

Chapter 20

A GNSS Anti-spoofing Method Based on the Cooperation of Multiple Techniques

Huiqi Tao, Hong Li and Mingquan Lu

Abstract An anti-spoofing technique based on the cooperation of multiple detections is proposed in this paper. A GNSS receiver could detect more than one correlation peak in one processing channel in acquisition when the spoofing signal exists. Signal quality monitoring (SQM) can detect abnormal changes of the correlation peak when spoofing attack on tracking receiver. Generally, receiver gives up the measurements of the abnormal channel to avoid the risk of tracking fault or spoofing signal. This decreases the number of available signals. Receiver autonomous integrity monitoring (RAIM) is capable of detecting and mitigating single error but lack of dealing with multiple errors. This paper proposes a cooperation method of these three techniques which are complementary. Detailed discussion of the method's procedure and performance are provided in this paper. Simulation results demonstrate that the method is feasible and effective to detect and mitigate multiple spoofing signals.

Keywords Anti-spoofing · Multi-peak detection · SQM · RAIM · Cooperation

20.1 Introduction

Security of GNSS applications has been paid more and more attention with the popularization of positioning and navigation applications. As GNSS signals are vulnerable to interferences and easy to be counterfeited, and there have been relevant reports that devices with low cost had implemented successful spoofing. The experiment taken by Humphreys's team in 2013 has been widely known, they

H. Tao (✉) · H. Li · M. Lu
Department of Electronic Engineering, Tsinghua University, Beijing 100084, China
e-mail: thq12@mails.tsinghua.edu.cn

spoofed a yacht successfully using a GPS spoofing device, and the yacht was tricked onto a parallel track hundreds of meters from its intended one. Therefore, anti-spoofing technique has become a new focus in GNSS studies. There have been many anti-spoofing techniques in different processing levels [1], such as power monitoring in signal processing, consistency check of ephemeris in data bit level, and comparing with other system in position solution level, etc. Some techniques are effective but complex, for instance, spatial processing which uses multi-antenna array is effective to detect medium spoofing that uses only one transmit antenna, but it is too sophisticated to implement in a general GNSS receiver.

Receiver autonomous integrity monitoring (RAIM) is a practical implementation that does not impose extensive hardware modifications to the receiver [2]. RAIM uses the redundant information to detect and exclude the fault signal by checking the consistency of measurements or position solution. In essence, spoofing signals are faults to authentic signals. Therefore, RAIM is a practical anti-spoofing implementation. Typically, RAIM is effective to defense single fault signal or spoofing. For the purpose of improving RAIM's performance, additional information needs to be provided. Some extended RAIM methods take advantage of measurements in other frequencies, constellations, and systems [3, 4], they can detect and mitigate more than one fault signal, but they are too hard to implement in low cost receiver.

Besides, some basic detection may be helpful to RAIM, such as power monitoring, multi-peak detection in acquisition, or signal quality monitoring (SQM) [5] in tracking, etc. These techniques could detect the abnormal changes of receiver's processing channels, such as abnormally sharp or elevated correlation peaks. In fact, any abnormality is likely to indicate the error, especially spoofing signal. It's arbitrary to give up the measurements of these channels and this would decrease the number of available signals. On the other hand, it's difficult to make sure that abnormalities are caused by spoofing. For instance, multipath effects and thermal noise may affect the performance of SQM. However, receiver could take advantage of these techniques to detect the abnormal changes and check them using RAIM. The cooperation of them could exclude more spoofing signals and improve the reliability of PVT solution.

This paper researches the cooperation of these techniques to defense more than one spoofing signal, and the cooperation is medium complexity to implement in general GNSS receivers. The architecture of cooperation is proposed in this work. Some spoofing scenarios are discussed, and the performance of the cooperation solution is simulated as well. The remainder of this paper is organized as follows: Sect. 20.2 analyzes the performance of basic RAIM under multi-spoofing signals and discusses RAIM detection with the aids from acquisition and tracking. Multi-peak detection and SQM which provide the aids are discussed in this section as well. Section 20.3 provides the simulation of the cooperation anti-spoofing method for detecting and mitigating two and three spoofing signals. The finally conclusions are provided in Sect. 20.4.

20.2 The Cooperation of Multiple Techniques

Anti-spoofing techniques could be classified in terms of spoofing detection and spoofing mitigation, authors of [1] provide a brief review of them. Although each technique plays unique role in anti-spoofing architecture, the cooperation of them has not received enough attention. Especially, some detection techniques could find but cannot mitigate the faults, while some mitigating techniques do not have enough ability to deal with multiple faults. Thus, cooperation of multiple detections is necessary to improve the performance of anti-spoofing. This section focuses on three basic techniques and the cooperation of them. They are multi-peak detection in acquisition, SQM in tracking, and RAIM in positioning solution. These three techniques aim at different problems in different steps of signal and information processing, they are complementary and easy to cooperate.

20.2.1 Multi-peak Detection in Acquisition

Compared with other techniques in acquisition such as power monitoring, multi-peak detection does not require complex hardware and is easier to implement. Assuming that an authentic signal and its counterfeit are mixed and received before the victim receiver locks the authentic signal of this satellite, the received signal can be expressed as follow

$$\begin{aligned}
 s^i(t) &= s_A^i(t) + s_S^i(t) \\
 &= \sqrt{P_A}D_A(t)C^i(t) \sin(2\pi ft) + \sqrt{P_S}D_S(t - \tau)C^i(t - \tau) \sin(2\pi f_s(t - \tau))
 \end{aligned}
 \tag{20.1}$$

where the subscripts A and S correspond the authentic signal and spoofing signal. P, D, C, f, and τ are the signal power, navigate data, pseudo-random code, carrier frequency integrated Doppler shift, and code delay, respectively. Although the power of spoofing signal maybe higher than the authentic signal, it's very hard to suppress the authentic signal completely. Unless the spoofer aligns the carrier frequency and phase and code delay to the authentic signal, there would be more than one correlation peak in the process of acquisition in the receiver. If two correlation peaks are detected in acquisition, receiver needs to track both two signals to avoid the risk of tracking the counterfeit signal. The authenticity of two signals can be checked by subsequent detections such as code and phase rate consistency check, RAIM, and so on. This strategy of acquisition and tracking requires additional tracking channels and increases processing complexity. But in some cases, it's not necessary to implement this strategy for all satellites, detailed discussion is provided in subsequent section.

20.2.2 SQM in Tracking

If the spoofing signal attacks the receiver which is tracking the authentic signal, abnormal changes of correlation peak may appear in the process of aligning the spoofing signal to authentic signal. SQM is a basic technique to monitor the correlation peak quality. Two detection tests, delta test and ratio test, are proposed in [5], they are given by (20.2) and (20.3) respectively.

$$\Delta = \frac{I_E - I_L}{2I_P} \quad (20.2)$$

$$R = \frac{I_E + I_L}{2I_P} \quad (20.3)$$

where I_E , I_L , and I_P are the respective in-phase early, late, and prompt accumulations. Delta test is designed to identify asymmetric correlation peaks while ratio test is designed to identify abnormally sharp or elevated correlation peaks. Assuming that signal has been locked by the carrier PLL and the space of correlators is half code chip, the nominal value of delta test is 0 while the nominal value of ratio test is 0.5. The threshold of the test is a key point because the thermal noise or multipath effects may affect the shape of correlation peak. Discussion about threshold can be found in [3] as well.

20.2.3 RAIM Under Multi-spoofing Signals

RAIM is a basic technique to detect and exclude single fault in GNSS receivers. It is based on the assumption that simultaneous multiple-satellite faults occur with an extremely small probability, but this assumption is not true in case of spoofing. Spoofing signals are difficult to distinguish with authentic GNSS signals as the structure of GNSS signal is known publicly. The spoofer would project the false signals with correct signal delay and strength as far as possible for the purpose of misleading or deceiving the victim receiver into pre-specified PVT solution. Thus, more than one spoofing signal is possibly locked by the victim receiver.

RAIM detects the fault signal by comparing test statistic based on pseudorange measurements with the threshold calculated using chi-square method. Least square residual method and parity vector method are two basic RAIM algorithms and they are equivalent [2]. Some improved methods based on them could deal with two faults, such as NIORAIM [6], OWAS [7], and some other extended RAIM algorithms [8]. But they need additional information such as measurements in other frequencies or constellations, they are too complicated to implement in low cost receivers. A detailed theoretical analysis of RAIM under the condition of two errors has been provided in [9], the position error vector and test statistic are given as follows.

$$\begin{aligned}
 E_{ij} &= A[0, \dots, \varepsilon_i, \dots, \varepsilon_j, \dots, 0] \\
 &= [A_{1i}\varepsilon_i + A_{1j}\varepsilon_j, A_{2i}\varepsilon_i + A_{2j}\varepsilon_j, A_{3i}\varepsilon_i \\
 &\quad + A_{3j}\varepsilon_j, A_{4i}\varepsilon_i + A_{4j}\varepsilon_j]^T \\
 &= E_i + E_j
 \end{aligned}
 \tag{20.4}$$

$$\begin{aligned}
 SSE_{ij} &= \sqrt{w^T w} \\
 &= \sqrt{S_{ii}\varepsilon_i^2 + S_{jj}\varepsilon_j^2 + 2S_{ij}\varepsilon_i\varepsilon_j}
 \end{aligned}
 \tag{20.5}$$

Equations (20.4) and (20.5) give the PVT error vector and the test statistic of RAIM under two errors. E_i and E_j denote the PVT errors vector corresponding to measurement errors ε_i and ε_j respectively. E_{ij} is the sum of vectors E_i and E_j . As shown in (20.5), the statistic test is determined by not only the errors but also the geometric distribution of receiver and satellites. It can be concluded that the test statistic is related to the combination of two errors. Some combinations would be easy to be detected and some would be hard. Assuming that one of two errors can be detected and mitigated by RAIM, the other one can be dealt with by RAIM again.

20.2.4 The Cooperation of Three Techniques

Based on the above discussion, three techniques are located in different steps of signal and information processing steps. Multi-peak detection in acquisition and SQM in tracking are capable of finding spoofing signals but they cannot mitigate the spoofing signals, while RAIM in position solution can mitigate the error but it is lack of finding more errors. They are complementary and easy to implement the cooperation. The procedure of cooperation anti-spoofing method based on them is proposed as Fig. 20.1.

As shown in Fig. 20.1, multi-peak detection and SQM classify the measurements into three sets and RAIM check the correctness of them respectively. If more than

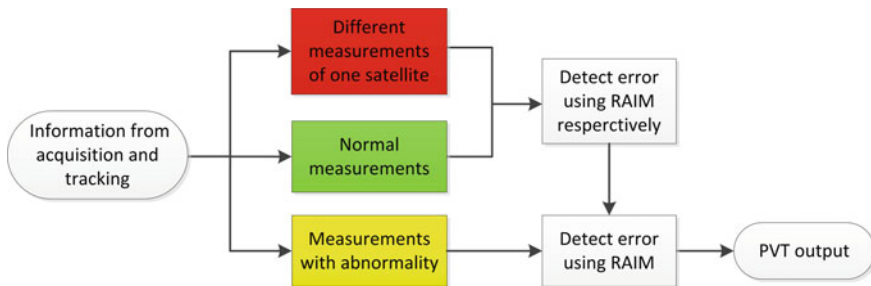


Fig. 20.1 Procedure of cooperation anti-spoofing method

one correlation peak is detected in acquisition, each of them is tracked by receiver and the measurements are classified a set. Besides, SQM can detect abnormalities of channels where spoofing signals attack the authentic, measurements of these channels are classified a set as abnormal. Each measurement of these two sets must be check with normal measurements using RAIM respectively. The correctness of the classification is the key of this method. In theory, every spoofing signal can be detected and mitigated as long as the normal measurements' number is no less than 5, where 5 is the minimum number required by RAIM algorithms.

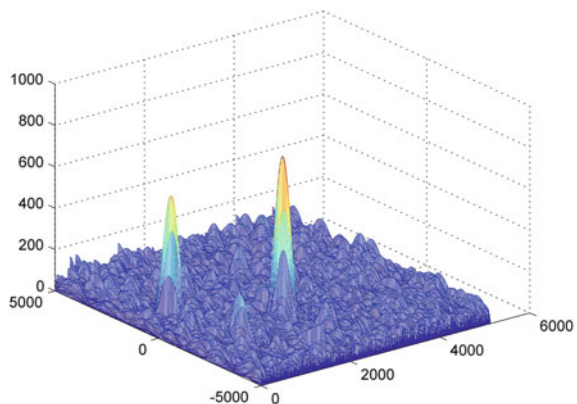
20.3 Simulations

The previous three techniques are simulated respectively in a software-defined GPS receiver. The authentic signal is generated by a GPS signal generator which is capable of generating 10 channels of GPS L1 C/A-code signals simultaneously. Spoofing signals are the delayed sampling of authentic signals and the strength can be falsified. The delays can simulate the pseudorange errors of spoofing signals, especially the retransmit-spoofing signals.

Multi-peak detection in acquisition can be realized in general GPS receivers. Figure 20.2 shows the result of multi-peak detection if an authentic signal and its counterfeit are mixed and acquired together. The amplitude of correlation peak relates to signal's power. Spoofer must project the counterfeit signal with proper strength to skip the detection based on power monitoring. The power of authentic and spoofing signal would be similar and this is propitious to multi-peak detection. As previously mentioned, as long as more than one peak is detected, receiver should set up corresponding channels to track each of them.

The key point of the proposed cooperation method is to track each acquired signal and provide the measurements to PVT solution respectively. SQM in tracking and RAIM in PVT solution are simulated in detail. Figure 20.3 shows the process of spoofing attack on tracking receivers.

Fig. 20.2 The change of correlation peak in the process of spoofing attack on tracking receivers



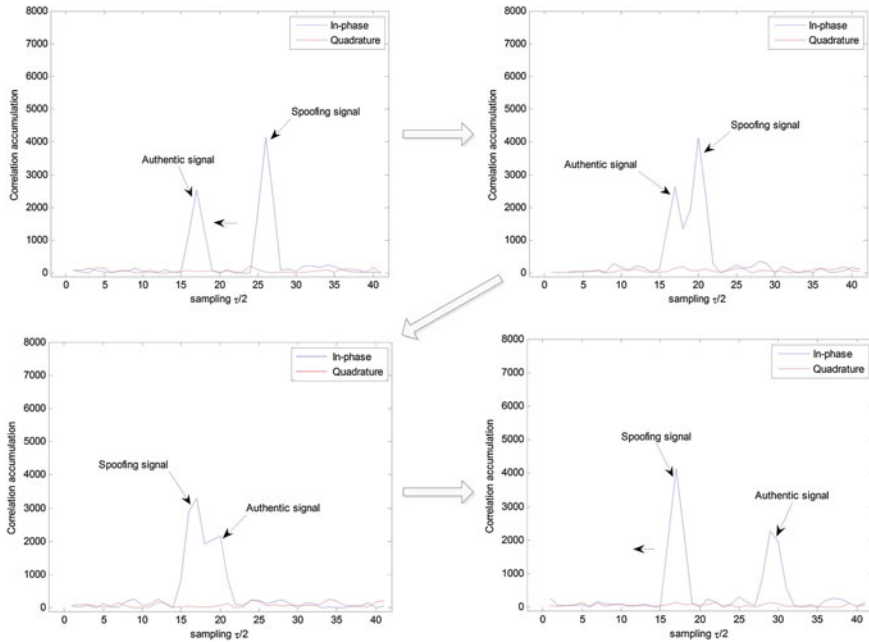


Fig. 20.3 The change of correlation peak in the process of spoofing attack on tracking receivers

As shown in Fig. 20.3, authentic signal is locked by receiver at the start and the spoofing signal is moving toward the authentic with the rate of 4 chips per second. The spoofing signal’s power is 3.5 dB higher than the authentic signal’s power. When the spoofing signal’s code phase aligns the authentic signal, both signals are locked. Then, the receiver locks the signal with higher power, that is, authentic signal is suppressed by the spoofing signal. There is an obvious change on the shape of correlation peak and this change can be reflected from the SQM tests.

Figure 20.4 shows the ratio test and delta test defined as (20.2) and (20.3) in different signal-to-noise ratio (SNR). The value of delta test is no longer equal to 0 and the nominal value of ratio test is no longer equal to 0.5 when the spoofing signal closes to the authentic. The SNR in left figure is -10 dB and the SNR in right figure is -15 dB. Comparing tow figures, it’s obvious that the curves of both tests have different jitter in different SNR. However, these changes of SQM tests are obvious and they indicate the faults. PVT solution can not employ this channel’s measurements as normal. They are treated as distrustful and checked using RAIM respectively in the follow-up process.

As described in Fig. 20.1, abnormalities of acquisition and tracking should be dealt with respectively in PVT solution using RAIM. However, RAIM’s performance without any aids under multi-spoofing is simulated, and this is meaningful to assess the performance of cooperation anti-spoofing. Assuming that one of the two errors can be isolated correctly using RAIM, the remainder measurements still

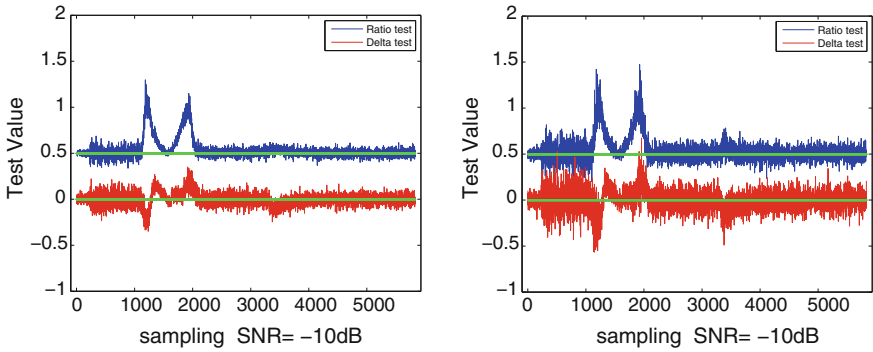


Fig. 20.4 The SQM tests in the process of spoofing attack on tracking receivers

contain one error and this one can be detected and mitigated using RAIM again. The simulation results of repeat RAIM in the case of two errors are provided in detail next.

In this simulation, the signal of 9 satellites is acquired and tracked by the software-defined GPS receiver. The constellation of 9 satellites is shown in Fig. 20.5. Receiver extracts the pseudo-range measurements and falsifies them to simulate the spoofing signals.

Two measurements errors are combined in simulations. The number of two measurements combinations is 36 as the total number of satellites is 9. Table 20.1 shows 8 measurements errors add to the riginal measurements. The errors range from 50 M–100 K. These values cover the most cases of spoofing in practice. Accordingly, there are 64 combinations of two errors with two different satellites.

Fig. 20.5 Constellation of the 9 GPS satellites in simulations

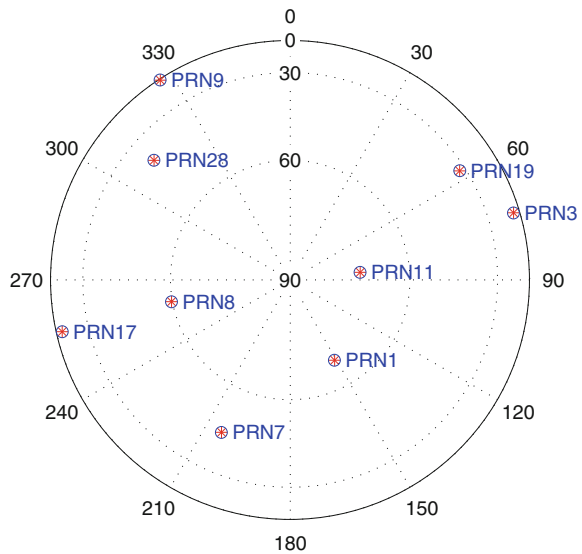


Table 20.1 Numerical value of measurements errors

Errors	Value (m)	Errors	Value (m)
E1	5×10^1	E5	5×10^3
E2	1×10^2	E6	1×10^4
E3	5×10^2	E7	5×10^4
E5	1×10^3	E8	5×10^5

Table 20.2 The statistics of numerical value of successful detection for every pair of measurements of 9 satellites

	E1	E2	E3	E4	E5	E6	E7	E8
E1	36	36	36	36	36	36	36	36
E2	36	36	36	36	36	36	36	36
E3	36	36	29	35	36	36	36	36
E4	36	36	34	29	36	36	36	36
E5	36	36	36	36	29	35	36	36
E6	36	36	36	36	34	29	36	36
E7	36	36	36	36	36	36	29	35
E8	36	36	36	36	36	36	34	29

The simulation results statistics of RAIM in two errors scenarios is shown in Table 20.2. The number in each unit of the table corresponds to the number of successful spoofing detection. For instance, the number in lower right unit is 29, it means that there are 29 successful spoofing detections while 7 detections are failed. A successful detection means both errors are detected correctly and the PVT errors do not exceed the preset limit. Table 20.2 shows that only a few errors combinations can't be detected and mitigated completely. The units with these combinations are colored. It is obvious that the failed detections are concentrated in the diagonal line of the table which represents the combinations that both errors are equal. Figure 20.6 shows the diagonal line numbers' bar graph.

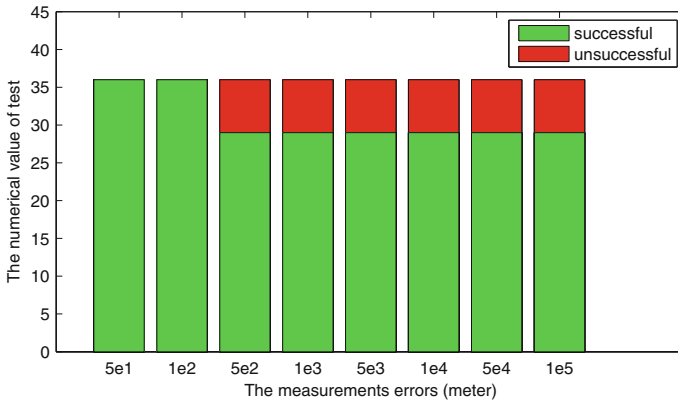


Fig. 20.6 Bar graph of detections with equal errors for every pair of measurements of 10 satellites

The simulation results show that RAIM performs well without any aids in most cases of two errors. It can be concluded that cooperation of RAIM and other spoofing detections would perform better. In fact, most unsuccessful detections are concentrated in a few satellites combinations and a few errors combinations. In other words, just a few combinations are easy to get wrong using RAIM repeatedly. As mentioned previously, it's unnecessary to implement multi-peak detection and tracking each peak strategy for all satellites, for instance, in the case of two spoofing signals, only a few satellites combinations need that strategy, and this is depend on the distribution of satellites and receiver.

Combine the above simulations, it can be concluded that classification of the measurements in Fig. 20.1 determines the performance of the proposed cooperation anti-spoofing method. As long as the number of normal measurements is no less than 5, every spoofing signal can be detected and mitigated. 5 is the minimum number required by RAIM and it ensures the consistency check of the normal measurements. The actual performance of the method can be better than this, because repeat RAIM is capable of dealing with more than one spoofing signal without any aids in some cases. Besides, it can ensure the precision of PVT solution because the number of usable signals does not obviously decrease.

20.4 Conclusions

The cooperation of multiple anti-spoofing techniques is necessary as the insufficient of each technique. This paper proposes a cooperation method of three anti-spoofing techniques. They are multi-peak detection in acquisition, SQM in tracking, and RAIM in position solution. They locate in different steps of signal and information processing steps of receiver and their capabilities of spoofing detection and mitigation are complementary. The cooperation method does not impose extensive hardware modifications to the receiver, it's a feasible and effective way to detect and mitigate more than one spoofing signal. Simulations demonstrate the validity of this method. Nevertheless, there are some problems. As the acquisition and tracking strategy needs more tracking channels, multipath effects and thermal noise may increase the false-alarm probability of SQM, repeat RAIM increases the processing complexity, it's necessary to optimize the architecture and improve the efficiency. Further studies could focus on them.

References

1. Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G (2012) GPS vulnerability to spoofing threats and a review of antispoofing techniques. *Int J Navig Obs*, Vol 2012 Article ID 127072, 16 p
2. Kaplan ED, Hegarty CJ (2006) *Understanding GPS-principles and applications*, 2nd edn. Artech House, Boston

3. Brown R (1992) A baseline RAIM scheme and a note on the equivalence of three RAIM methods. In: Proceedings of ION NTM 1992, San Diego, CA, USA, pp 127–137, Jan 1992
4. Hewitson S, Wang J (2010) Extended receiver autonomous integrity monitoring (eRAIM) for GNSS/INS integration. *J Surv Eng* 136(1):13–22
5. Phelts RE (2001) Multicorrelator techniques for robust mitigation of threats to GPS signal quality. Ph.D. thesis, Stanford University, Palo Alto, Calif, USA
6. Hwang P, Brown R (2005) NIORAIM integrity monitoring performance in simultaneous two-fault satellite scenarios. In: Proceedings of ION GNSS 2005, Long Beach, CA, USA, pp 1760–1771, Sept 2005
7. Lee Y, Braff R, Fernow J et al (2005) GPS and Galileo with RAIM or WAAS for vertically guided approaches. In: Proceedings of ION GNSS 2005, Long Beach, CA, USA, pp 1801–1825, Sept 2005
8. Guo J, Lu M, Cui X, Feng Z (2011) A new RAIM algorithm for triple-frequency GNSS receivers. In: Proceedings of ION ITM 2011, San Diego, CA, USA, Jan 2011
9. Liu JX, Lu MQ, Cui XW et al (2007) Theoretical analysis of RAIM in the occurrence of simultaneous two-satellite faults. *IEE Proc Radar Sonar Navig* 1(2):92–97