# Chapter 65
# Analysis of the Anti-Spoofing Performance of Acquisition with Threshold Method

**Jian Wang, Hong Li, Xiaowei Cui and Mingquan Lu**

**Abstract** With the rapid development of navigation technologies, spoofing has become a significant threat to navigation system. As a key step in receiver signal processing, acquisition is an important barrier to anti-spoofing. Nowadays, researching on anti-spoofing performance of acquisition is in a blank stage, threshold method in acquisition is the most commonly used detection strategy. In this article, we add a single spoofing signal on GPS P code and through the construction of mathematical model, we define successful probability of anti-spoofing as the assessment standard, then we analyze the relationship between factors influencing acquisition threshold and the successful probability of anti-spoofing, finally we give the theoretical calculate method of upper bound of threshold method's anti-spoofing performance, which all have a guiding significance for the design of receiver.

**Keywords** Threshold · Acquisition · Amplification factor of spoofing signal · Successful probability of anti-spoofing

## 65.1 Introduction

With the rapid development of navigation technologies, safety of navigation signal has gradually become a topic of concern by the user, and research on spoofing and anti-spoofing of GPS signal has also become a hot spot.

Currently, there are some anti-spoofing methods existed, for example: an internal memorandum [1] from the MITRE recommended six techniques to counter spoofing and Wen proposed ten countermeasures for civil GPS signal

J. Wang (✉) · H. Li · X. Cui · M. Lu
Department of Electronic Engineering, Tsinghua University,
Beijing 100084, China
e-mail: tswangjian05@gmail.com

J. Sun et al. (eds.), *China Satellite Navigation Conference (CSNC) 2013 Proceedings*, Lecture Notes in Electrical Engineering 243,
DOI: 10.1007/978-3-642-37398-5_65, 

spoofing [2], both of which introduced kinds of methods comprehensively, but simply enough to put forward ideas, no further studies or results. Humphreys et al. [3] proposed two technique based on baseband processing technology; Cavaleri et al. [4] further elaborated how to achieve anti-spoofing on monitor phase-locked loop and delay locked loop, both of which focused on the technical aspects of baseband, mainly on the loop design. The Novariant Corporation detailed their research results on anti-spoofing platform with dual-antennas [5] and Daneshmand et al. [6] published their research results and the experimental data on GNSS12 meeting, both of which introduced multi-antenna technology to detect and eliminate spoofing. Huang et al. [7] presented a series of countermeasures and steps for spoofing in the point of signal designing and processing, which do some research on anti-spoofing methods and evaluation means. Generally speaking, the anti-spoofing technology is still in the groping stage. Though some countermeasures have been introduced, they have not been achieved yet. What is more, there is not effective assess tools to evaluate the merits of the anti-spoofing methods.

Acquisition determines whether the receiver can find the true signal, so it is an important barrier to anti-spoofing. However, researching on anti-spoofing performance of acquisition is in a blank stage. In this paper, we deal with GPS P-code, define successful probability of anti-spoofing as the assessment standard and analyze the anti-spoofing performance of acquisition with threshold method, then we give the theoretical calculate method of upper bound of threshold method's anti-spoofing performance, which all have a guiding significance for the design of receiver.

## 65.2 Assessment Standard of Anti-Spoofing

### *65.2.1 The Basic Principle of Acquisition with Threshold Method [8]*

Acquisition of GNSS signal is a two-dimensional search process. In each search grid, since the thermal noise is a Gaussian distribution, when the local signal is not aligned with the received true signal and spoofing signal, envelope $\sqrt{I^2 + Q^2}$ is formed, thus the noise is Rayleigh distribution and otherwise Rician distribution. The corresponding probability density function can be unified as formula 65.1:

$$p(z) = \begin{cases} \frac{z}{\sigma_n^2} \exp\left(-\frac{z^2+A^2}{2\sigma_n^2}\right) I_0\left(\frac{zA}{\sigma_n^2}\right), & z \geq 0 \\ 0, & z < 0 \end{cases} \tag{65.1}$$

Where $\sigma_n^2$ is RMS noise power, A is RMS signal amplitude and $I_0\left({}^{zA}/_{\sigma_n^2}\right)$ is zero order modified Bessel function. When it indicates noise, $A = 0$, and true signal, $A = A_s$, and spoofing signal, $A = A_j$.

In order to distinguish between signal and noise, we utilize NP criteria that calculate threshold after determining the probability of false alarm $p_{fa}$, showed as formula 65.2:

$$V_t = \sigma_n \sqrt{-2\ln p_{fa}} \tag{65.2}$$

Where $V_t$ is the threshold. When the envelop detected is lower than $V_t$, we regard it as noise and when higher, it is signal, therefore, detection probability of true signal and spoofing signal is as follows:

$$p_d^s = \int_{V_t}^{\infty} p_s(z)dz \tag{65.3}$$

$$p_d^j = \int_{V_t}^{\infty} p_j(z)dz \tag{65.4}$$

### 65.2.2 Successful Probability of Anti-Spoofing

The purpose of spoofing is to enable the receiver to lock spoofing signal. The first correlation value higher than threshold is the result when using threshold method. In this case, whether the receiver detect the true signal or it doesn't detect both the true and the spoofing, we can consider it as successful anti-spoofing, and define its probability as successful probability of anti-spoofing. Assume that detecting the true signal and spoofing signal be relatively independent, successful probability of anti-spoofing can be expressed as formula 65.5:

$$p_d = p_d^s + \left(1 - p_d^s\right)\left(1 - p_d^j\right) = \int_{V_t}^{\infty} p_s(z)dz + \int_{0}^{V_t} p_s(z)dz \int_{0}^{V_t} p_s(z)dz \tag{65.5}$$

Integrated formula 65.1, 65.2 and 65.5, we can get the calculate method of successful probability of anti-spoofing: First, we determine the threshold according to the probability of false alarm $p_{fa}$ and noise power $\sigma_n^2$, then the probability density function based on the input signal to noise ratio and coherent integration time, finally the successful probability of anti-spoofing through integration. Describe amplitude relation between true signal and spoofing signal as formula 65.6, we can make sure that the factors influencing ting successful probability of anti-spoofing $p_d$ are the input signal-to-noise ratio (SNR) without spoofing signal, spoofing signal amplification factor (k), probability of false alarm ($p_{fa}$) and coherent integration time ($c_h$).

$$A_j/A_s = k \tag{65.6}$$

## 65.3 Analysis of Factors that Influence Anti-Spoofing Performance

According to Sect. 65.2.2, there are many factors influencing successful probability of anti-spoofing, and the followings are the influence of each factor.

### *65.3.1 Input SNR and Spoofing Signal Amplification Factor k*

S/N and k are both factors which influence and noise power of signal received, and therefore influence the threshold and the probability density function. Figure 65.1 shows the influence to the success probability of anti-spoofing $p_d$, where the probability of false alarm $p_{fa} = 0.001$ and coherent integration time $c_h = 1$ ms.

Following points can be seen from Fig. 65.1: (1) When the input SNR is too low to detect the true signal, the successful probability of anti-spoofing is the probability that spoofing signal can't be detected; (2) The success probability of anti-spoofing increases as the input SNR increases, and increases as the spoofing signal amplification factor decreases, for the reason that it actually increases the SNR received, which increases the detection probability of true signal; (3) When the spoofing signal amplification factor is less than 1,the successful probability of anti-spoofing is approximately equal to 1, which indicates that when spoofing signal is weaker than true signal, it can't achieve spoofing. Overall, input SNR

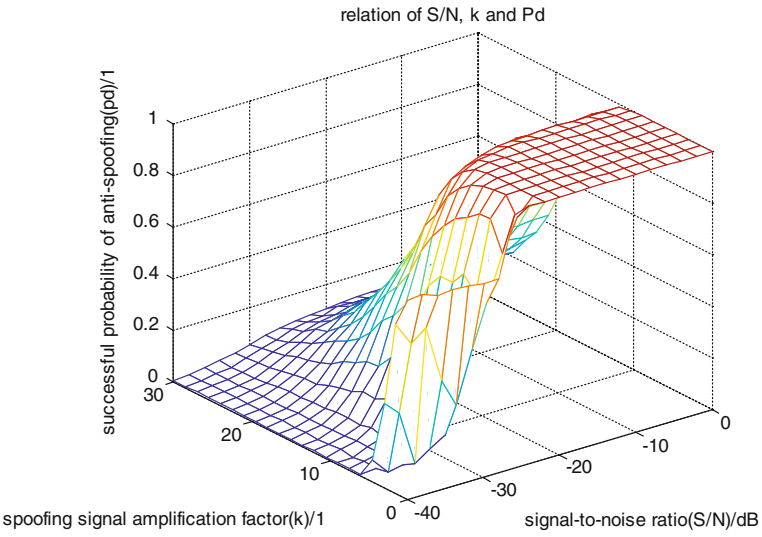


**Fig. 65.1** Influence of S/N and amplification factor of spoofing signal to the probability

plays a positive role to the successful probability of anti-spoofing, while spoofing signal amplification factor is negative. However, for the received signal, input SNR and spoofing signal amplification factor is immutable (unless changing the signal gain by using a directional antenna or by means of beam-forming), though they can affect the success probability of anti-spoofing, but do little use of anti-spoofing.

### 65.3.2 Coherent Integration Time $c_h$

The coherent integration time can bring the coherent integration gain, which can influence SNR and noise power of signal received, and therefore influence the threshold and the probability density function. Figure 65.2 shows the influence to the success probability of anti-spoofing $p_d$, where the probability of false alarm $p_{fa} = 0.001$ and input SNR $= -19$ dB.

Following points can be seen from Fig. 65.2: (1) The successful probability of anti-spoofing increases as the coherent integration time increases, for the reason that more coherent integration gain will be acquired when the coherent integration time increases, which actually increases the SNR received and increases the detection probability of true signal; (2) When the coherent integration time is determined, it can tolerable limited spoofing signal amplification factor, which means if the power rate between the spoofing signal and the true signal exceeds a certain threshold, it needs to increase the coherent integration time. Therefore, the coherent integration time plays a positive role to the successful probability of anti-

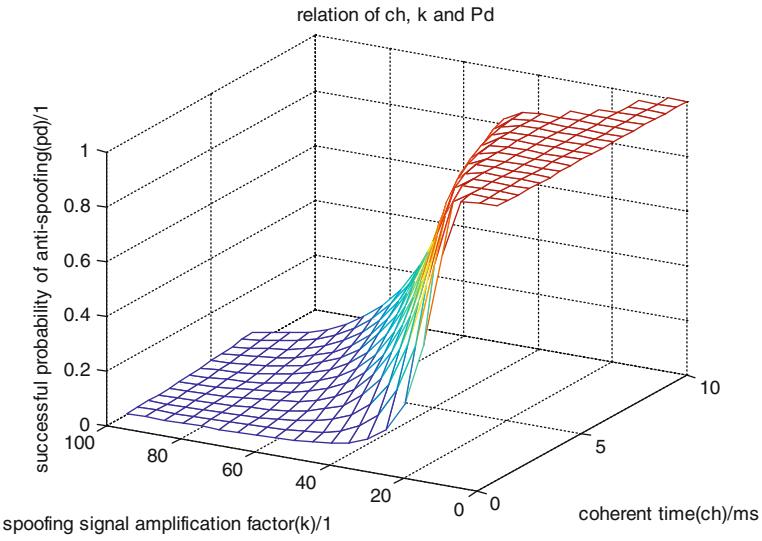


**Fig. 65.2** Influence of coherent integration time to the probability

spoofing, and the receiver can increase the successful probability of anti-spoofing by increasing the coherent integration time. However, the coherent integration time is influenced by the bit flip, and the frequency grid for searching will also increase as its increases, so the coherent integration time can't be increased unlimited.

### 65.3.3 Probability of False Alarm $p_{fa}$

According to formula 65.2, the probability of false alarm can have a direct influence on the threshold, which can influence the successful probability of anti-spoofing. Figure 65.3 shows the influence to the success probability of anti-spoofing $p_d$, where the input SNR $= -19$ dB and the coherent integration time $c_h = 1$ ms.

Following points can be seen from Fig. 65.3: (1) The successful probability of anti-spoofing increases as the probability of false alarm increases, for the reason that the threshold will be decreased when the probability of false alarm increases, which actually increases the detection probability of true signal; (2) When the probability of false alarm is determined, it can tolerable limited spoofing signal amplification factor, which means if the power rate between the spoofing signal and the true signal exceeds a certain threshold, in order to ensure a certain successful probability of anti-spoofing, it needs to increase the probability of false alarm. Therefore, the probability of false alarm plays a positive role to the successful probability of anti-spoofing, and the receiver can increase the successful probability of anti-spoofing by increasing the probability of false alarm. However, higher

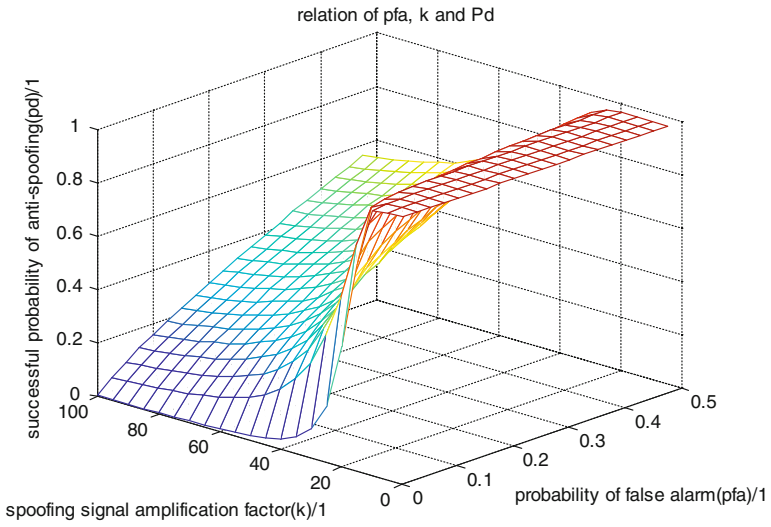


**Fig. 65.3** Influence of probability of false alarm to the probability

probability of false alarm means higher risk of error acquisition, for example: if the probability of false alarm is sixteen percent, it means that error acquisition may be occurred 16 per 100 times, which is a serious burden to receiver.

### *65.3.4 Summary of Factors that Impact Anti-Spoofing Performance*

There are many factors influencing anti-spoofing performance of threshold method. The input SNR and spoofing signal amplification factor influence the SNR of signal received by the receiver, which belong to the input of the receiver and can't be a mean of anti-spoofing (unless changing the signal gain by using a directional antenna or by means of beam-forming), but the revelation is that higher input SNR (such as the open environment) does favor to anti-spoofing performance; The coherent integration time and the probability of false alarm can also improve receiver's anti-spoofing performance, which both have their own limitations.

## 65.4 Analysis of the Upper Bound of Anti-Spoofing Performance

According to the above, it is not easy to absolutely quantize the anti-spoofing performance of the threshold method, however, we can quantitative assessment its anti-spoofing performance by deducing its bounds.

### *65.4.1 Determining the Upper Bound of Anti-Spoofing Performance*

The spoofing signal can cause interference and decrease the input SNR of the true signal. Considering carrier-to-noise ratio as standard of signal's quality available, we can describe influence of the spoofing signal as formula 65.7 [8] and 65.8:

$$(C_s/N_0)_{\text{eff,dB}} = -10\lg\left[10^{-\frac{(C_s/N_0)_{\text{dB}}}{10}} + \frac{k^2}{QR_c}\right] \tag{65.7}$$

$$(C_s/N_0)_{\text{dB}} = S/N + 10\lg(B) \tag{65.8}$$

Where $(C_s/N_0)_{\text{eff,dB}}$ is the carrier-to-noise ratio of the true signal with the spoofing signal added; $(C_s/N_0)_{\text{dB}}$ is the carrier-to-noise ratio of the true signal without the spoofing signal added; B is the bandwidth of the signal received; Q is

the quality factor of anti-jamming and for GPS P code, Q is approximately equal to 1.5; $R_c$ is the code rate.

To enable to detect the true signal, it is required that the signal-to-noise rate after the coherent integration is equal to which introduced by the threshold. In this case, the successful probability of anti-spoofing is approximately equal to 0, which is the upper bound of anti-spoofing performance of the threshold method. We can get formula 65.9:

$$(C_s/N_0)_{\text{eff,dB}} - 30 + 10\lg(c_h) - L(c_h) + \varepsilon = 10\lg(-2\ln p_{fa}) \tag{65.9}$$

Where $L(c_h)$ is the incoherent loss and $\varepsilon$ is losses of baseband signal processing.

In formula 65.9, in order to ensure that the threshold method can detect the true signal, it is needed that threshold is higher than the noise, so the right term is required to be larger than 0. Therefore, we can obtain the constraint condition as formula 65.10:

$$p_{fa} < 1/\sqrt{e} \tag{65.10}$$

Integrated formula 65.7, 65.8, 65.9 and 65.10, the upper bound of spoofing signal amplification factor tolerated can be calculated by the parameters given.

### 65.4.2 *Examples of the Upper Bound of Anti-Spoofing Performance*

The essence of anti-spoofing with threshold method is that the receiver competes with spoofing signal amplification factor by acquisition algorithm. According to the above, the algorithm is related to the coherent integration time and the probability of false alarm, and the input SNR also influences the anti-spoofing performance. As is given in formula 65.7 and 65.8, Fig. 65.4 shows the upper bound of the spoofing signal amplification factor tolerated when the probability of false alarm is fixed. In the figure, each curve represents a set of upper bound.

## 65.5 Conclusion

Threshold method is the most common algorithm used by the receiver, and research on its anti-spoofing performance is of great significance. In this paper, we define successful probability of anti-spoofing as the assessment standard and propose four factors that influence the successful probability of anti-spoofing: input SNR without spoofing signal, the spoofing signal amplification factor, the coherent integration time and the probability of false alarm. The results show that the input SNR without spoofing signal, the coherent integration time and the probability of false alarm can increase the anti-spoofing performance of the

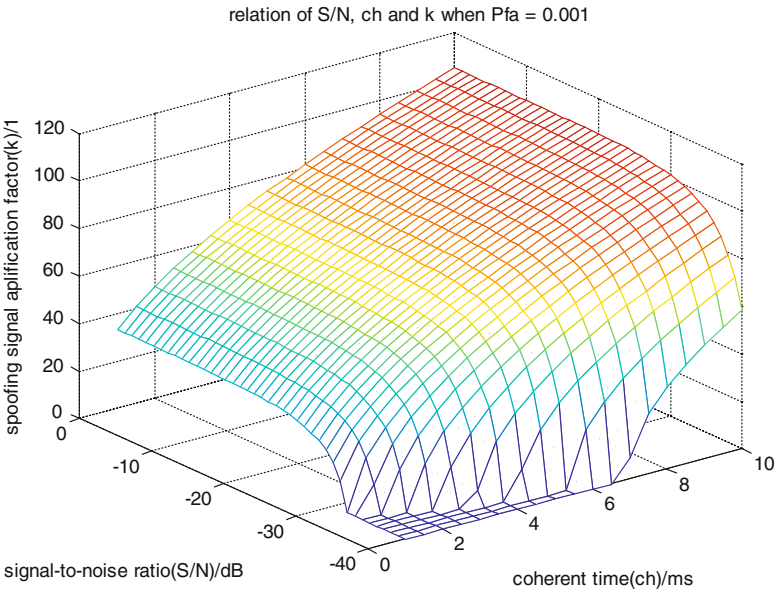


**Fig. 65.4** Influence of coherent integration time to the upper bound

receiver, but all have some limitations, the receiver need to balance each other in order to get the best anti-spoofing performance. Finally, we present the theoretical upper bound of the anti-spoofing performance of threshold method and give some examples, unify anti-spoofing performance with various factors, which has a guiding significance for the design of the receiver.

## References

1. Key EL (1995) Techniques to counter GPS spoofing, internal memorandum. MITRE Corporation, USA, Feb 1995
2. Wen H et al. (2005) Countermeasures for GPS signal spoofing. ION GPS, Long Beach. 13–16 Sept 2005
3. Humphreys TE et al (2008) Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: Proceedings of ION GNSS2008. Savannah, Institute of Navigation, GA, 2008
4. Cavaleri A et al. (2010) Detection of spoofed GPS signals at code and carrier tracking level. In: Satellite navigation technologies and European workshop on GNSS signals and signal processing, 2010
5. Montgomery PY, Humphreys TE, Ledvina BM (2009) Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In: Proceedings of the 2009 international technical meeting of the institute of navigation, Anaheim, 26–28 Jan, 2009
6. Daneshmand S, Jafarnia-Jahromi A, Broumandan A, Lachapelle G (2012) A low-complexity GPS anti-spoofing method using a multi-antenna array. In: Proceedings of ION GNSS 2012, 8–21 Sept, 2012

7. Huang L, Tang X, Wang F (2011) Anti-spoofing techniques for GNSS receiver. Geomatics Inf Sci Wuhan Univ 36(11): 1344–1347
8. Elliott D. Kaplan etc. (2008) Understanding GPS-principles and applications, 2nd edn. Publishing House of Electronics Industry