

# Simulation and Analysis for Error from Satellite Tracking Segment Anti-spoofing

Liu You-ming<sup>1</sup>, Feng Qi<sup>1</sup> and Li Ting-jun<sup>1</sup>

<sup>1</sup>*Department of Electronic and Information Engineering, Naval Aeronautical University, Yantai 264001, China  
E-mail: 15615659977@163.com*

## Abstract

*It is the first and most important step in the detection of satellite navigation deception attack. For the detection of the regenerative deception attack, a method based on carrier phase tracking spectrum analysis is proposed. The simulation experiment results show that this method can be used in the case that the false alarm probability is no more than 0.5%, and the detection probability is almost 100%. The method is not necessary for the transformation of the hardware, the signal processing module in the software receiver can be added to the corresponding processing module, and the detection of the deception attack can be realized.*

**Keywords:** *Satellite; Anti deception; Phase; Deception; Satellite tracking*

## 1. Introduction

Satellite navigation system determines the location of the user by using the principle of arrival time, the satellite to the receiver of the propagation delay times the speed of light that can be the two. The navigation satellite orbit has a fixed law, so the change of the time delay of the satellite signal propagation is determined by [1]. By ionospheric refraction and other factors, the satellite signal propagation delay can not be accurately measured, the factors that cause the error can be considered as a zero mean Gauss type noise, the noise will not change the time delay of the receiver to receive satellite signal. When the target receiver is to be a target, the delay variation characteristics of the target receiver are not easy to be consistent with the variation of satellite time delay. The change of time delay in the receiver loop performance of the code phase before and after the move, by tracking the code phase change in the tracking code, can be used to detect [2].

Under the condition of smooth and normal receiving satellite signal, the amplitude of the complex correlation peak of the receiver is more stable. Spoofing of source to receiver target attack, by way of increasing the transmit power control loop tracking points, the deceptive signals in the receiver's tracking loop complex correlation peak amplitude is higher than the real signal complex correlation peak amplitude, in the process, correlation peak amplitude changes will receive satellite signals in normal and by monitoring receiver multiple correlation peak change situation, which can detect anomalies caused by spoofing attacks.

## 2. Anti Deception Technology based on Code Phase Shift Speed

### 2.1. Scene Analysis

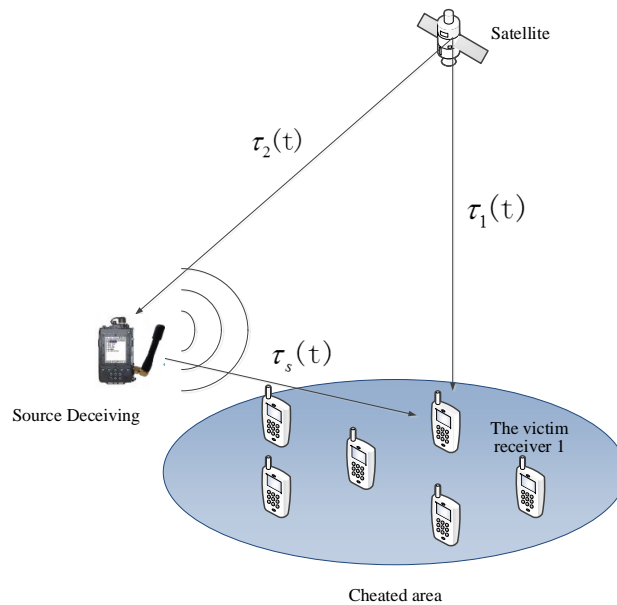
The mathematical model of the pseudo range of the received satellite down-link signal is as follows:

$$\begin{cases} \rho_1(t) = \sqrt{(x_1(t) - x_0)^2 + (y_1(t) - y_0)^2 + (z_1(t) - z_0)^2} + c \cdot (T_s + T_u) \\ \rho_2(t) = \sqrt{(x_2(t) - x_0)^2 + (y_2(t) - y_0)^2 + (z_2(t) - z_0)^2} + c \cdot (T_s + T_u) \\ \rho_3(t) = \sqrt{(x_3(t) - x_0)^2 + (y_3(t) - y_0)^2 + (z_3(t) - z_0)^2} + c \cdot (T_s + T_u) \\ \rho_4(t) = \sqrt{(x_4(t) - x_0)^2 + (y_4(t) - y_0)^2 + (z_4(t) - z_0)^2} + c \cdot (T_s + T_u) \end{cases}$$

Assuming that With a regenerative repeater deception source, it can change the forwarding delay after the control tracking loop, then the pseudo range model of the receiver to receive the deception signal is as follows:

$$\begin{cases} \rho_1(t) = \sqrt{(x_1(t) - x_0)^2 + (y_1(t) - y_0)^2 + (z_1(t) - z_0)^2} + c \cdot (T_s + T_u + T_{s1}(t)) \\ \rho_2(t) = \sqrt{(x_2(t) - x_0)^2 + (y_2(t) - y_0)^2 + (z_2(t) - z_0)^2} + c \cdot (T_s + T_u + T_{s2}(t)) \\ \rho_3(t) = \sqrt{(x_3(t) - x_0)^2 + (y_3(t) - y_0)^2 + (z_3(t) - z_0)^2} + c \cdot (T_s + T_u + T_{s3}(t)) \\ \rho_4(t) = \sqrt{(x_4(t) - x_0)^2 + (y_4(t) - y_0)^2 + (z_4(t) - z_0)^2} + c \cdot (T_s + T_u + T_{s4}(t)) \end{cases}$$

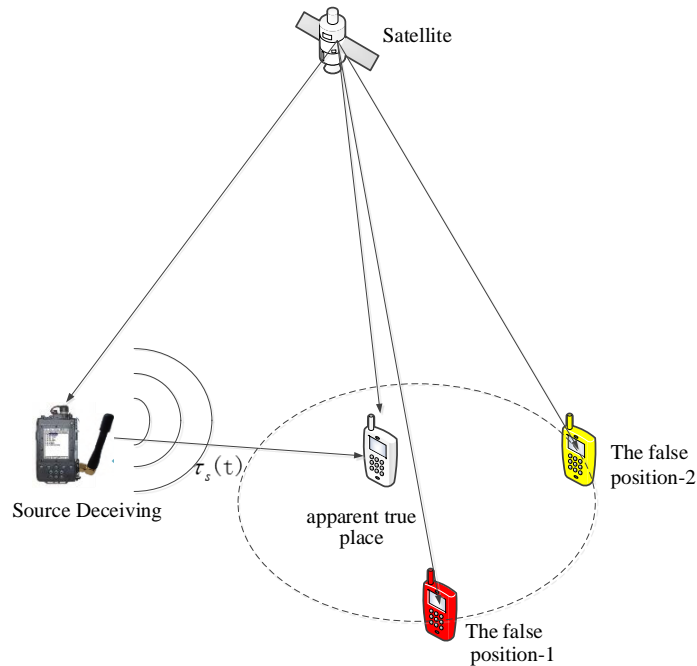
In Which  $\rho_i(t)$  is the i false satellite distance,  $(x_0, y_0, z_0)$  is the ECEF coordinates of the I satellite,  $(x_i(t), y_i(t), z_i(t))$  the coordinates of the receiver, the ECEF coordinates of the I satellite, the C is the speed of light,  $T_s$  is the satellite clock error  $T_u$  is the receiver clock error  $T_{si}(t)$ .



**Figure 1. Deception Detection**

Above is for the regeneration of forwarding deception and regenerative repeater deception which has two kinds of change of the satellite and the receiver receiving distance, a tampered ephemeris, another is to change the delay information, the scene for the latter. To receive a satellite signal from the source, the signal is sent to the cheat area by controlling the time delay. Victim receivers to receive satellite signals through the delay  $\tau_1(t)$  and deceive the source receives satellite signals experience a delay for  $\tau_2(t)$ , spoofing of source transmitted signal delay  $\tau_s(t)$ , which is received by the receiver to

deceive signal delay is  $\tau_2(t) + \tau_s(t)$ , spoofing of source can be through the change to arbitrary control receiver of the target area by the satellite receiver distance value  $\tau_s(t)$ , so as to change the target area receiver PVT results. Below is a simple schematic:



**Figure 2. Deception**

The I satellite receiver pseudo-range  $\rho_i(t)$ , with an interval of 1s measurements, which can be the sequence  $\{\rho_i(n)\}$ ,  $n=1, 2, \dots, N$ , the present moment and the next moment of the pseudo range from the single differential:

$$\Delta\rho_i(n) = \rho_i(n+1) - \rho_i(n)$$

STK simulation software navigation satellite orbit, take on earth a point coordinates for the location of the target receiver, 1s interval recording satellite I to receiver distance measurement value, the sequence  $\{\rho_i(n)\}$ ; take the other as the position of the source deceiving, the same to 1s interval recording satellite to deceive the source distance measurement value, the sequence  $\{\rho_s(n)\}$ ; spoofing of source control loops of the receiver at a certain speed change delay on the receiver of the eccentric tension, the sequence  $\{\Delta\rho(n)\}$  above  $n = 1, 2, 3, \dots, N$ ;

A satellite navigation system contains three types of satellites, such as GEO, MEO, and IGSO. The three kinds of satellites are used to build up the deception scene, and the influence of the behavior of the STK, and in the distance measurement is observed.

Static scene: GEO Satellite

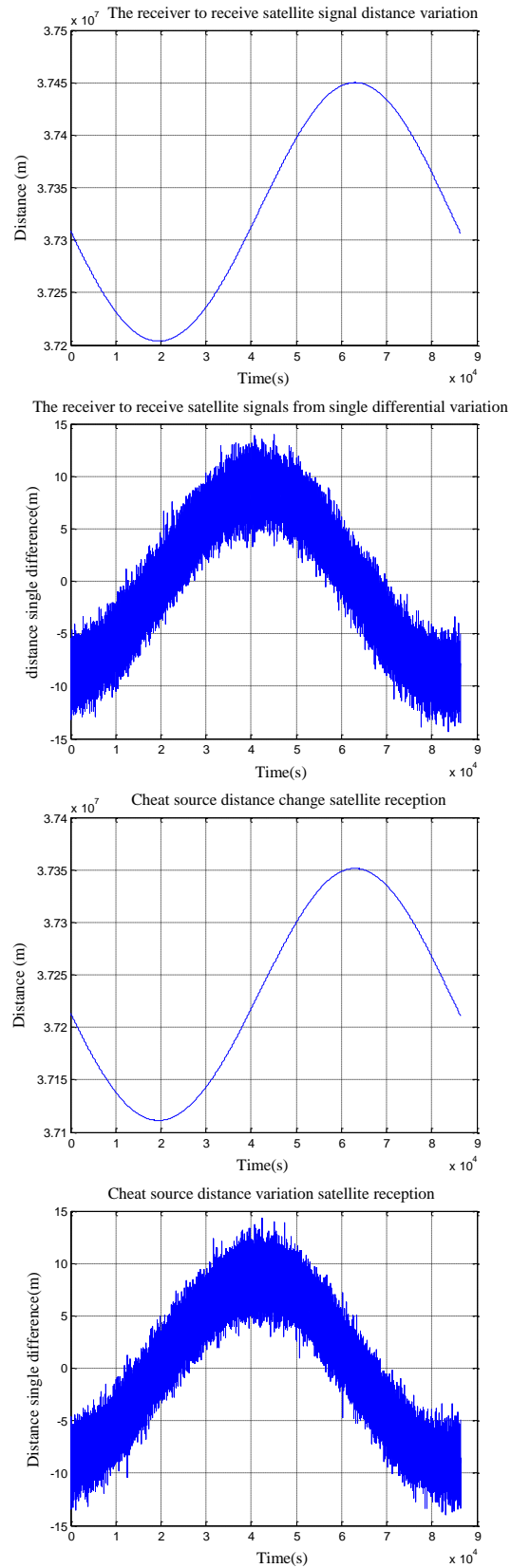
Satellite: compass GEO, longitude: 140 degrees angle: 1.8 degrees, E, eccentricity: 0.0003, cycle: 86166s.

City: Nanjing, latitude: latitude 32.0484 degrees, 118.769 degrees east longitude: longitude, height: 200m

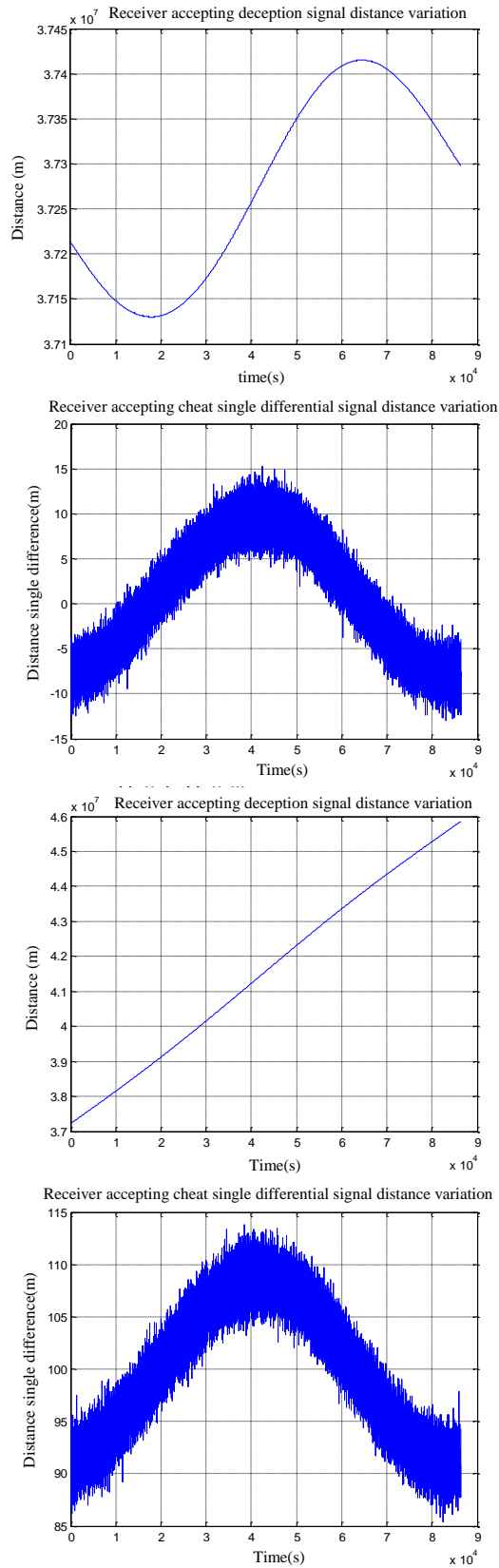
Deceive the source: latitude: latitude 31 degrees, 119.5 degrees east longitude: longitude, height: 5000m

The distance between the source and the receiver is 135.538 km, and the source is used to pull the target at a constant speed, and the speed is 1m/s, 100m/s

Data sampling: sampling a day's ranging value, that is, the 86400 sampling points, the sampling frequency is 1/s



(1) The source of the 1m/s is carried out at a uniform speed.



(2) The source of the 100m/s is carried out at a uniform speed.

**Figure 3. Receiver and Deception Source to Receive Satellite Signal Ranging**

MEO satellite

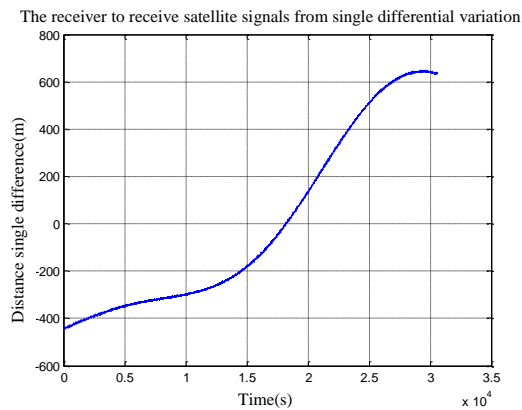
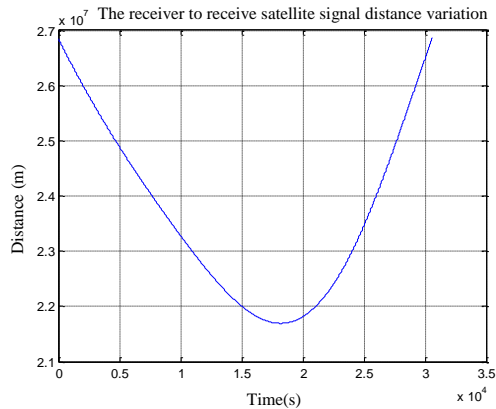
Beidou Satellite: MEO, cycle: 46392s, angle: 55 degrees E, eccentricity: 0.0025.

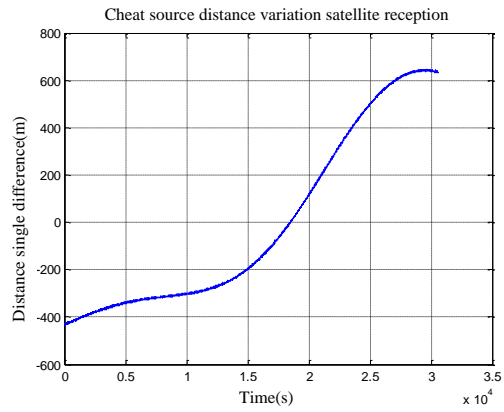
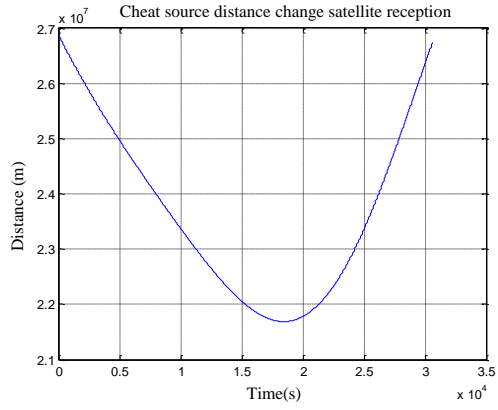
City: Nanjing, latitude: latitude 32.0484 degrees, 118.769 degrees east longitude: longitude, height: 200m

Deceive the source: latitude: latitude 31 degrees, 119.5 degrees east longitude: longitude, height: 5000m

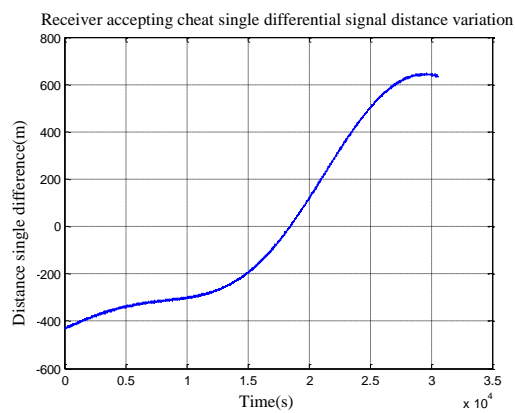
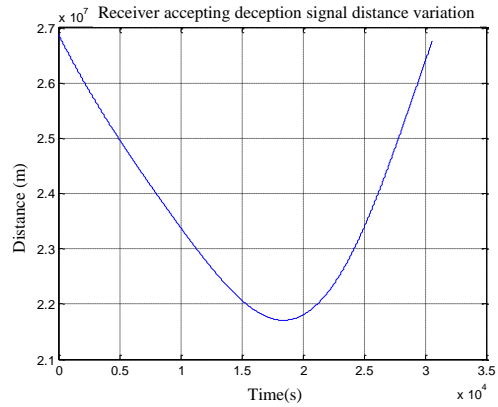
The distance between the source and the receiver is 135.538 km, and the source is used to pull the target at a constant speed, and the speed is 1m/s, 100m/s

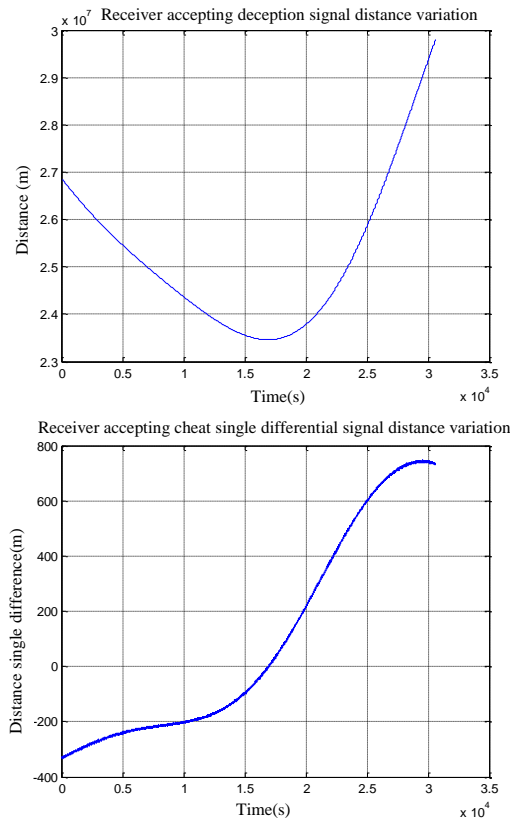
Data sampling: sampling of a transit arc section of the value, the passage of time and the receiver of the deception of the satellite, the sampling frequency of 1 points /s





(1) The source of the deception is 1m/s uniform.





(2) Deceive to 100m / s uniform pull side

**Figure 4. Receivers and Receiving Satellite Signals Ranging Deceive Source Value**

IGSO satellite

Beidou Satellite: IGSO, cycle: 86150s, angle: 55.09 degrees E, eccentricity: 0.00265.

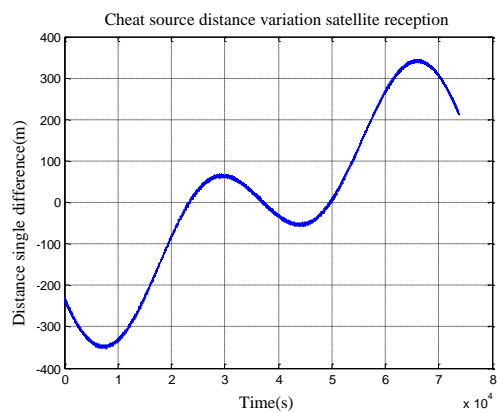
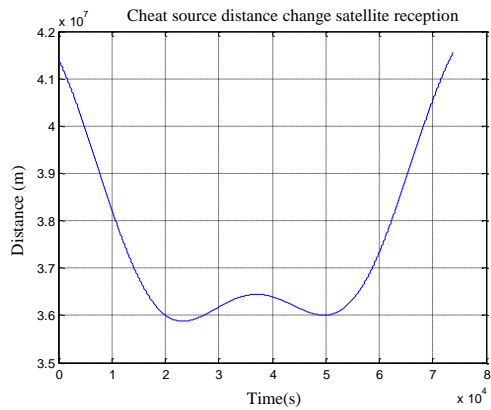
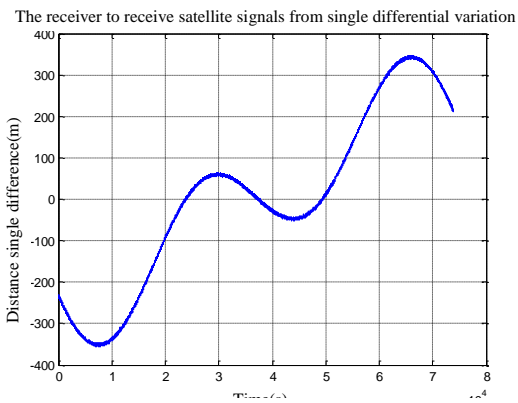
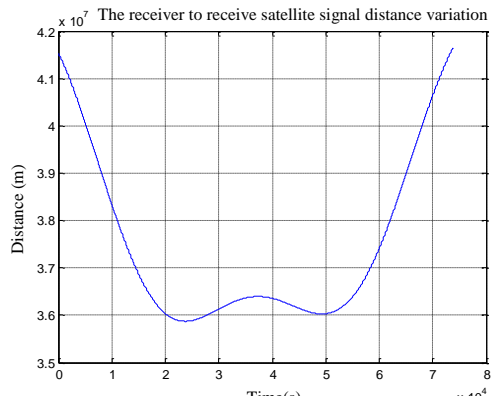
Receiver: latitude: latitude 32.0484 degrees, 118.769 degrees east longitude: longitude, height: 200m

Deceive the source: latitude: latitude 31 degrees, 119.5 degrees east longitude: longitude, height: 5000m

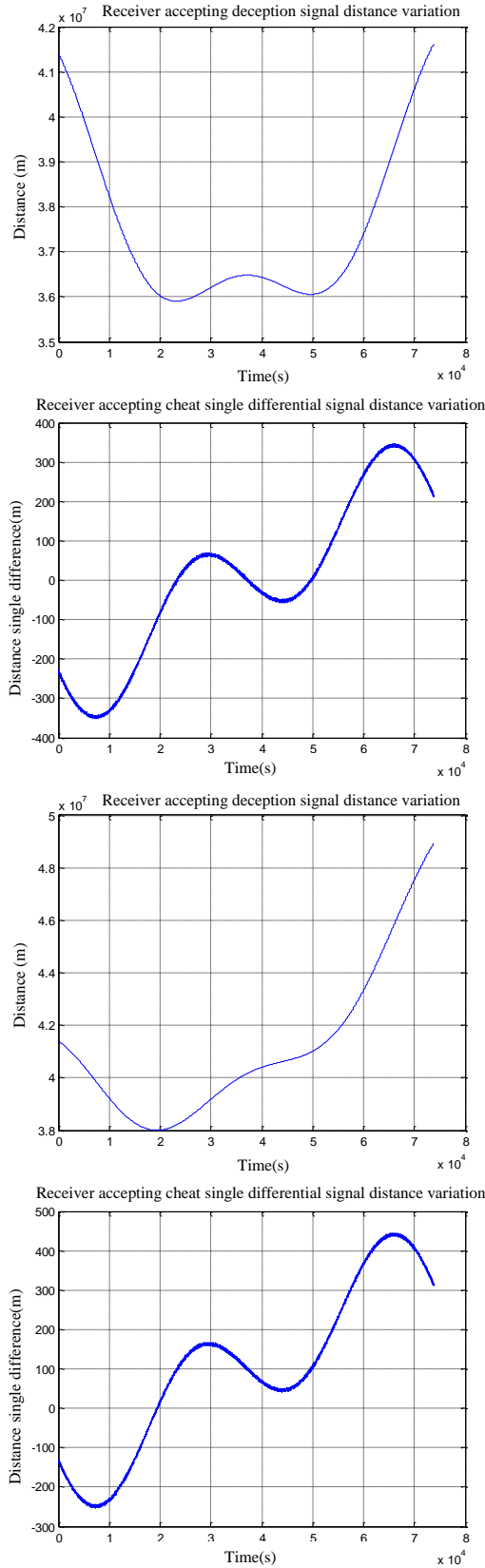
The distance between the source and the receiver is 135.538 km, and the source is used to pull the target at a constant speed, and the speed is 1m/s, 100m/s

Data sampling: sampling of a transit arc section of the value, the passage of time and the receiver of the deception of the satellite, the sampling frequency of 1 points /s





(1) The speed is 1m/s uniform.



(2) At a uniform speed of 100m/s

**Figure 5. Receiver and Deception Source to Receive Satellite Signal Ranging**

Seen from the simulation diagram, the spoofing of source to receiver pull partial behavior in the pseudo distance has a larger change, spoofing of source pull side with greater speed. The receiver receives the signal deceiving the distance compared to receiving, the real signal is high, and the receiving distance single difference from the perspective of graphic smaller, it is only longitudinal axis of translation in the real signal from the single difference based, this shows that spoofing signal can be pulled through partial to change the relative velocity of the satellite receiver. Using this principle, the method of sequence dependent method is used to detect the deception.

## 2.2. Anti Deception Technology based on Code Phase Shift Rule

According to type,  $\{\rho_i(n)\}$  single poor characterization of the receiver is to receive satellite signal loop code phase variation and  $\{\rho_s(n) + \Delta\rho(n)\}$  single differential characterization of the spoofing signal of the receiver code loop phase variation, the sequence  $\{\rho_i(n)\}$  single difference and sequence  $\{\rho_s(n) + \Delta\rho(n)\}$  difference is performed by computing the correlation, set the relevant threshold value, if the correlation calculation value is less than the threshold, the correlation of two sequences difference, namely the detection signal can be convicted of spoofing signal. If the value of correlation operation is greater than the threshold, the correlation of two sequences good, signal detection can be sentenced to the true signal.

## 3. Anti Deception Technology based on Correlation Peak of Tracking Loop

### 3.1. Scene Analysis

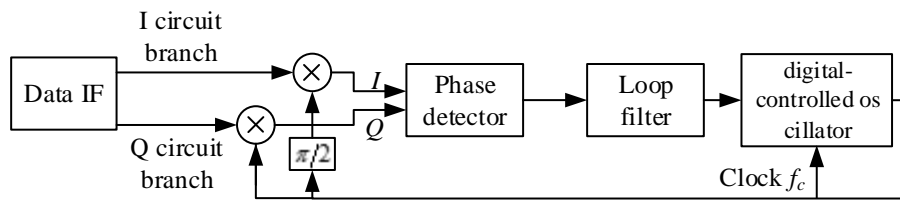
If the receiver receives only 1 satellite signals, the received signal is:

$$S_r = S_s + S_A + N_T$$

Among them,  $S_r$  is the received signal,  $S_s$  for the deception signal,  $S_A$  for the real signal,  $N_T$  for the noise. The power ratio of deception signal and real signal is expressed by  $J/S$ .

In the actual situation, because of the different position of the receiver and the influence of terrain features, the amplitude of the received satellite navigation signal received by the receiver is larger than that of 10dB. Therefore, only from the received signal power it can not be detected by deception. In addition, because of the existence of the dynamic, the received signal has a large Doppler frequency shift (frequency difference). Therefore, it is unable to determine whether the signal is the signal of the lock or it is the real signal after the Doppler frequency shift.

Tracking of satellite navigation signal includes two aspects of code tracking and carrier tracking. Because of the difference between the signal and the real signal in a code chip, it can not be detected effectively in the code tracking phase. The main purpose of carrier tracking is to maintain the measurement and tracking of the carrier Doppler shift. Costas Loop Phase (Lock) is usually used in the carrier tracking loop due to the presence of data modulation in the base-band signal. Figure 6 shows a typical block diagram of a carrier tracking loop based on the PLL Costas loop. Table [11] summarizes 1 Costas PLL discriminator and its common characteristics. Regardless of which a discriminator algorithm is used, in the loop is locked, the loop phase error mainly includes thermal noise caused by phase jitter and dynamic stress error. In the interference environment, it also includes the error caused by interference.



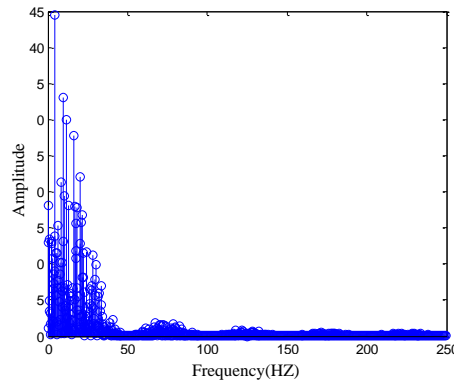
**Figure 6. Block Diagram of a Typical Satellite Navigation Signal Carrier Tracking Loop**

**Table 1. Commonly used Costas Loop Discriminator**

Discriminator algorithm	Output phase difference	Characteristic
$Q \times I$	$\sin 2\phi$	Costas classic analog discriminator. Near the best in low snr. The slope is proportional to the square of the signal amplitude, and the calculation amount is required to be moderate.
$Q \times \text{Sign}(I)$	$\sin \phi$	Decision oriented Costas. In the high SNR, close to the best. The slope is proportional to the amplitude of the signal. Low computational requirements.
$Q / I$	$\tan \phi$	The second best, but in high and low SNR when good. The slope is independent of the signal amplitude. High computational requirements. At the point where the error is divided by zero.
$ATAN(Q / I)$	$\phi$	Two quadrant arc-tangent. At high and low signal-to-noise ratio, the slope is independent of the signal amplitude. Computational requirements are high, usually with the look-up table method to achieve.

### 3.2. Deception Detection Technology based on Carrier Phase Tracking Spectrum Analysis

In the case of the PLL loop phase detector, the phase error caused by the phase error of the loop phase detector is only caused by the noise and the dynamic stress. In low dynamic environment, it is mainly caused by noise. The output signal power spectrum of the phase detector will be spread over the whole frequency range. When there are interference signals, the signal of the phase detector output is closely related to the input signal. Whether the deception signal or the real signal, because of its low symbol rate, the energy is mainly concentrated in the low frequency part. Figure 3 shows the spectrum of the navigation information as the random signal and the symbol rate of 50Hz signal. In the graph, the signal energy is mainly concentrated in the low frequency part of the symbol rate. Therefore, when the input signal contains the deception signal, the energy of the loop phase detector output signal will be mainly concentrated in the low frequency part. Because the signal of the deception is the same as the real signal, the signal can be detected by the spectral analysis of the PLL loop phase detector. This is the basic principle of the [3] based on the carrier phase tracking spectrum analysis.



**Figure 7. The Symbol Rate for the Random Signal of 50sps**

There are many methods and ways to analyze the spectrum of the output signal of the phase detector. The frequency domain analysis is the simplest and most basic method. The spectrum analysis of the output signal can get a lot of characteristic parameters, including the amplitude maximum, the output variance of the phase detector and so on. Because of the large variation range of the received signal, the signal noise ratio of the signal to noise ratio is close, so these parameters can not be used directly as a cheat detection. Since the energy of the deception jamming signal is mainly concentrated in the low frequency part, a characteristic variable can be defined as the formula (1):

$$\gamma = \frac{E[E_i]}{E[E_j]} \quad (1)$$

Among them,  $E[\cdot]$  the mean value,  $E_i, E_j$  the output of the phase detector output by the fast Fourier transform (Fast Fourier Transform FFT), the frequency components of the corresponding energy.  $i = 1, 2, \dots, N_1, j = N_1 + 1, \dots, N$  Where  $N$  is for the FFT arithmetic points are expressed  $R_s$  as the frequency points corresponding to the symbol rate of the navigation information,  $N_1 = NR_s / f_s$  the phase detection rate  $f_s$  is indicated. In the ideal case, the noise energy is distributed in the entire frequency band,  $\gamma$  should be equal to 1; the low frequency deception or interference signal  $\gamma$  is greater than 1. Therefore, by calculating  $\gamma$  the value to make a judgment whether there is a deceptive signal. Figure 8 gives a signal detection model based on carrier phase tracking spectrum analysis.  $\gamma_t$  The default decision threshold for a graph. By comparing  $\gamma$  with the threshold of default judgment, whether the input signal is included in the decision of the deception signal.



**Figure 8. A Deception Detection Model based on Carrier Phase Tracking Spectrum Analysis**

The performance of detection model is usually measured by detecting probability and false alarm probability  $P_d$   $P_{fa}$  .  $P_d$  The probability that the correct detection of the deception signal,  $P_{fa}$  in the case of the absence of deception, to identify the true signal as the probability of deception signal. If there is a time for the N experiment, there are  $n^+$  times to receive the signal,  $n^-$  the second no deception signal, obviously  $n = n^+ + n^-$  .  $P_d$  And  $P_{fa}$  were expressed as:

$$P_d = \lim_{n \rightarrow \infty} \frac{n_+^+}{n_+} \tag{2}$$

$$P_{fa} = \lim_{n \rightarrow \infty} \frac{n_-^+}{n_-} \tag{3}$$

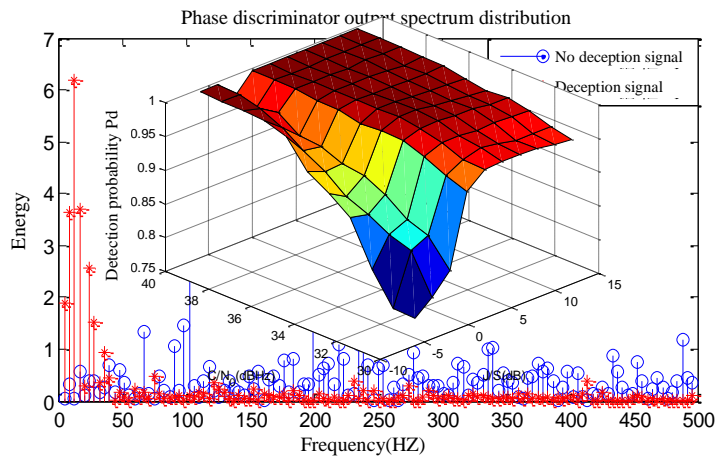
In the formula,  $n_+^+$  and  $n_-^+$  respectively represents the correct identification of the deception signal and the true signal to identify the number of the signal of deceiving.

In order to verify the validity of the proposed method, we use Matlab software to carry out simulation experiments, the simulation parameters are shown in Table 2. If the real signal is not dynamic, the carrier frequency of the signal is changed according to the law of sine wave, the maximum amplitude of the signal is 3Hz, and the change rate is 1Hz/s. The Costas loop discriminator discriminator for judgment. In the process of simulation, the signal is normalized by the maximum signal before entering phase detector.

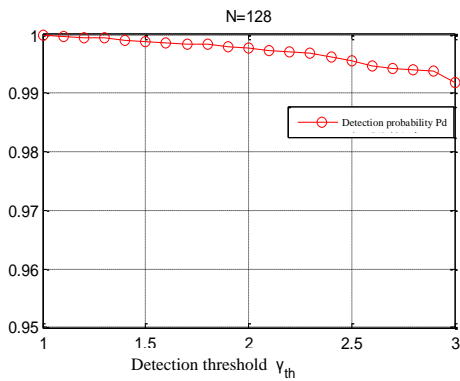
**Table 2. Simulation Parameters Table**

parameter	Real signal	Deceptive signal
Symbol rate (SPS)	50	50
Phase rate (Hz)	1000	1000
carrier-to-noise ratio $C/N_0$ (dBHz)	30~40	$J/S = -6 \sim 12$ dB
Preliminary testing integration time (ms)	1	1
simulation time (s)	10	10
Biggest deviation signal (Hz)	0	3
Frequency fluctuation rate (Hz/s)	0	1
loop bandwidth (Hz)	20	20
signal detection threshold $\gamma_t = 2$	2	2

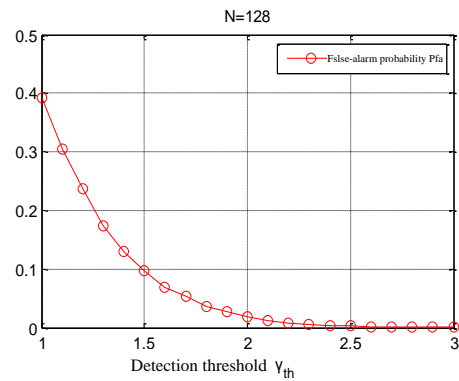
By Using the Matlab software, as shown in Table 2 under the parameters of 5000 times the monte carlo simulation was carried out. Figure 9 shows the real signal, no deception signals and the output signal of the phase discriminator spectrum diagram. By figure you can clearly see, joining after deception signals appeared a lot of energy in low frequency high frequency component.



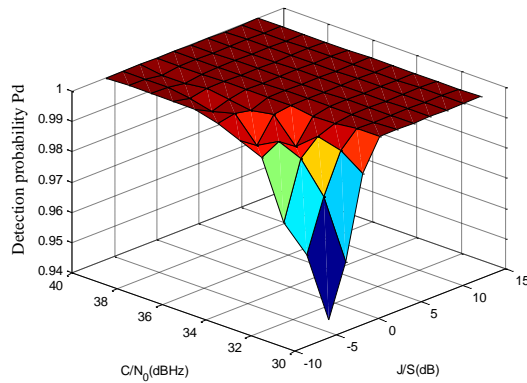
**Figure 9. Cases, Deceive Signal Phase Discriminator Output Spectrum**



Detection threshold and the relationship between the detection probability

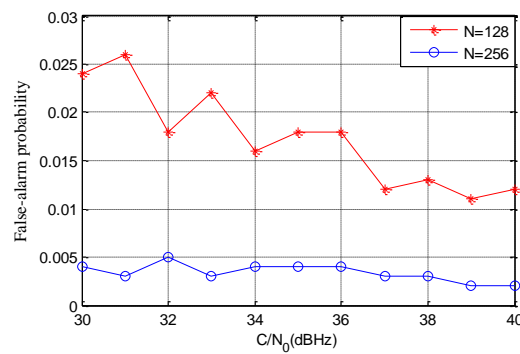


The relationship between detection threshold and false-alarm probability



N=128 Point detection probability

N=256 Point detection probability



**Figure 10. Carrier to Noise Ratio and the Relationship between False-alarm Probability**

The relationship between detection threshold and detection probability and false alarm probability is given in Figure 8, 7 and 9, 10. The detection results of N=128 and 256 FFT are given respectively. The following conclusions can be drawn from Figure 7-10:

(1) The detection threshold  $\gamma_t$  is higher, the smaller the false-alarm probability and detection probability which is lower. Adjust the detection threshold  $\gamma_t$ , then the expectation of detection probability and false alarm probability. In practical application, which should according to the specific requirements, setting up reasonable detection threshold;

(2) in the case of the detection threshold  $\gamma_t = 2$ , in addition to the part of the signal-to-noise ratio is very low, it is easy to under 2%, under the false alarm probability of more than 95% of detection probability; The 256 point FFT transform, the false alarm probability is not more than 0.5% of cases, which almost can obtain the detection probability of 100%;

(3) In deception signals under the condition of smaller ( $J/S \leq 0$ ), the loop lock on real signal, the detection probability with deception signals and real signal-to-noise ratio increases, and the false alarm probability decreases with the increase of signal-to-noise ratio. Therefore, under the condition of high SNR the method detecting effect is better;

(4) In the case of jamming signal is larger ( $J/S \geq 2$ ), the loop lock on deception signal, detection probability and deceive signal power. In fact, at this point the loop real signal is treated as interference. Therefore, the real signal power, the greater the detection probability is higher;

(5) The more sampling points FFT, the higher the frequency resolution, the higher detection probability and false alarm probability is lower. Under the same decision threshold, the FFT points increased from 128 points to 256 points, the false alarm probability was reduced to 1/5 of the original. However, the more points of FFT computing, whatever computational complexity is, it is greater to make a trade-off according to the actual situation.

#### 4. Conclusion

Due to reaching the ground receiver satellite distance changes associated with satellite orbit, so as to cheat the source to the receiver slanting distance change law, which do not tally with the satellite, putting forward the target loop code phase change law of resistance to cheat. Change of the stars for a specific satellite ground set up corresponding protection threshold, achieving the target of anti cheat.



## References

- [1] S. Zhou, L. Mi, H. Chen and Y. Geng, "Building detection in Digital surface model", 2013 IEEE International Conference on Imaging Systems and Techniques (IST), (2012) Oct.
- [2] J. He, Y. Geng and K. Pahlavan, "Toward Accurate Human Tracking: Modeling Time-of-Arrival for Wireless Wearable Sensors in Multipath Environment", IEEE Sensor Journal, vol. 14, no. 11, (2014) Nov., pp. 3996-4006.
- [3] Lv Z., Halawani A and Fen S., "Touch-less Interactive Augmented Reality Game on Vision Based Wearable Device[J]", Personal and Ubiquitous Computing, vol. 19, no. 3, (2015), pp. 551-567.
- [4] G. Bao, L. Mi, Y. Geng, M. Zhou and K. Pahlavan, "A video-based speed estimation technique for localizing the wireless capsule endoscope inside gastrointestinal tract", 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), (2014) Aug.
- [5] D. Zeng and Y. Geng, "Content distribution mechanism in mobile P2P network", Journal of Networks, vol. 9, no. 5, (2014) Jan., pp. 1229-1236.
- [6] Gu W., Lv Z. and Hao M., "Change detection method for remote sensing images based on an improved Markov random field[J]", Multimedia Tools and Applications, (2015), pp. 1-16.
- [7] Chen Z., Huang W. and Lv Z., "Towards a face recognition method based on uncorrelated discriminant sparse preserving projection[J]", Multimedia Tools and Applications, (2015), pp. 1-15.
- [8] J. Hu and Z. Gao, "Distinction immune genes of hepatitis-induced hepatocellular carcinoma[J]", Bioinformatics, vol. 28, no. 24, (2012), pp. 3191-3194.
- [9] Lv Z., Halawani A. and Feng S., "Multimodal hand and foot gesture interaction for handheld devices[J]", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 11, no. 1s, (2014), pp. 10.
- [10] G. Liu, Y. Geng and K. Pahlavan, "Effects of calibration RFID tags on performance of inertial navigation in indoor environment", 2015 International Conference on Computing, Networking and Communications (ICNC), (2015) Feb.
- [11] J. He, Y. Geng, Y. Wan, S. Li and K. Pahlavan, "A cyber physical test-bed for virtualization of RF access environment for body sensor network", IEEE Sensor Journal, vol. 13, no. 10, (2013) Oct., pp. 3826-3836.
- [12] W. Huang and Y. Geng, "Identification Method of Attack Path Based on Immune Intrusion Detection", Journal of Networks, vol. 9, no. 4, (2014) Jan., pp. 964-971.
- [13] Li X., Lv Z. and Hu J., "XEARTH: A 3D GIS Platform for managing massive city information[C]", Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2015 IEEE International Conference on. IEEE, (2015), pp. 1-6.
- [14] J. He, Y. Geng, F. Liu and C. Xu, "CC-KF: Enhanced TOA Performance in Multipath and NLOS Indoor Extreme Environment", IEEE Sensor Journal, vol. 14, no. 11, (2014) Nov., pp. 3766-3774.
- [15] N. Lu, C. Lu, Z. Yang and Y. Geng, "Modeling Framework for Mining Lifecycle Management", Journal of Networks, vol. 9, no. 3, (2014) Jan., pp. 719-725.
- [16] Y. Geng and K. Pahlavan, "On the accuracy of rf and image processing based hybrid localization for wireless capsule endoscopy", IEEE Wireless Communications and Networking Conference (WCNC), (2015) Mar.
- [17] Li X., Lv Z. and Hu J., "Traffic management and forecasting system based on 3d gis[J]", Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on, (2015), pp. 991-998.
- [18] Zhang S. and Jing H., "Fast log-Gabor-based nonlocal means image denoising methods[C]", Image Processing (ICIP), 2014 IEEE International Conference on. IEEE, (2014), pp. 2724-2728.

## Authors



**Liu You-ming**, He enrolled in Naval Aeronautical University, in communications and information engineering research, participated in a number of major national projects and Natural Science Foundation research projects, scientific research on communication has a great interest has published many articles in communication.

