Chapter 58
The Modeling and Analysis for the Assessment of GNSS Spoofing Technology

Meng Zhou, Hong Li and Mingquan Lu

Abstract As various application of navigation technology penetrating people's life and national security, spoofing and anti-spoofing techniques have become hot research topics. Since more and more complicated spoofers have emerged, from repeater to creator, then to receiver-spoofer, the research of anti-spoofing is very urgent. Moreover, research and assessment on spoofing are prerequisite and foundation for anti-spoofing research. Considering various aspects of spoofing technology, including spoofing efficiency, blanket factor, influence area, destructiveness, and the risk of being determined, this paper explores the factors needed in comprehensive evaluation of GNSS spoofing technology. Through modeling the spoofing signals, this paper builds up an evaluation computing model for various metrics. And it analyzes the evaluation results of common spoofing technologies by utilizing various models. This paper also builds up a reference score model for these various metrics through expert scoring method. Finally, the paper also introduces the plan for future research work.

Keywords GNSS · Spoofing · Assessment · Modeling

58.1 Introduction

In 2001, the U.S. Department of Transportation released a report, which is about the vulnerability of the U.S. transportation system [1]. It reported that "as GPS further penetrates into the civil infrastructure, it becomes a tempting target that could be exploited by individuals, groups, or countries hostile to the U.S." This report showed that the spoofing has become one of the primary threats to the satellite

M. Zhou (✉) · H. Li · M. Lu
Department of Electronic Engineering, Tsinghua University, Beijing 100084, China
e-mail: maggice-sun@163.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_58,

navigation system as an artificial malicious interference. Spoofing usually makes position/navigation receivers generate wrong positioning or timing information by delaying the real signal or self-generated pseudo-signal. Compared to blanket jamming, spoofing is more concealed. Spoofing threats cannot be ignored in the scenarios like life safety services, financial services, and military confrontation.

Spoofing techniques that have been proposed and implemented can be divided into three categories: (1) Repeater: This approach works through broadcasting the received signal to the interfered region after delaying it and amplifying it. (2) Creator: This approach works through generating the pseudo-signals consistent with the same structure of real signal through the local signal generator [2]. (3) Receiver-spoofer: This kind of spoofer takes the data including Doppler, the pseudo-code delay, the navigation message and the time information which are token from received real signal flow into spoofing signal generator as input, and then generates pseudo-signals flow as output [4].

Therefore, it's extremely necessary to establish GNSS spoofing defense system as soon as possible. However, only a based on the deep research, analysis and evaluation of these spoofing methods, we can effectively the defense systems. The assessments of the spoofing performance and potential threats, can provide reference and guidance for the defense system.

58.2 Assessment Metrics for Spoofing

58.2.1 Valid Probability

A direct result of spoofing has only two states: spoofed and non-spoofed. Valid probability is the probability that the spoofer can successfully deceived GNSS receiver. If a GNSS receiver under deception still receives the normal navigation signal, it will be named as spoofing failure probability.

Spoofing valid probability varies with the GNSS receivers used. In the case with both actual and spoofing signal, we can calculate the probability of the two states of a certain receiver, spoofed or non-spoofed, by analyzing its signal capturing strategy, the receiving process and the anti-spoofing measures. The detailed calculating model and method will be demonstrated and discussed in the Sect. 3.1.

58.2.2 Blanket Factor

Blanket Factor is defined as the power ratio between spoofing signal and normal navigation signal to reach certain spoofing valid probability. Under the same constraint conditions, including receiver, spoofing valid probability and so on, the smaller blanket factor is, the more advanced the spoofing technique is.

58.2.3 Spoofing Region

Spoofing region includes distance and space coverage. With the constraint of spoofing valid probability, the further distance is, or the greater coverage is, the stronger the spoofer is.

58.2.4 Destructiveness

When spoofing successes, the most obvious impact is put on the positioning or timing results. But, the measurement of destructiveness varies indifferent application fields. For example, in the smart grid monitoring system, the GNSS timing function is used to measure the voltage and current phase of grid network. Once the timing is spoofed, that may lead to estimation errors on the grid, which guides the operator to make the wrong operation. In such applications, destructiveness of spoofing should be measured by the economic losses. In the navigation warfare, the use of spoofing to misleading the positioning result to a hostile missiles or other offensive weapons, will reach the purpose of disrupting the enemy's strategy and tactics. Its destructiveness should be measured by the extent of the impact of the war.

58.2.5 Onset Time

The time slot needed between the spoofer launching signals and the target receiver being impacted to a certain extent (for example, the pre-defined positioning results, or deterioration of positioning accuracy to pre-defined threshold) is called onset time. The shorter onset time of the spoofer is, the better performance of the spoofing technology is.

58.2.6 Spoofing Risk

The risk always appears with the benefits. The risk of a spoofer is being detected by the target receiver or even exposing its position to the anti-spoofing technology, which can bring danger to its own. Therefore, if a spoofer cannot disguise itself, although it is highly destructive, we are not able to profit from it. Thus, spoofing risk is an important indicator to assessment one spoofing technology. This assessment should include the reasonableness of signal power, arrival time, arrival azimuth, positioning result, and the similarity between spoofing signal and real navigation signals. The probability that the spoofer will be detected by the target receiver is a

good measurement for spoofing risk. The probability of being discovered is higher, and the risk is greater; the probability of being discovered is lower, and the risk is smaller (higher probability of being discovered means greater risk).

58.2.7 Technology Costs

This indicator is to test the difficulty of the technique to be implemented. If a kind of spoofing technology is too difficult to be achieved, or too costly to be massively produced, it would be more like an armchair strategist than an application, even through it is theoretically feasible, or even with good results. The cost is also one of important evaluation indices.

58.2.8 Comprehensive Assessment

As we mentioned above, it can be found that assessment of spoofing technique includes many factors. Some factors can be calculated by quantifying the specific values, and other factors (such as destructiveness, difficulty of achievement, etc.) are difficult to be quantitatively calculated. Therefore, it is necessary to explore an assessment model, which considers all these factors, to get a more objective assessment of spoofing.

58.3 Computing Model of Evaluation

58.3.1 Valid Probability Calculation

If spoofing signals and GNSS satellite signals at the receiver side co-exist during the capture phase, the receiver may detect the positioning signals through the GNSS satellite signals, or also possibly through spoofing signals. When the GNSS receiver regards a spoofing signal as a normal navigation signal to process, it is a valid spoofing. Capture is the first part of the receiver to receive and process navigation signals. Once the receiver catches spoofing signal, it will probably use the spoofing signal for subsequently tracking, demodulating, ranging, positioning calculating, and etc. Then it will be impacted by the spoofing signal. Therefore, we analyze the valid probability of spoofing from the capturing aspect in this paper. Capture performances are closely related to capture strategies of the receiver. In the same way of spoofing, the receiver adopting different kinds of capture strategies will cause a different probability of spoofing. It is assumed that the receiver uses the decision strategy of maximum threshold value.

58.3.1.1 Computing Model

During the dwell time T, in each cell, the I and Q signals are integrated and dumped and the envelope $\sqrt{I^2 + Q^2}$ is computed or estimated. Each envelope is compared to a threshold to determine the presence or absence of the SV signal. This method called the threshold decision is widely used in GNSS receivers. Figure 58.1 shows the probability distribution functions (pdf) of the envelopes of three signals, including the noise, real signals and spoofing signals. A similar concept was explained in [3].

The pdf for noise with no signal present, p_n, has a zero mean. The pdf for noise with the signal present, p_s, has a nonzero mean. The pdf for noise with the real signal and spoofing signal present, p_j, has a nonzero mean larger than p_s. For the chosen threshold, V_t, any cell envelope that is at or above the threshold is detected as the presence of the signal. Any cell envelope that is below the threshold is detected as noise. The two statistics that are of most interest for us are the probability of detecting real signal, P_{sd}, and the probability of detecting spoofing signal, P_{jd}. These are determined as follows:

$$P_{sd} = \int_{V_t}^{\infty} p_s dz \tag{58.1}$$

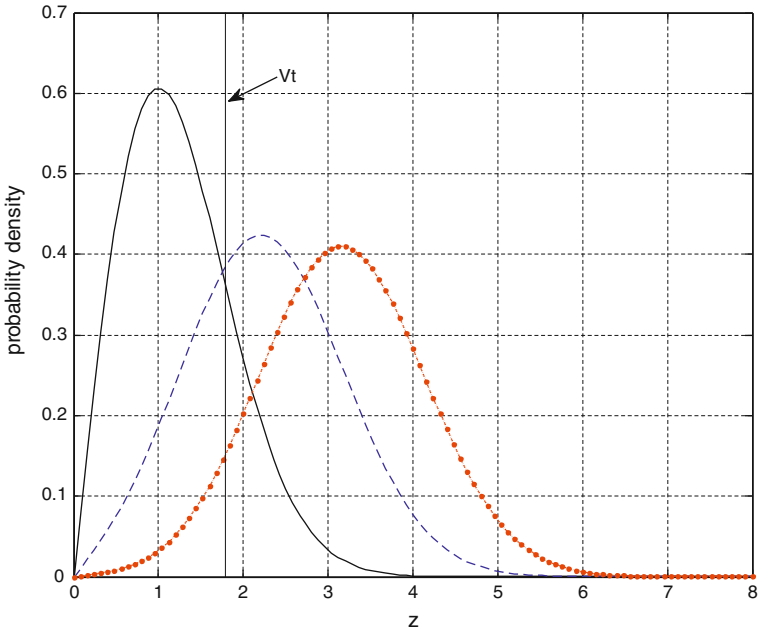

Fig. 58.1 Pdfs of the noise, navigation and spoofing signals

$$P_{jd} = \int_{V_t}^{\infty} p_j dz \tag{58.2}$$

where:
$p_s(z)$ pdf of the real signal's envelope
$p_j(z)$ pdf of the spoofing signal's envelope

We assume that case 1 represents a detection of a real signal, case 2 represents a detection of a spoofing signal, and case 1 and 2 are independent. Thus, we can have the following conclusions:

1. The probability that the real signal and spoofing signal are detected simultaneously is:
$$P_{s\cap j} = P_{sd} \times P_{jd} \tag{58.3}$$

2. The probability of only detecting the spoofing signal is:
$$P_{\bar{s}\cap j} = (1 - P_{sd}) \times P_{jd} \tag{58.4}$$

3. The probability of only detecting the real signal is :
$$P_{s\cap\bar{j}} = P_{sd} \times \left(1 - P_{jd}\right) \tag{58.5}$$

4. The probability that the real signal and spoofing signal are not detected is:
$$P_{\bar{s}\cap\bar{j}} = (1 - P_{sd}) \times \left(1 - P_{jd}\right) \tag{58.6}$$

When situation (2) occurs, the receiver is spoofed, and when situation (3) and (4) occur, the receiver is non-spoofed. Under situation (1), that the real signal and spoofing signal are detected simultaneously, the decision strategy of receiver determines whether the spoofing is successful or not. If the receiver selects signals by timing (first or second appear), the successful spoofing can be ensured by controlling the arrival time of spoofing signal. If the receiver adopts maximum decision, for example, choosing the bigger one between two signals, the probability of valid spoofing equals to the probability that spoofing signal j is higher than real signal s under situation (1), which is determined as follow:

$$\oint_{j>s} p(s,j) = \int_{V_t}^{\infty}\int_{s}^{\infty} p_{s\cap j} djds = \int_{V_t}^{\infty} p_s \int_{s}^{\infty} p_j djds \tag{58.7}$$

We assume that I and Q have a Gaussian distribution. Assuming that the envelope is formed by $\sqrt{I^2 + Q^2}$, then Thus,p_s and p_j are Ricean distributions defined by:

$$p_s(z) = \begin{cases} \frac{z}{\sigma_n^2} e^{-\left(\frac{z^2+A^2}{2\sigma_n^2}\right)} I_0\left(\frac{zA}{\sigma_n^2}\right), & z \geq 0 \\ 0, & z < 0 \end{cases} \tag{58.8}$$

where:

z	value of the random variable
σ_n^2	RMS noise power
A	RMS signal amplitude
$I_0\left(\frac{zA}{\sigma_n^2}\right)$	modified Bessel function of zero order

Equation (58.8) for z ≥ 0 can be expressed in terms of the predetection SNR as presented to the envelope detector, *C/N* (dimensionless), as follows:

$$P_s(z) = \frac{z}{\sigma_n^2} e^{-\left(\frac{z^2}{2\sigma_n^2} + C/N\right)} I_0\left(\frac{z\sqrt{2C/N}}{\sigma_n^2}\right) \tag{58.9}$$

where:

C/N	$C/N = A^2/2\sigma_n^2 = (C/N_0)T$, is predetection of signal to noise ratio
T	search dwell time

Considering formula (58.1), (58.2), (58.3), (58.4), (58.7) and (58.9), let $\sigma_n = 1$ (normalized), spoofing valid probability can be expressed as the function of C/N_0 (real signal to noise ratio), J/N_0 (spoofing signal to noise ratio), and T.

58.3.1.2 Analysis of Computing Results

The proposed method has been tested by the Matlab software in order to observe that how far the parameters like C/N_0, J/N_0, and T can impact the spoofing valid probability. The following parameters setting have been considered for the test:

1. The threshold in terms of the desired single trial probability of false alarm P_{fa} and the measured 1-sigma noise power: $V_t = \sqrt{-2\sigma^2 lnP_{fa}}$. Let $\sigma_n = 1$ (normalized), $P_{fa} = 0.16$, then the threshold $V_t = 1.9144615$.
2. Let C/N = 1 and J/N = 1–10(step intervals is 0.5). Let C/N = 2 and J/N = 2–10(step intervals is 0.5). Let C/N = 3 and J/N = 3–10 (step intervals is 0.5).

Figures 58.2, 58.3, 58.4 show the results with the parameters set above.

As can be seen from Figs. 58.2–58.4: (1) as detecting the two signals simultaneously, the probability that the spoofing signal is greater than the normal

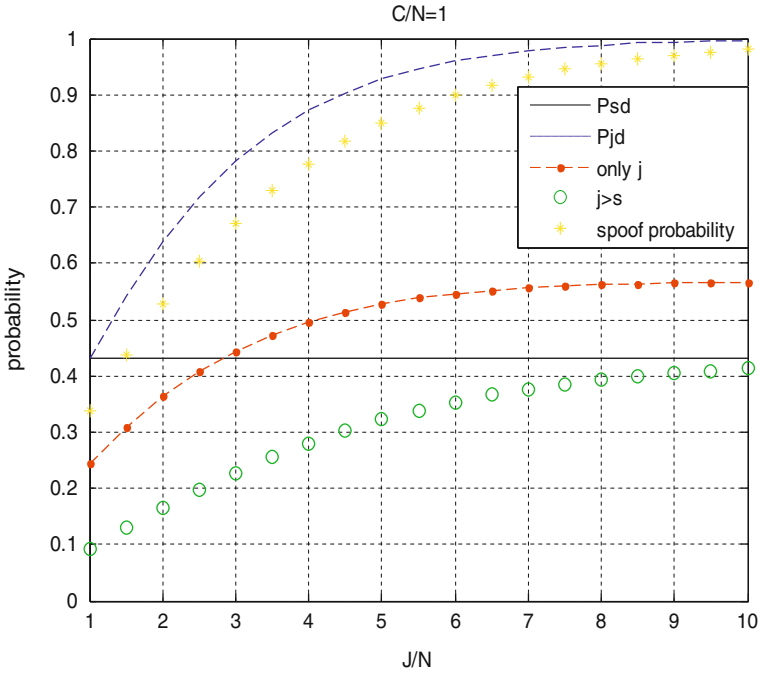

Fig. 58.2 The spoofing probability with C/N = 1

navigation signal increases significantly according to the increasing of J/N, whereas the probability that only the spoofing signal is detected does not change much; (2) spoofing probability is always less than the detection probability of spoofing signals, but with the increasing of J/N, spoofing probability will gradually approaching the detection probability; (3) when the C/N is small (C/N = 1), in the composition of the spoofing probability, the deception caused by situation (2) is greater than the one by situation (1); when C/N is greater (C/N = 2,3), the deception resulted by situation (1) is greater than the one by situation (2).

In addition, we can see from Figs. 58.2–58.4, the changing trend of the spoofing probability are accordant with different setting of C/N. When J/N is greater than 12, the spoofing probability tends to 100 %, and it changes slowly. In order to better observe the change trend of the spoofing probability, the first derivative plates of curve shown above are presented in Fig. 58.5.

As the plates suggest, at J/N∈[1, 6], the change rate of probability is much higher than in other region. When J/N is greater than 12, the change rate is less than 0.01. Therefore, we can get the greatest improvement of spoofing probability by increasing J/N in interval [1, 6]. However, once J/N is over 12, with the increase of J/N, it will raise the risk of being discovered, instead of the improvement of the spoofing valid probability.

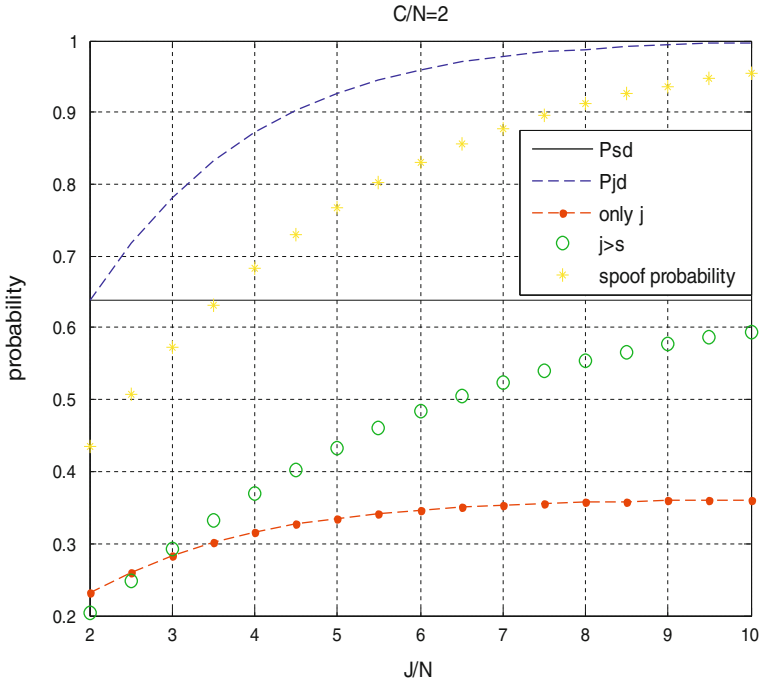

Fig. 58.3 The spoofing probability with C/N = 2

58.3.2 Calculation of Blanket Factor

58.3.2.1 Blanket Factor Lower Limit Computing Model

Blanket factor is the power ratio between spoofing signal and normal navigation signal to reach the certain spoofing valid probability. For $J/N = m \cdot C/N$, the m is named as the blanket factor. Based on the previous analysis, spoofing valid probability can be expressed with C/N and *m*.

Set the minimum blanket factor as the optimization target, and spoofing valid probability as the constraint. The optimization function can be determined as follow:

$$\begin{cases} \min \mathrm{m} \\ \text{s.t. } \mathrm{P}(\mathrm{m}, \dfrac{\mathrm{C}}{\mathrm{N}}) \geq \mathrm{P}_0 \end{cases} \tag{58.10}$$

According to formula (58.10), we can calculate the lower limit of the blanket factor *m*.

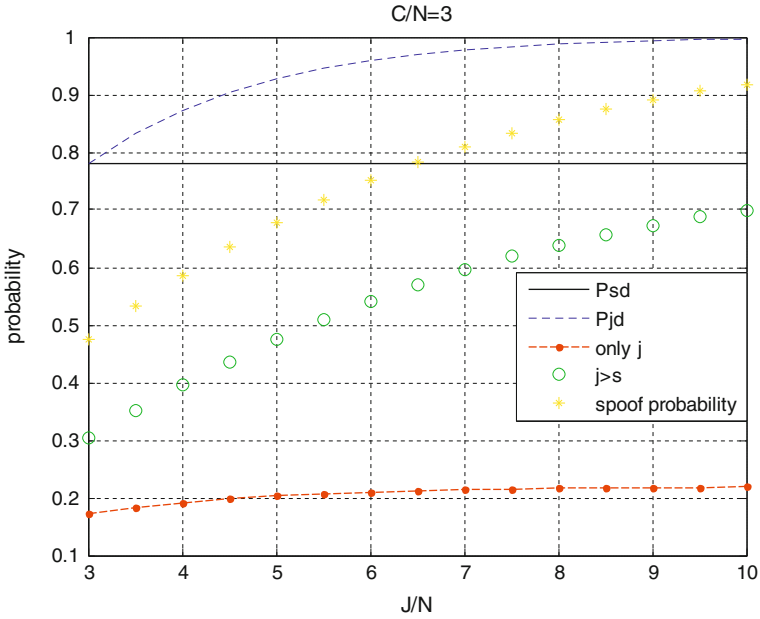

Fig. 58.4 The spoofing probability with C/N = 3

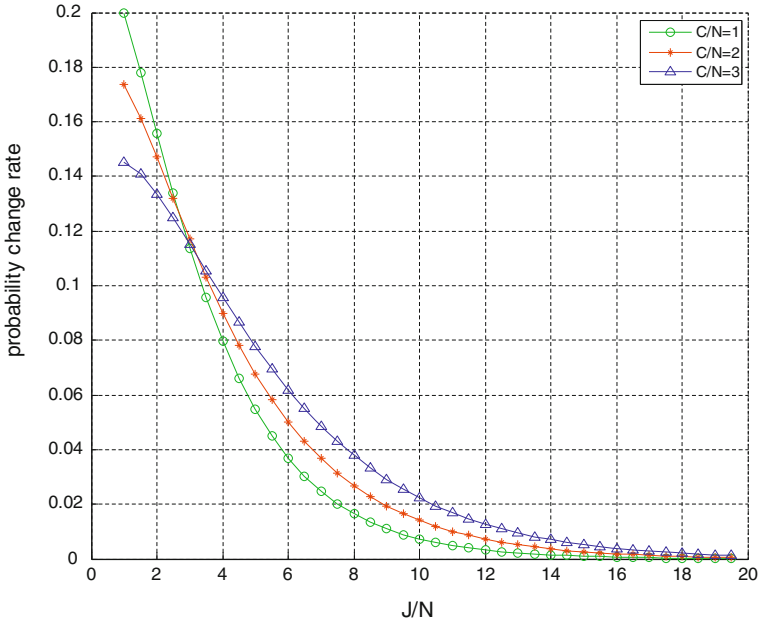

Fig. 58.5 The change rate of spoofing probability

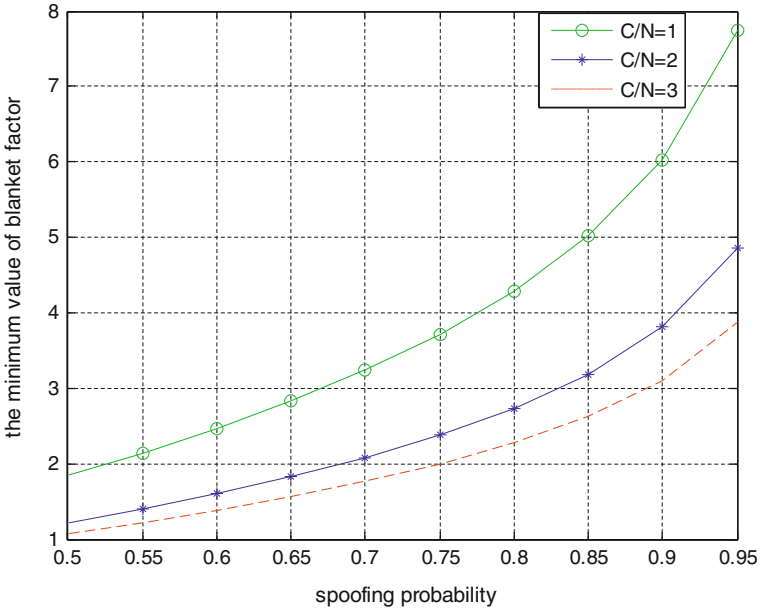

Fig. 58.6 The minimum value of blanket factor

58.3.2.2 Analysis of Computing Results

The proposed method has been tested with a Matlab simulation. The following parameters setting have been considered for the test:

1. Let $\sigma_n = 1$ (normalized), $P_{fa} = 0.16$, then the threshold $V_t = 1.9144615$.
2. Let C/N = 1, 2, and 3, respectively, and spoofing valid probability = 50–95 % (step intervals is 5 %).

Figure 58.6 shows the results with the parameters set above.

As shown in Fig. 58.6, the bigger C/N is, the lower the lower limit of blanket factor is. This is because the blanket factor is equivalent to the amplification factor between J/N and C/N. With the increasing of C/N, the desired blanket factor is smaller to reach the same J/N.

58.3.3 Onset Time

Determination of the Onset Time is divided into two parts. One is the time t_1, represents the time slot from the spoofer emitting the spoofing signal to the receiver capturing that spoofing signal. Another is the time t_2, represents the time slot from the receiver capturing the spoofing signal to its positioning or GPS clock

resulting error to reach the desired value. It is necessary to measure the two time values to assess the performance of spoofer respectively, and gives a comprehensive evaluation result.

58.3.4 Spoofing Risk

The risk of spoofing can be quantitatively evaluated by the probability of being perceived by the target receiver. Means of spoofing detection are usually independent to each other, that is, the detection process can be considered to be a series of several detectors. We assume that P_1 is the detection probability of detector A and P_2 is the detection probability of detector B, then the probability of the two detectors to perceive spoofing signals is given follow:

$$\mathrm{P} = 1 - (1 - P_1) \times (1 - P_2) \tag{58.11}$$

Without loss of generality, we can define the risk function of a specific spoofing technique as follow:

$$\mathrm{P} = 1 - \prod_{i=1}^{n} (1 - P_i) \tag{58.12}$$

where, P_i is the probability that the *i*th detector of the target receiver perceives this spoofing signal.

As can be seen from the definition of the risk function, the more spoofing detection means of a receiver have, the greater risk of the spoofing signal to be detected.

58.3.5 Other Indicator

The other assessment indicators such as destructiveness and technology cost are difficult to be quantified. So we consider to adopt the expert evaluating method for these indicators.

58.3.6 Comprehensive Assessment

Expert scoring method is a qualitative description method. First, it selects several indicators according to the specific requirements. Then it develops the criteria based on the evaluation project. After that, a number of representative experts will be employed. Each of the experts will give a score to the indicators by their experience. Last, the score will be compiled. The characteristics of this method are simple, intuitive, and easy in computing. Furthermore, it is able to calculate

quantitatively and can conduct the evaluation for those indicators, which cannot be calculated. Therefore, this is a good way to do comprehensive assessment. Nowadays, to compile the scores, additive evaluation method, product evaluation method, and multiplying evaluation method, the weighted evaluation method, the efficiency coefficient method are often used.

Because of the multi-attribute of spoofing technical, we usually use the weighted evaluation method for the assessment. The valid probability is the assessment constraints, based on expert experience. And we calculate jamming indicator, destructiveness and onset time, to obtain a comprehensive assessment of the results.

58.4 Conclusions

This paper has mentioned many factors to provide a comprehensive assessment for GNSS spoofing technic, such as: valid probability, blanket factor, spoofing region, destructiveness, spoofing risk. An evaluation model for these indicators is established in this paper. Furthermore, evaluation results based on this model are analyzed. In future research, in order to prove the models and methods which are presented above, a spoof simulation environment will be built to generate spoof signal.

References

1. John A (2001) Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System, Tech. rep. Volpe National Transportation Systems Center, USA
2. Warner J, Johnston R (2003) A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. J Secur Admin (In Press)
3. Kaplan ED, Hegarty CJ (2006) Understanding GPS: principles and applications [M]. Artech House Publishers, UK
4. Humphreys TE, Ledvina BM, Psiaki ML, O'Hanlon BW, Kintner PM Jr (2008) Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: Proceedings of the ION GNSS meeting. Institute of Navigation, Savannah