was derived. The simulation and experimental results proved the feasibility of the traction code. Compared to conventional traction strategies, the proposed strategy has the following advantages:

1. The change in the phase discriminator output is small, and the code loop, carrier frequency, and baseband signal power are ensured to be stable. The observations' RMSE percentage change in the proposed strategy is significantly better than those of Strategies 1 and 2. The Ratio Test metric values prove that this strategy can bypass the SQM detection. Therefore, the proposed strategy can resist TOA and power detection.
2. Under the condition of a high or low C/N_0, the proposed spoofing traction strategy also exhibits an optimal good performance; hence, it is still effective when the GNSS signal is enhanced in the battlefield or when the signal quality is poor owing to the low elevation.
3. This strategy expands the range of traction speeds and has the potential to quickly and covertly accomplish traction.
4. The proposed strategy can also be applied to narrow- and pulse-aperture correlators.

Author Contributions: Conceptualization, N.J.; methodology, N.J. and Y.R.; software, N.J., X.C. and Y.G.; validation, N.J. and Y.R.; formal analysis, X.W. and N.J.; investigation, N.J.; resources, N.J., Y.R., X.W., D.Z. and X.C.; data curation, N.J. and Y.G.; writing—original draft preparation, N.J.; writing—review and editing, Y.R., X.W., D.Z., X.C. and Y.G.; visualization, N.J.; supervision, Y.R., X.W. and D.Z.; project administration, Y.R. and D.Z.; funding acquisition, Y.R., X.W. and D.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This study received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Qi, Y. Research on GNSS Multi Spoofing Strategy Based on Software Defined Receiver. Master's Thesis, Nanjing University of Aeronautics and Astronautics, Nanjing, China, 2019.
2. Zhou, X.; Li, G.; Cai, D.; Cheng, J. Review and Prospect of GNSS Anti-spoofing Techniques. *J. Navig. Position* **2013**, *1*, 79–84. [CrossRef]
3. Zhang, X. Overview of Satellite Navigation Spoofing Signal Detection Technology. *GNSS World China* **2018**, *43*, 1–7. [CrossRef]
4. Gao, Y.; Li, H.; Lu, M.; Feng, Z. Intermediate Spoofing Strategies and Countermeasures. *Tsinghua Sci. Technol.* **2013**, *18*, 599–605.
5. Dehghanian, V.; Nielsen, J.; Lachapelle, G. GNSS Spoofing Detection Based on Signal Power Measurements: Statistical Analysis. *Int. J. Navig. Obs.* **2012**, *2012*, 313527. [CrossRef]
6. Jahromi, A.J.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. *Int. J. Satell. Commun. Netw.* **2012**, *30*, 181–191. [CrossRef]
7. Mosavi, M.R.; Nasrpooya, Z.; Moazedi, M. Advanced Anti-Spoofing Methods in Tracking Loop. *J. Navig.* **2016**, *69*, 883–904. [CrossRef]
8. Cavaleri, A.; Motella, B.; Pini, M.; Fantino, M. Detection of Spoofed GPS Signals at Code and Carrier Tracking Level. In Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies/European Workshop on GNSS Signals and Signal Processing (NAVITEC), European Space Res & Technol Ctr, Noordwijk, The Netherlands, 8–10 December 2010.
9. Yang, Y.C.; Li, H.; Lu, M.Q. Performance Assessment of Signal Quality Monitoring Based GNSS Spoofing Detection Techniques. In Proceedings of the 6th China Satellite Navigation Conference (CSNC), Xi'an, China, 13–15 May 2015; pp. 783–793.
10. Zhang, P.; Lv, H. Research on GNSS Intelligent Coherent Tracking Spoofing Jamming Method andIts Effectiveness Analysis. *Mod. Navig.* **2018**, *9*, 163–171.
11. Fu, D.; Peng, J.; Ma, M.; Chen, F.; Ou, G. GNSS time spoofing detection and discrimination based on clock bias hypothesis test. *Syst. Eng. Electron.* **2022**, *44*, 948–955.

12. Gao, Y. Research on Key Technologies of Satellite Navigation Spoofing Interference. Master's Thesis, PLA Strategic Support Force Information Engineering University, Zhengzhou, China, 2020.
13. Fantino, M.; Molino, A.; Mulassano, P.; Nicola, M.; Rao, M. Signal Quality Monitoring: Correlation Mask Based on Ratio Test Metrics for Multipath Detection. In Proceedings of the International Global Navigation Satellite Systems Society, IGNSS Symposium 2009, Surfers Paradise, Australia, 1–3 December 2009.