electronics

MDPI

Article

A Novel GPS Meaconing Spoofing Detection Technique Based on Improved Ratio Combined with Carrier-to-Noise Moving Variance

Xuefen Zhu [1,*], Zhengpeng Lu [1], Teng Hua [1], Fan Yang [2], Gangyi Tu [3] and Xiyuan Chen [1]

[1] Key Laboratory of Micro-Inertial Instrument and Advanced Navigation Technology of Ministry of Education, School of Instrument Science and Engineering, Southeast University, Nanjing 210000, China; 220213669@seu.edu.cn (Z.L.); 220203499@seu.edu.cn (T.H.); chxiyuan@seu.edu.cn (X.C.)
[2] Shanghai Aerospace Control Technology Institute, Shanghai 200000, China; yangfan183292@163.com
[3] School of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210000, China; tugangyi@nuist.edu.cn
* Correspondence: zhuxuefen@seu.edu.cn; Tel.: +86-13645161372

Abstract: The Global Navigation Satellite System (GNSS) becomes vulnerable in a challenging environment, among which spoofing is the most dangerous threat. Meaconing, as the most convenient way to conduct spoofing, is widely studied around the world, and also leads to lots of research into corresponding anti-spoofing techniques. This paper develops a semi-hardware meaconing platform and proposes a novel GPS meaconing spoofing detection method based on Improved Ratio combined with Carrier-to-noise Moving variance ($C/N_0 - MV$). The effectiveness has been validated theoretically and experimentally. The proposed method is proven useful when the meaconing signal has 5 dB power gain over the authentic signal, presenting 98% detection rate whereas the classic Signal quality monitoring (SQM) method with the Ratio metric presents only 30%.

Keywords: improved ratio; Carrier-to-noise ratio variance; meaconing spoofing detection; signal quality monitoring

check for updates

Citation: Zhu, X.; Lu, Z.; Hua, T.; Yang, F.; Tu, G.; Chen, X. A Novel GPS Meaconing Spoofing Detection Technique Based on Improved Ratio Combined with Carrier-to-Noise Moving Variance. *Electronics* **2022**, *11*, 738. https://doi.org/10.3390/electronics11050738

Academic Editor: Athanasios Kanatas

Received: 20 January 2022
Accepted: 25 February 2022
Published: 27 February 2022

1. Introduction

More and more devices and services count on the PVT (Position, Velocity, Time) service, which is continuously provided by the Global Navigation Satellite System (GNSS) in all-weather conditions [1]. Better reliability and safety are required for multiple GNSS applications, such as police systems, power plant systems, air-to-ground transportation and criminal tracking. However, the service can be quite vulnerable when facing challenging environments including jamming, spoofing, city canyon, etc. Civil satellite signals are particularly vulnerable, given the fact their open structure makes the signal susceptible to different hackers and terrorist attacks. Among the attacking approaches, spoofing has the best concealment and can cause the most severe outcomes. Defined as a way to broadcast false signals in order to deceive receivers [2], spoofing can induce false GNSS solutions and trigger unexpected movement in all autonomous vehicles. Among all the spoofing experiments carried out so far, it is the most well-known that Iran captured American military's drone in 2011 [3]. Similar spoofing attacks have been proven effective on unmanned aircraft and electric power systems, which rely on the high timing from GNSS system [4,5].

The spoofing broadcast signals are similar to the authentic signal, and make the target receiver track the spoofing signal from the authentic signal with a power advantage, so that the receiver will generate the false positioning information. Two main classes of spoofing techniques have been proposed and tested, namely Signal Generation and Meaconing. Meaconing spoofing changes the delay of the authentic signal to the target receiver by forwarding the authentic signal, so that the receiver generates false pseudo-range, changing the position calculation of the receiver. The generation spoofing causes false navigation by generating the similar signals directly with the false position information in the satellite navigation message. A typical spoofing signal can be displayed as follows:

$$F_{si} = D_{si}[t]C_{si}[t - \tau_{si}(t)]e^{j[w_{sc}t - \phi_{si}(t)]} \tag{1}$$

where D_{si} is the estimated data bit of satellite i, C_{si} is the spreading code or C/A code, $\tau_{si}(t)$ is the code phase of the fabricated signal, and $\phi_{si}(t)$ is the corresponding carrier phase. To successfully deceive a receiver, the carrier beat frequency, carrier phase, code phase and data bits of satellite received in the targeted receiver need to be estimated with enough precision [2], or the sudden change of them can easily expose the spoofing signals. A spoofing system using software defined radio (SDR) was tested and proved useful by Mosavi [6]. However, it is obviously difficult for a spoofer to know the status of a target receiver unless the target is a willing victim, which invokes the idea of meaconing; the simplest way to conduct a spoofing attack [7]. If positioned adjacent to the victim, the attacker can estimate the carrier frequency and other features with much less effort. Several methods have been proposed for the successful implementation of meaconing [8–10].

Correspondingly, the updated ideas of spoofing lead to emerging detection methods, most of which focus on finding particular patterns or useful indicators of spoofing attack. Some non-sophisticated spoofing can be uncovered through the monitoring of received GNSS signal power, as the received signal power may display a sudden boost in the presence of spoofing from the analysis of the influence of spoofing signal power on GNSS signal power in the Cross correlation noise model [11]. Meanwhile, it is reported that the correlation peak of the correlation function between the received signal and the local signal will be distorted owing to the drag-off conducted by the spoofing signal [12]. To detect the spoofing, Broumandan tested and analyzed the variance of this distorted correlation peak (variance analysis), excessive amounts of structured signal power in received signals (Structural Power Content Analysis method) and Signal Quality Monitoring along with the Ratio Metric at the beginning of attacks from the spoofing signal [13,14]. Besides, external auxiliary equipment, including multiple antennas and IMU sets, are always used in spoofing detection. From the differences in spatial information of the spoofing signal and authentic signal, such as the arrival angles of the signals, multiple antennas could detect the spoofing signal and tell the direction where the signals come from [15,16], while IMU sets the focus on the inconsistency between the GNSS solutions and IMU solutions [17,18]. To precisely detect spoofing, some creative ideas like using a multipath effect, asymmetric encryption, or repeated acquisition have been suggested [19–21].

The main drawbacks of the mentioned strategies can be summarized as follows:

- The existence of distortions of SPCA, SQM or variance analysis can only be observed for a short moment, making them easily missed.
- The implementation of an external auxiliary can be rather troublesome and expensive for civil applications.
- The encryption method needs adjustment to all currently used satellites and receivers, which is extremely expensive.
- The repeated acquisition and multipath effect require a lot of extra computations in the receiver, causing unnecessary burden and delay.

As a solution to the problems mentioned above, we propose the use of Improved Ratio combined with Carrier-to-noise Moving variance ($C/N_0 - MV$) to detect meaconing spoofing signals, which is theoretically verified and experimentally testified in this paper.

The combined spoofing detection method does not require external equipment such as antennas or making changes to existing satellite navigation systems. It just makes some improvements in the satellite receiver, and also brings less computational load to the receiver. At the same time, compared with the traditional methods such as SQM with Ratio metric, the combined method improves the threshold of spoofing detection and could reduce the false detection caused by other interference such as changes in the elevation of the satellite. In addition, in the combined spoofing detection method, we are still able to observe the different detection index between the normal receiver and the deceived receiver after the satellite receiver tracks the deception signal stably.

This study makes a contribution to designing an accurate and efficient receiver with spoofing jamming detection methods, and improves the robustness of GNSS. As such, this study is of great significance to maintaining the normal operation of GNSS. In addition, with the increasingly widespread application of satellite navigation in civil fields such as smart transportation and autonomous driving, we believe that this combined method for detecting meaconing spoofing can effectively improve the reliability and security of GNSS in these civil fields.

The remainder of the article will be structured as follows. Section 2 introduces the spoofing detection system. Section 3 introduces the methodology, especially the extraction of Carrier-to-noise Moving variance and Improved Ratio. Section 4 introduces the procedures and results of experiments and analyzes the discovery. Section 5 concludes this paper with a summary of the experiments and the effectiveness of the proposed methods.

2. Spoofing Detection System and Data Collection

The spoofing detection system is composed of a semi-hardware meaconing system and detection software, which will be introduced with the details provided on the system structure, the chosen devices and the operation flow of the detection software.

2.1. The Meaconing Spoofing System

Firstly, a meaconing system has been developed with a hardware GNSS signal simulator, a hardware intermediate frequency signal sampler and a software defined GNSS receiver (SDR), as exhibited in Figure 1.

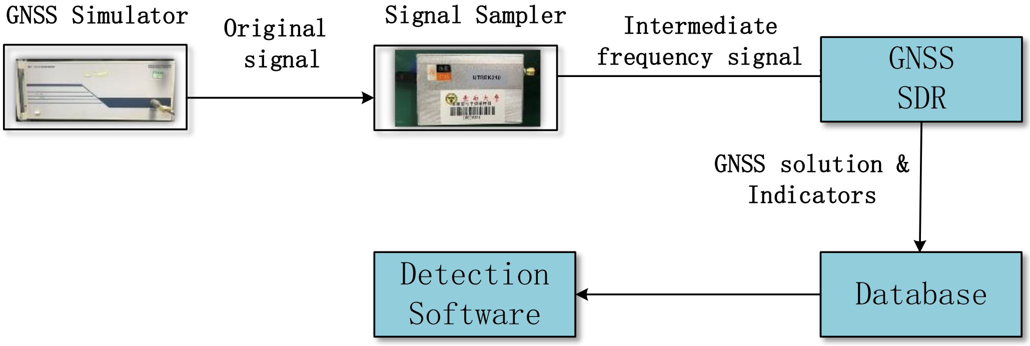


Figure 1. The meaconing system.

In this system, the GNSS simulator generates the original GNSS signal and the meaconing signals, the signal sampler receives the signals from the GNSS simulator and transmits an intermediate frequency signal to a GNSS software defined receiver (SDR), and a GNSS solution, with possibly useful indicators, are extracted and stored in a database, which are later sent to the detection software.

The GNSS simulator used in the experiment is the NSS8000, developed by the National University of Defense Technology (NUD). This simulator is a high-precision RF signal simulation equipment for GNSS. This simulator can simulate satellite signals of BDS/GPS/GLONASS/Galileo navigation system. The differences between the original signal and the meaconing signal are signal delay and signal power. The key parameters of the original signal and the meaconing signals generated by the simulator in this experiment are shown in Table 1.

As shown in Table 1, the four simulated signals are GPS L1 signals with a center frequency of 1575.42 MHz. Compared to the original signal, each meaconing signal delay is 500 ns. The power of each signal also has been given.

Table 1. Key parameters of simulated signals.

Simulated Signals	Center Frequency	Signal Delay	Signal Power
original signal	GPS L1 (1575.42 MHz)	0 ns	−130 dBm
meaconing signal 1	GPS L1 (1575.42 MHz)	500 ns	−127 dBm
meaconing signal 2	GPS L1 (1575.42 MHz)	500 ns	−125 dBm
meaconing signal 3	GPS L1 (1575.42 MHz)	500 ns	−122 dBm

The intermediate frequency signal sampler is UTREK210, as displayed in Figure 1. The sampler receives from the simulator and sends signals to the computer through a serial port. The intermediate frequency is set 4.5 MHz and the sampling rate is 19.1 MHz.

The database is combined with these key variables from the output of the receiver, and they are positioned by information in X, Y and Z directions, the carrier beat doppler, code doppler, Carrier-to-noise ratio C/N_0, three correlations from early, present and late in-phase channels, and also three correlations from early, present and late quadrature channels. The receiver outputs these variables every 1 ms and, since our experiments lasted for 120 s, each variable has 120,000 data.

2.2. The Detection Software

Figure 2 presents the operation flow of the detection software. Upon initiation, it extracts a sample from the database and examines the current flag. The flag is set by analyzing the $C/N_0 - MV$, an indicator able to tell if there is any interference including multipath or spoofing. Once the flag is set, the proposed Improved Ratio is automatically calculated, and compared with the upper threshold and the lower threshold later to determine the potential of meaconing spoofing.

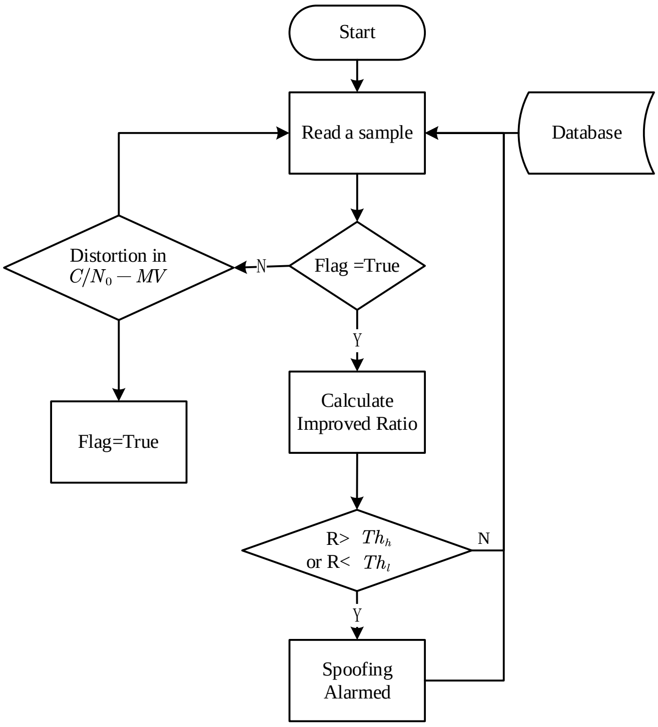


Figure 2. The operation flow of the detection software.

The $C/N_0 - MV$ in the software functions like the computation complexity-saving mechanism and a primary filter. The irregular distortion of it can exclude some lasting environmental noise like city canyon, multipath and low satellite elevation angle, which may bring in noise, however does not lead to the sudden change of $C/N_0 - MV$.

As shown in Figure 2, the $C/N_0 - MV$ is the Carrier-to-noise ratio Moving variance, R is the Improved Ratio proposed in this paper, Th_l is the lower threshold and Th_h is the upper threshold.

3. Methodology

3.1. Derivation of the $C/N_0 - MV$

As depicted in Figure 2, a $C/N_0 - MV$ method is employed as the indicator to imply possible interference like spoofing. It is reported that C/N_0 is useful in revealing spoofing attacks in the environment [22], which may however cause a false alarm when the satellite elevation angle is mistakenly too low for spoofing signals. C/N_0 detection method detects spoofing signal by setting a certain threshold, however the change of satellite elevation angle will also lead to the slow decrease in Carrier-to-noise ratio, which leads to the false detection. When the spoofing signal begins to attack the receiver, the original value of C/N_0 received by the receiver fluctuates greatly. Therefore, this phenomenon is considered to design a method with a high detection threshold for spoofing detection to improve the accuracy of detection. The variance is specially used to characterize the dispersion of a set of data, and it can reflect the changing degree of C/N_0 at the beginning of the spoofing attack. Meanwhile, the variance is not sensitive to the normal change of the satellite elevation angle [13], which means that it can reduce the false detection caused by the satellite elevation angle.

Signal-to-Noise Ratio (SNR) is always adopted to judge the quality of GNSS signals, which is defined as the ratio of signal power (P_R) to noise power (N). While Carrier-to-noise ratio (C/N_0) is defined as the ratio of signal power (P_R) to the noise power spectral density (N_0). The relationship between them can be expressed as follows:

$$N = N_0 B_n \tag{2}$$

$$C/N_0 = SNR \times B_n \tag{3}$$

where B_n is the noise bandwidth.

Apparently, the C/N_0 will decline if the noise floor inclines, which is how the meaconing spoofing signal affects the signal C/N_0.

Assuming the output of the correlation function in branch l of the acquisition loop can be expressed as follows:

$$y_l = \sqrt{P_l}\exp(\varphi_l) + \sum_{i=1,i\neq l}^{N} \sqrt{P_i}R_{il} + \sum_{k=1}^{N_s} \sqrt{P_k}R_{kl} + \eta \tag{4}$$

where y_l is the output of the correlation function, P_l is the power of the received signal power of satellite l, P_i is the power of the received signal power of satellite i,N is the number of observable satellites, R_{il} is the correlation function between branch l and signal of satellite i, k refers to the spoofing signal of satellite k, P_k is the power of the spoofing signal, R_{kl} is the is the correlation function between branch l and spoofing signal of satellite k, N_s is the number of spoofing signals, and η is the random noise.

Generally, the correlation function of the authentic signal from the satellite i will dominate in y_l after successful acquisition, in which the remaining three parts are treated as noise, and thus Equation (4) can be presented as follows:

$$y_l = \sqrt{P_l}\exp(\varphi_l) + e_1 + e_2 + \eta \tag{5}$$

$$e_1 = \sum_{i=1,i\neq l}^{N} \sqrt{P_i}R_{il}, e_2 = \sum_{k=1}^{N_s} \sqrt{P_k}R_{kl} \tag{6}$$

Undoubtably, meaconing signals will increase the noise floor, as a consequence of which, the C/N_0 extracted from the acquisition will decrease. With the rise of the power of spoofing signals, the noise caused by cross-correlation (e_1) will stay steady, whereas the noise caused by meaconing (e_2) will increase and eventually surpass the original signal ($\sqrt{P_l}\exp(\varphi_l)$).

However, high noise floor is not definitely caused by spoofing signals, just as is often observed when the satellite elevation angle is low or in a multipath environment. As the improvement of simple C/N_0, $C/N_0 - MV$ is proposed as an indicator for spoofing detection. As presented in Figure 3, a sliding window is employed to perform the calculation of moving variance.

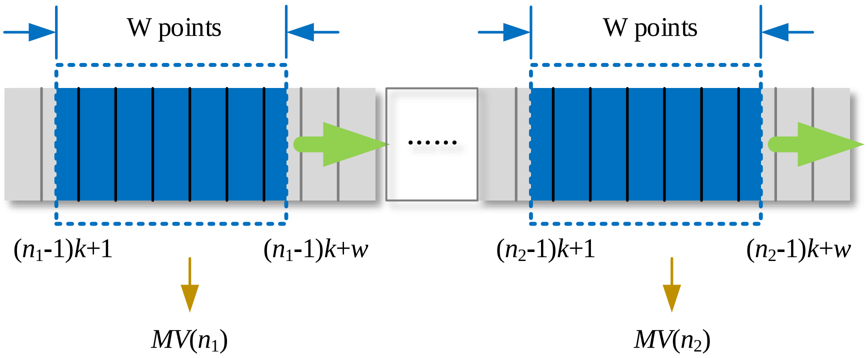

W points
W points
......
$(n_1\text{-}1)k\text{+}1$
$(n_1\text{-}1)k\text{+}w$
$(n_2\text{-}1)k\text{+}1$
$(n_2\text{-}1)k\text{+}w$
$MV(n_1)$
$MV(n_2)$

Figure 3. Sliding window model.

As shown in Figure 3, where W is the length of the window, $MV(n_1)$ is the n_1th moving variance.

The nth moving variance can be expressed as follows:

$$MV(n) = \frac{1}{w}\sum_{i=(n-1)k+1}^{(n-1)k+w}[x(i) - E(X)]^2 \quad (7)$$

where w is the length of the moving window, which is 200 or 0.4 s in the experiment, $x(i)$ is the correlation value at the point i, $E(X)$ is the average of w points, k is the sliding interval, and a threshold of the $C/N_0 - MV$ is set to detect spoofing signals.

3.2. Derivation of Improved Ratio

With obvious distortion at the beginning of spoofing, Signal quality monitoring (SQM) is widely used to detect the spoofing signal. SQM detection is the method to detect the distortion degree of the distorted correlation peaks.

Ratio metric or Delta metric are widely used in SQM detection. Considering there is an improvement in Ratio in the combined method in this paper, we choose the Ratio metric as a comparison, which is defined as follows [23]:

$$Ratio = \frac{E_I + L_I}{P_I} \quad (8)$$

where E_I is the coherent integral of correlation of early in-phase channel, P_I is the coherent integral of correlation of present in-phase channel and L_I is the coherent integral of correlation of late in-phase channel. All three coherent integrals are on the I branch.

However, the tracking loop is not stable when disturbed, as this causes a distribution of signal power to the quadrature arm. The proposed Improved Ratio makes full use of the correlation results in the quadrature arm, which is ignored by the previous Ratio defined in Equation (8) and employs an incoherent integral to combine the correlation functions of two arms. The Improved Ratio is defined as follows:

$$R_{improved} = \frac{E + L}{2P} \quad (9)$$

$$E = \sqrt{E_I^2 + E_Q^2}\ P = \sqrt{P_I^2 + P_Q^2} L = \sqrt{L_I^2 + L_Q^2} \tag{10}$$

where $R_{improved}$ is the Improved Ratio proposed in this paper, E_I is the correlation of the early in-phase channel, E_Q is the correlation of early quadrature channel, P_I is the correlation of present in-phase channel, P_Q is the correlation of early quadrature channel, L_I is the correlation of late in-phase channel, L_Q is the correlation of late quadrature channel.

As shown in Figure 4, the correlation function of both arms is squared and added up to get the Improved Ratio. The Improved Ratio is later compared with an upper threshold and a lower threshold to determine if there is a spoofing signal.

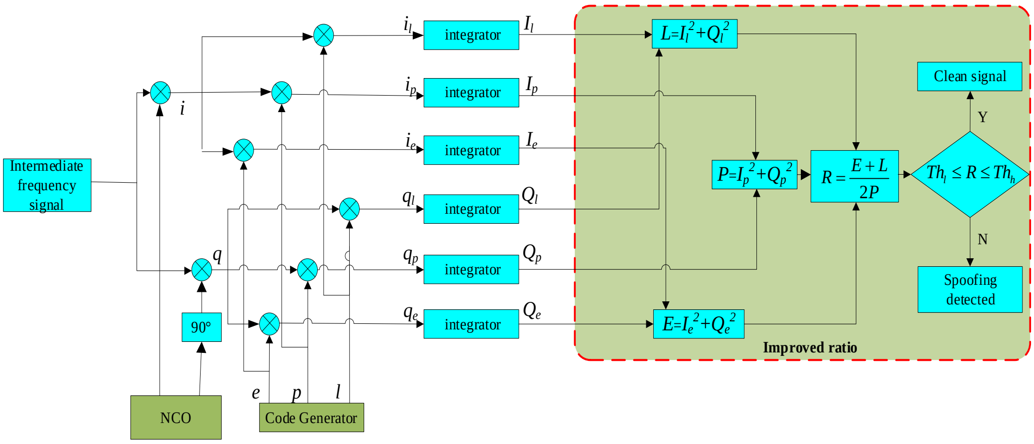


Figure 4. Detection model with Improved Ratio.

In Figure 4, NCO is the carrier generator, i_L, i_P, i_E, q_L, q_P, q_E are the correlation functions of in-phase arm and quadrature arm, with I_L, I_P, I_E, Q_L, Q_P, Q_E being the corresponding integrals, R is the Improved Ratio composed of E, P, L, Th_l is the lower threshold and Th_h is the upper threshold.

4. Results and Discussion

4.1. Meaconing Spoofing Detection Experiment

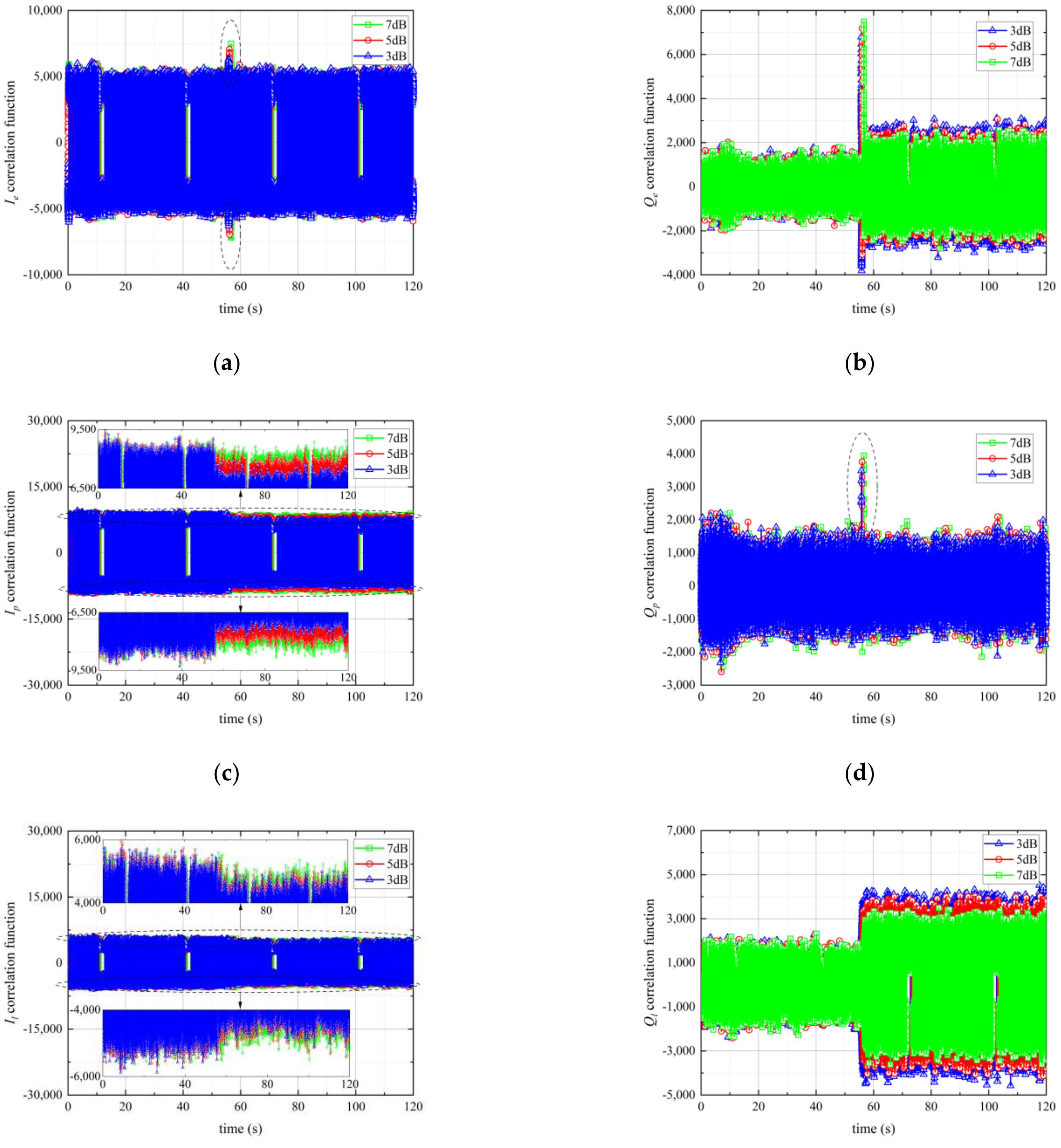
The experiment was conducted by the following steps:

- Clean GNSS signal was generated and transmitted by the meaconing spoofing system in Figure 1 for the first 56 s, with data extracted from the SDR and stored in the database.
- The GNSS simulator generated the meaconing signal, along with the clean signal and sent them through the whole system. Data were recorded and saved at the meantime.
- We repeated the steps above with different power gain and delay set to meaconing signals.
- The detection software was later run upon the data kept in database.

Only the signal with 500 ns delay is selected for analysis and discussion in this paper. As a reasonable explanation, the correlation peak of meaconing signal is too close to the original signal to perform a conspicuous drag-off that can be observed and analyzed in the situation where the delay is less than 500 ns, while in the circumstance of delay more than 500 ns, the drag-off is unsuccessful as the correlation peak of the meaconing signal is too far from the clean signal to be noticed by the tracking loop.

As shown in Figure 5 below, the correlation function of each channel from either arm is displayed separately.

Evidently, the correlation function of every channel presents distortion when the spoofing signal appears, which clarifies that the receiver is affected by the meaconing signal. Among them, channel E from the in-phase arm and channel P from the quadrature arm presents only a moment of distortion, while the other four displayed various degrees of long-term change.



(**a**)

(**b**)

(**c**)

(**d**)

(**e**)

(**f**)

Figure 5. The Correlation Function of Each channel from either Arm: (**a**) Correlation Function of E Channel from In-phase arm; (**b**) Correlation Function of E Channel from Quadrature arm; (**c**) Correlation Function of P Channel from In-phase arm; (**d**) Correlation Function of P Channel from Quadrature arm; (**e**) Correlation Function of L Channel from In-phase arm; (**f**) Correlation Function of L Channel from Quadrature arm.

In Figure 5, E channel is the early channel, P channel is the present channel, L channel is the late channel, the blue '3 dB' means the meaconing signal has 3 dB power gain over the authentic GNSS signal, the red '5 dB' means 5 dB power gain and the '7 dB' means 7 dB power gain.

As shown in Figure 6 below, it presents the carrier beat doppler and code doppler when we add spoofing signals with different power gain. Significant hopping change can be recognized in the figures, which is bigger if the spoofing signal has stronger power gain.

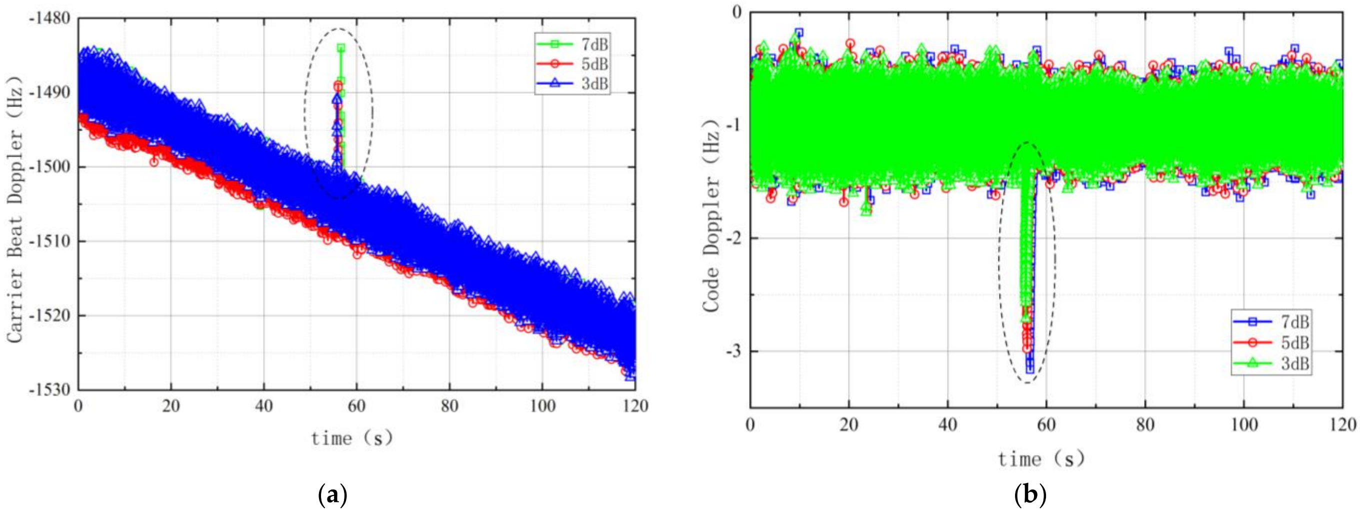


Figure 6. Carrier Beat Doppler Shift and Code Doppler Shift Changes. (**a**) The Carrier Beat Doppler Shift; (**b**) The Code Doppler Shift.

In Figure 6, the blue one is the Carrier/Code Doppler Shift curve line under the 3 dB spoofing signal, the red one is under the 5 dB spoofing signal and the green one is under the 7 dB spoofing signal.

As the confirmation of successful spoofing, the corresponding GPS solution is analyzed as shown in Figure 7. After imposing the meaconing signal at the 56 s point, the position from the GPS solution has a dramatic change, in which there is 50 m in x axis, 150 m in y axis and 80 m in z axis under the ECEF reference frame.

In Figure 7, the axis is under the ECEF reference frame, the green is the position under 3 dB spoofing signal, the red curve is under 5 dB spoofing signal and the blue curve is under 7 dB spoofing signal.

4.2. Spoofing Detection

4.2.1. The Effectiveness of SQM Detection with Ratio Metric

As we chose a Ratio metric in SQM detection as a comparison, we analyzed the Ratio of each satellite channel. As shown in Figure 8, the Ratio remains steady around 0.5 and later presents a stable bias after a jumping change, and it increases to 0.64 when the spoofing power gain is 3 dB, 0.52 when the gain is 5 dB, and 0.5 when the gain is 7 dB.

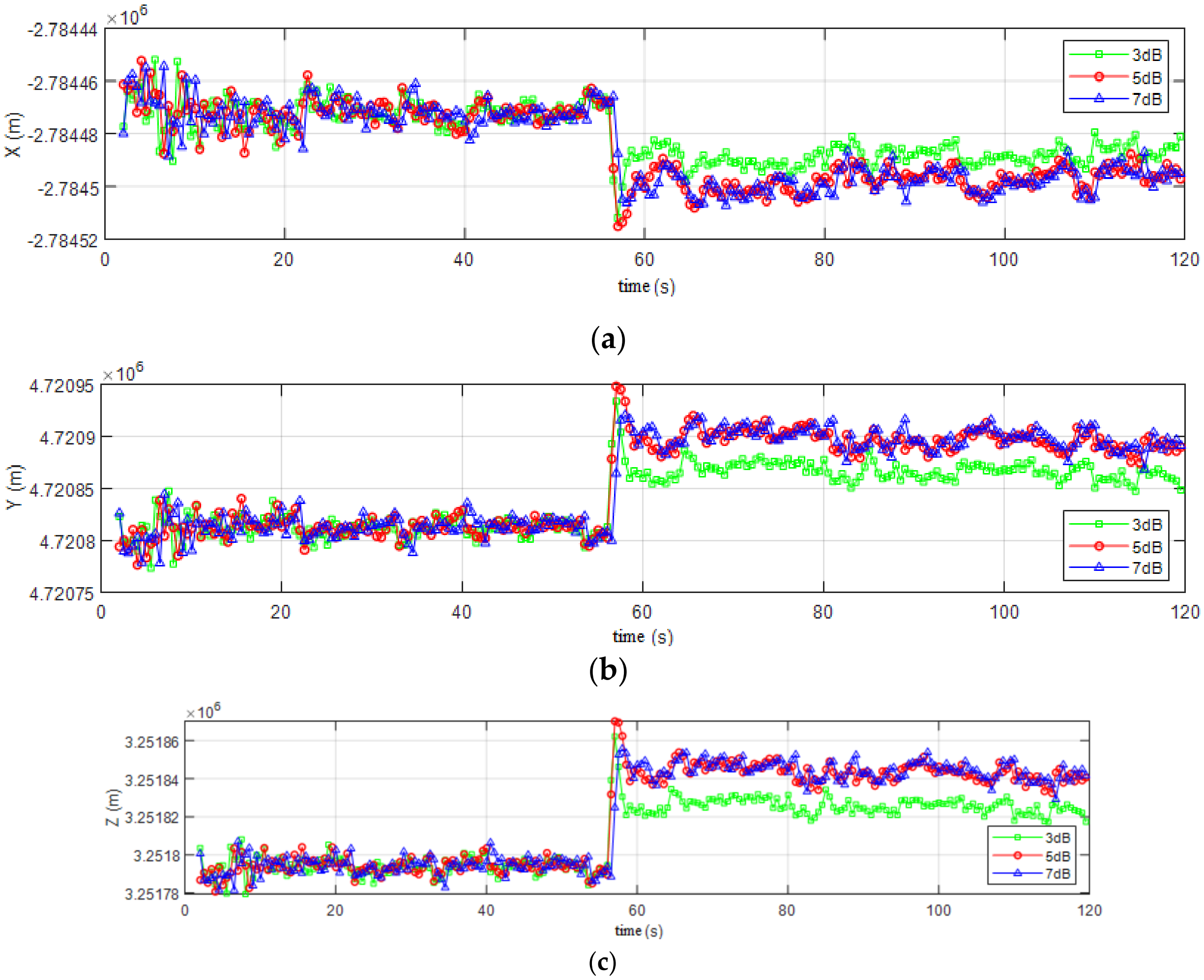
However, the change is hardly perceptible at the 7 dB gain, which means it is nearly impossible to tell the difference from the clean signal. It appears that with the increasing spoofing power gain, the gap between clean signal and spoofed signal gets more and more narrow. As a reasonable explanation, after being spoofed, the authentic signal is forced to play the role of noise and makes less contribution to the noise floor if the spoofing power gets stronger.

4.2.2. The Effectiveness of $C/N_0 - MV$

The effectiveness of $C/N_0 - MV$ as the trigger for spoofing detection is evaluated in comparison with simple C/N_0 in the first place.

As shown in Figure 9, we make a comparison between the C/N_0 and the $C/N_0 - MV$. The C/N_0 maintains stability at a level of 50 dB-Hz before the spoofing signal is added, and drops later when the spoofing signal is presented at 56 s point. The C/N_0 declines to 41 dB-Hz, 39 dB-Hz and 37 dB-Hz separately when the corresponding spoofing signal has

3 dB, 5 dB and 7 dB power gain, which confirms the idea that noise floor increases with the power gain of the spoofing signal.



(**a**)

(**b**)

(**c**)

Figure 7. The Position of Receiver in Spoofing Environment: (**a**) Position in X direction; (**b**) Position in Y direction; (**c**) Position in Z direction.

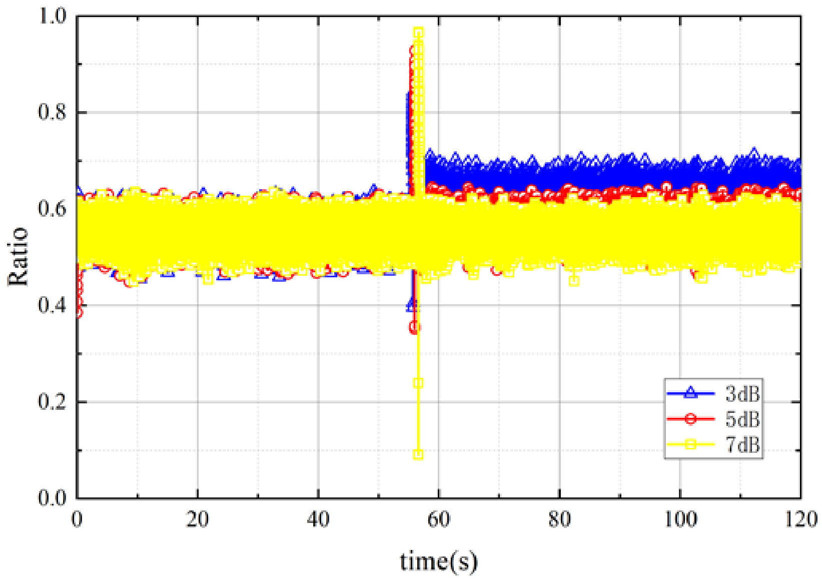


Figure 8. The Ratio with different spoofing power gain.

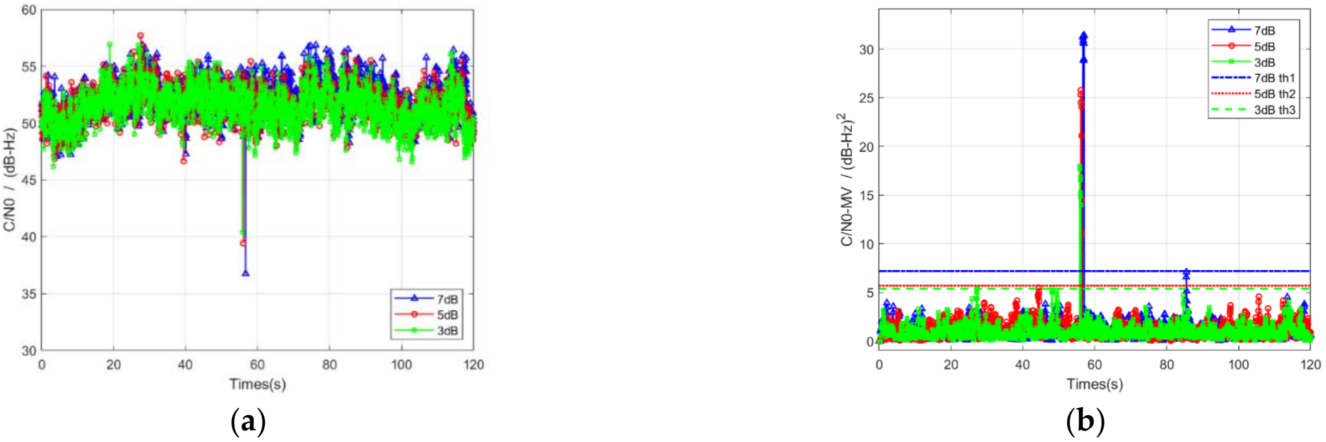


Figure 9. The C/N_0 and the $C/N_0 - MV$ with Different Spoofing Power Gain: (**a**) C/N_0 with Different Spoofing Power Gain; (**b**) $C/N_0 - MV$ with Different Spoofing Power Gain.

In Figure 9, the blue line is the 7 dB curve, the red line is the 5 dB curve and the green line is the 3 dB curve.

As a contrast, the $C/N_0 - MV$ displays a more considerable distortion when it encounters a meaconing signal. It is apparent that higher spoofing power gain provokes higher $C/N_0 - MV$ at the moment when spoofing signal appears. The thresholds are set 5.4 $(dB - Hz)^2$, 5.7 $(dB - Hz)^2$, 7.2 $(dB - Hz)^2$ separately in response to the spoofing signal with 3 dB gain, 5 dB gain and 7 dB gain.

As the results indicate, the $C/N_0 - MV$ outperforms the C/N_0 in the function as the trigger for successive detection by Improved Ratio.

4.2.3. The Effectiveness of Improved Ratio

As shown in Figure 10, it illustrates the Improved Ratio and the Ratio of satellite G13 with different spoofing power gains. The Ratio is analyzed in Section 4.2.1. The Improved Ratio is stable before the presence of a spoofing signal and has a stable bias after a jumping change when spoofing is implemented. Three figures show the performance and difference of the Improved Ratio and Ratio when the spoofing power gain is 3 dB, 5 dB and 7 dB. Figure 10 obviously shows that the increase in the improved Ratio is much more noticeable than that of the Ratio under the same spoofing power gain.

In comparison with the previously defined Ratio, Figure 10 demonstrates the Improved Ratio, which is represented by red points when spoofing signals with different power gain is added. The improved Ratio stands around 0.5 and presents an increase with a jumping change after the implementation of the spoofing attack, and later presents a stable bias. It increases to 0.74 when the spoofing power gain is 3 dB, 0.65 when the gain is 5 dB, and 0.58 when the gain is 7 dB, while the Ratio is 0.64, 0.52 and 0.5, respectively.

4.2.4. Analysis of Combined Method and SQM Detection with the Ratio Metric

A hypothesis testing method is employed to analyze the result. From the flow chart in Figure 2, we could find that the Spoofing attack is alarmed when the improved Ratio is found above Th_l or below Th_h, so as the following hypothesis:

$$\phi(n) = \begin{cases} 0 \sim H_0,\ Th_l < M < Th_h \\ 1 \sim H_1,\ Th_h < M \text{ or } M < Th_l \end{cases} \tag{11}$$

where M is the Ratio or the improved Ratio, H_0 is the hypothesis that no spoofing signal detected, H_1 is the hypothesis that there is spoofing signal. Considering that the correlation function obeys a gaussian distribution, the Ratio or the Improved Ratio also obeys a gaussian distribution, which is presented as follows:

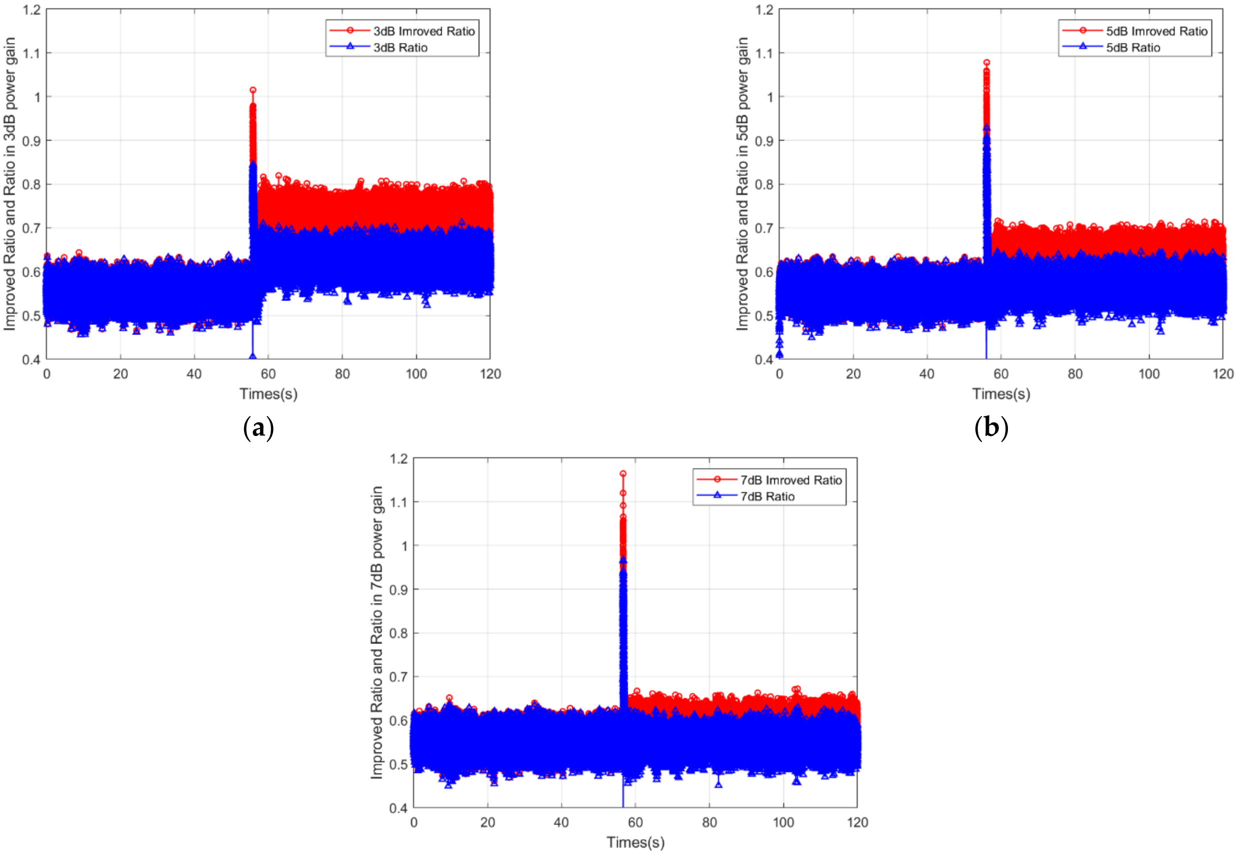
$$p(M) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{(\frac{-(M-\mu)^2}{2\sigma^2})} \tag{12}$$

where $p(M)$ is the distribution function, μ is the expectation of M, σ^2 is the variance of M. Thus, the false positive rate and the detection rate can be asserted as follows:

$$P_f = \int_{-\infty}^{Th_l} p(M; H_0) dM + \int_{Th_h}^{+\infty} p(M; H_0) dM \tag{13}$$

$$P_d = \int_{Th_l}^{Th_h} p(M; H_1) dM \tag{14}$$

where P_f is the false positive rate and P_d is the detection rate.



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

Figure 10. The Improved Ratio and Ratio with Different Spoofing Power Gain: (**a**) The comparison of Improved Ratio and Ratio in 3 dB power gain; (**b**) The comparison of Improved Ratio and Ratio in 5 dB power gain; (**c**) The comparison of Improved Ratio and Ratio in 7 dB power gain.

Figure 11 is the receiver operator characteristic curve (ROC) that compares the performance of the SQM detection with the Ratio metric and the Combined Method of improved Raito and $C/N_0 - MV$ under different spoofing power gain. Greater detection performance is indicated by how close the line is to the point (0,1). It is evident that the Combined Method surpasses the Ratio no matter what power gain is added. The Combined Method reaches the detection rate at 99%, 98% and 62% separately when the false positive rate is 10%.

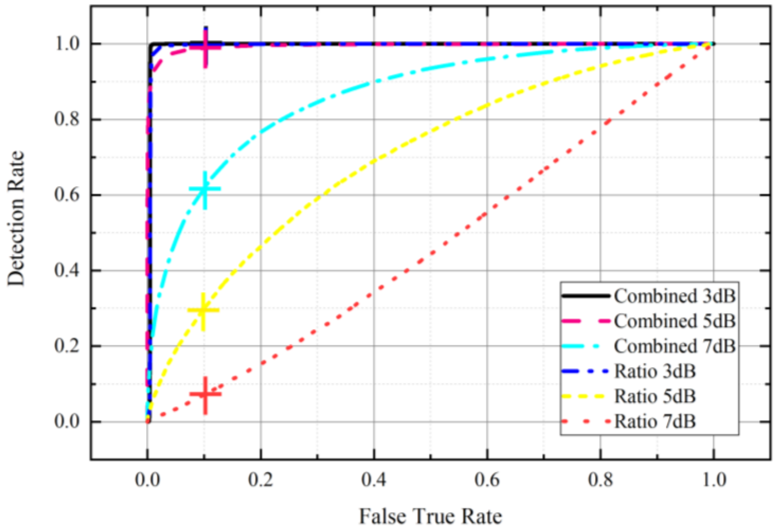


Figure 11. The ROC of Ratio and the Combined Method of Improved Ratio and $C/N_0 - MV$.

As shown in Figure 11, the Combined Method reaches 99.99%, 98.80% and 61.79% in detection rate, whereas the Ratio reaches 99.89%, 29.97% and 7.23% when the false positive rate is set at 10%.

Constant False Alarm Rate (CFAR) is selected in this work, with the false positive rate set at 10%.

As shown in Figure 12, with the time variation, the results also verify that the combined method is better than the Ratio method. The Combined means the Combined method of Improved Ratio and $C/N_0 - MV$.

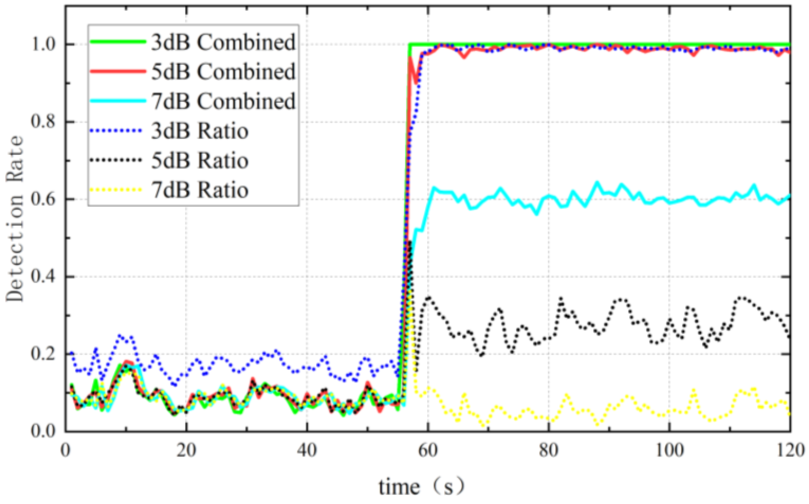


Figure 12. The performance of Ratio method and Combined method with the time variation.

The Combined Method reached almost 100% in detection rate under 3 dB power gain after the presence of a spoofing signal, whereas the Ratio, also nearly 100%, has about 20% of false detection when no spoofing signal is added. When spoofed by signal with 5 dB power gain, the Combined towers over the Ratio a lot, by approximately 80%. Finally, the Combined remains about 60% of the detection rate when the Ratio almost fails to detect any spoofing signal.

5. Conclusions

Meaconing detection method based on the Improved Ratio combined with $C/N_0 - MV$ is evaluated theoretically and experimentally. We first describe the structure of the meaconing spoofing system and the operation flow of the detection software in detail with the device model specifications provided. Furthermore, the theoretical analysis is provided alongside the derivation of the indicators used in the method. Finally, experiments are conducted in order to test the mentioned methods and verify the effectiveness of the proposed method. The findings can be concluded as follows:

- The $C/N_0 - MV$ has better performance than the C/N_0 in triggering the successive spoofing detection.
- The Combined Method of Improved Ratio and $C/N_0 - MV$ outperforms the Ratio a lot under the same spoofing power. For instance, the Combined one reaches 98% under 5 dB power gain, whereas the Ratio reaches only about 30%.

Besides, the study of interference detection in this paper is only for meaconing spoofing, and the effective classification method of different interference needs to be studied in the future. The final purpose of detecting spoofing is to address the impact of spoofing, and there is a lack of spoofing suppression algorithm at present. Therefore, developing an algorithm that can accurately identify and effectively suppress spoofing will be of great significance to maintain the normal operation of satellite navigation systems.

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

Funding: This research was funded by National Key Research and Development Plan of China (2018YFB0505103) and National Natural Science Foundation of China (61873064).

Data Availability Statement: Relevant data are available on request from the corresponding author. Please contact to Xuefen Zhu (zhuxuefen@seu.edu.cn).

Acknowledgments: We would like to appreciate for kind technical guidance from Xinhua Tang at the School of Instrument Science and Engineering, Southeast University, China.

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

References

1. Liu, P.; Chen, S.; Ren, C.; Liu, S. Research and Analysis of Anti-Spoofing Technology for Satellite Navigation. *Navig. Position. Timing* **2020**, *7*, 123–130.
2. Psiaki, M.L.; Humphreys, T.E. GNSS spoofing and detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
3. Rawnsley, A. Iran's Alleged Drone Hack: Tough, but Possible. Available online: http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps (accessed on 15 September 2020).
4. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned aircraft capture and control via GPS spoofing. *J. Field Robot.* **2014**, *31*, 617–636. [CrossRef]
5. Fu, N.; Fan, J.; Yang, F.; Xu, D. Study of anti–Jamming technology of GNSS timing receiver in electric power system. *Radio Eng.* **2020**, *50*, 81–84.
6. Mosavi, M.R.; Baziar, A.R.; Moazedi, M. De-noising and spoofing extraction from position solution using wavelet transform on stationary single-frequency GPS receiver in immediate detection condition. *J. Appl. Res. Technol.* **2017**, *15*, 402–411. [CrossRef]
7. Chen, J.; Chen, S.; Liu, P. Analysis of GNSS repeater deception jamming signal effect on the receiver. In Proceedings of the 9th China Satellite Navigation Academic Annual Conference-S03 Satellite Navigation Signal and Anti-jamming Technology, Harbin, China, 23 May 2018; pp. 74–78.
8. Takujiebinuma. Software-Defined GPS Signal Simulator. Available online: https://github.com/osqzss/gps-sdr-sim (accessed on 17 September 2020).
9. Shi, P.L.; Wang, X.Y.; Xue, R. Research on power control strategy of GNSS repeater deception jamming. *Mod. Navig.* **2021**, *4*, 79–89.
10. Shi, P.; Jin, W.; Wu, S. Research on satellite selection algorithm of GNSS repeater deception jamming. *Trans. Beijing Inst. Technol.* **2019**, *39*, 524–531.
11. Chen, J.; Chen, S.; Wu, H.; He, R. Cross correlation noise model of multiple GNSS spoofing signals. *Appl. Res. Comput.* **2019**, *36*, 2488–2491.
12. Zhang, Q. Research on Anti-deception Jamming Technology of GNSS Navigation Signal Based on Residual Signal Detection. Master's Thesis, University of Electronic Science and Technology of China, Chengdu, China, 2020.

13. Broumandan, A.; Jafarnia-Jahromi, A.; Lachapelle, G.; Ioannides, R.T. An approach to discriminate GNSS spoofing from multipath fading. In Proceedings of the 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, The Netherlands, 14–16 December 2016; pp. 1–10.
14. Gong, J. Single antenna GNSS spoofing detection based on moving variance of SQM. Master's Thesis, Civil Aviation University of China, Tianjin, China, 2020.
15. He, H. Research on Anti-spoofing for Satellite Navigation Based on Array. Master's Thesis, Harbin Engineering University, Harbin, China, 2019.
16. Daneshmand, S.; Jafarnia-Jahromi, A.; Broumandan, A.; Lachapelle, G. A GNSS structural interference mitigation technique using antenna array processing. In Proceedings of the 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), A Coruna, Spain, 22–25 June 2014; pp. 109–112.
17. Wu, Z.; Wu, W.; Liu, K.; Tang, K. Research on Algorithm of Gradually Induced Spoofing Detection Based on Tightly Coupled INS/GNSS Integration. *Navig. Position. Timing* **2019**, *6*, 7–13.
18. Liu, Y.; Li, S.; Fu, Q.; Zhou, Q. Chip-scale atomic clock aided INS/GNSS integrated navigation system spoofing detection method. *J. Chin. Inert. Technol.* **2019**, *27*, 654–660.
19. Guo, J.; Sun, J.; Li, D. Analysis and design of a new GNSS encryption authentication scheme. *Telecom World* **2020**, *27*, 125–126.
20. Zhao, W.; Tang, B.; Peng, A.; Meng, F. Global navigation satellite system spoofing detection based on time variant pattern of multipath signal power. *J. Xiamen Univ.* **2020**, *59*, 972–978.
21. Shen, C.; Guo, C. Simulation of Spoofing Signal Detection in GNSS. *Comput. Simul.* **2019**, *36*, 109–113+119.
22. 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]
23. Manfredini, E.G.; Dovis, F.; Motella, B. Validation of a signal quality monitoring technique over a set of spoofed scenarios. In Proceedings of the 2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, The Netherlands, 3–5 December 2014; pp. 1–7.