GNSS Receiver Anti-spoofing Techniques: A Review and Future Prospects

Ling Xiao, Peng-Cheng Ma, Xiao-Mei Tang and Guang-Fu Sun

Abstract Spoofing interference can mislead a target receiver to report a wrong position and time. This can pose a serious threat to the security of global navigation satellite system (GNSS) applications, and may cause undesirable consequences. As such, anti-spoofing techniques have become a hot research topic within the GNSS discipline. This paper provides a review of recent research in the field of GNSS anti-spoofing on the receiver side. The vulnerability of GNSS receivers to spoofing attacks is studied, and the anti-spoofing algorithms around the base band digital signal processing layer and the information processing layer of the receiver is discussed. The limitation, cost and applicability of these anti-spoofing methods are investigated and the trend of anti-spoofing research in the future is analyzed.

Keywords GNSS receiver · Spoofing interference · Anti-Spoofing technique

1 Introduction

With the development of GNSS, the position, navigation and time (PNT) services, provided by GNSS, have a large influence in our daily life. Nowadays, various applications such as aircraft navigation and landing systems, electrical power distribution grids, digital communication networks, stock exchange transactions,

L. Xiao (✉) · P.-C. Ma · X.-M. Tang · G.-F. Sun
Satellite Navigation R&D Center, School of Electronic Science and Engineering,
National University of Defense Technology, Changsha 410073, China
e-mail: xiaoling_nudt@163.com

P.-C. Ma
e-mail: mapengcheng1001@163.com

X.-M. Tang
e-mail: txm_nudt@hotmail.com

G.-F. Sun
e-mail: sunguangfu_nnc@163.com

A. Hussain (ed.), *Electronics, Communications and Networks V*,
Lecture Notes in Electrical Engineering 382, DOI 10.1007/978-981-10-0740-8_8

police and rescue services and many more are relying on GNSS signals. With the increased use of GNSS, the security of these services is becoming more and more important. However, as the signals become extremely weak when they reach the earth, they are vulnerable to interference. In addition, because the working frequency band, the modulation type, the civilian pseudo-random noise (PRN) codes and data information are public, GNSS signals can be easily faked.

These counterfeit signals are termed spoofing interference. Among all the types of interference, spoofing is most harmful, because it can fool the target receiver into reporting wrong position or time results without perception, which may lead to serious consequences, for example, leading an unmanned aerial vehicle (UAV) off course [1], blocking digital communication networks [2], creating power grid equipment failure [3] and so on.

Therefore, there are many anti-spoofing techniques that have been proposed in recent years. This paper first investigates the vulnerability of GNSS receivers to spoofing attacks around the signal processing and information processing layers. Then, a brief summary of current anti-spoofing techniques in the above two layers will be provided. Finally, the trend of future research within this topic will be analyzed.

This paper is organized as follows: GNSS vulnerability against spoofing attacks is studied in Sect. 2. Anti-spoofing techniques will be discussed in Sect. 3. In Sect. 4, the study trends of anti-spoofing methods will be analyzed. Finally, the conclusion is drawn in Sect. 5.

2 GNSS Vulnerability Against Spoofing Attacks

As shown in Fig. 1, a GNSS receiver mainly has three functional modules: the radio frequency (RF) front end module, the base band signal processing module and the navigation generating module, which is also termed the information processing

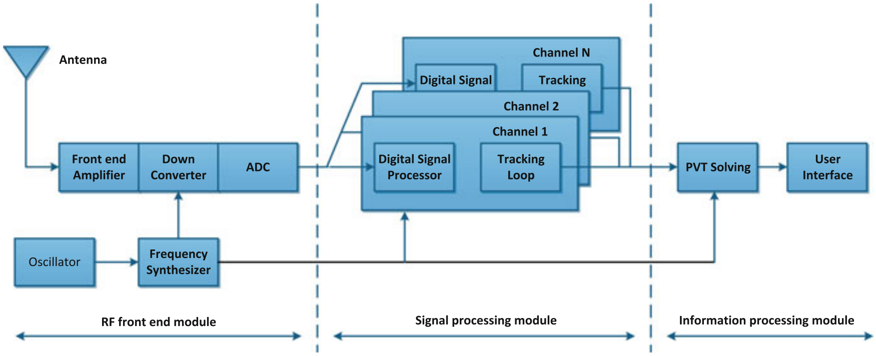

Fig. 1 The three function modules of a classical GNSS receiver

module. The tasks of the RF front end module are signal amplifying, frequency down-conversion and signal filtering; the incident signal almost hasn't been changed in this module. Thus, this module is vulnerable to all kinds of interferences that fall in its processing band. Spoofing signals are aimed to attack the last two modules and control the receiver to report false position or time. We will investigate the receiver vulnerability to spoofing at the two modules in the following.

2.1 GNSS Receiver Vulnerability in Signal Processing Module

The main tasks of the signal processing module are signal acquiring and tracking. In the signal acquiring phase, the spoofer can transmit counterfeit signals that are much more powerful than authentic ones (as shown in Fig. 2), which can cause the receiver to acquire the counterfeit signal. In the signal tracking phase, a more covert spoofing attack can take place, which transmits a counterfeit signal that slowly approaches the authentic one, and then drags the tracking loop away (as shown in Fig. 3). Once the receiver is working on the fake signals, the receiver is controlled by the spoofer.

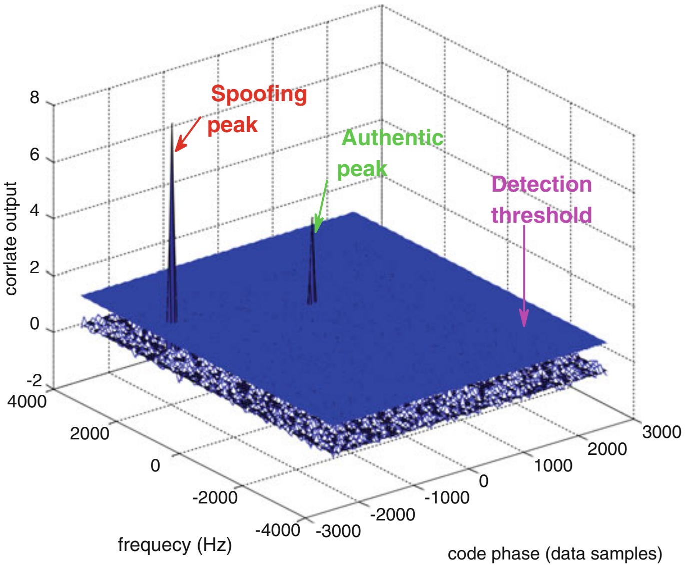

Fig. 2 The scenario of spoofing attack during signal acquiring phase

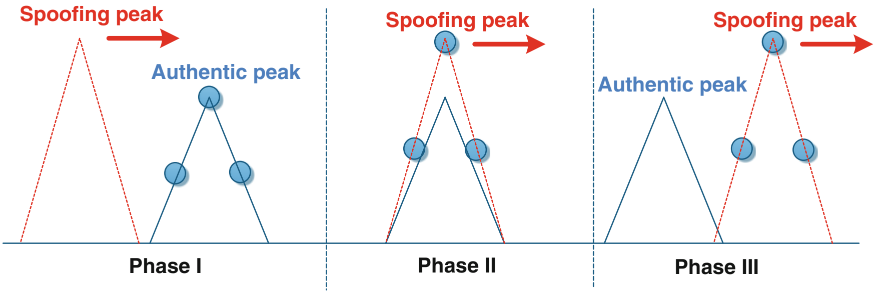

Fig. 3 The scenario of a spoofing attack during the signal tracking phase (the *three dots* denote signal tracking points)

2.2 GNSS Receiver Vulnerability in Information Processing Module

In the information processing module, the information is extracted from the data messages, and the PNT are solved using the measurement quantities provided by the signal processing module. As the framing structure of the data message is publicly known and the information does not change rapidly during some time intervals, the data message can be easily faked, which makes the receiver trust the faked message casually. During the PVT (Position, Velocity and Time) solving phase, the receiver autonomous integrity monitoring (RAIM) procedure can detect abnormal events based on range residuals. However, when the receiver is fully controlled, the range residuals are too small to trig alarms. Also, a well-designed spoofer can change the PVT results gradually and make the receiver not notice the danger.

3 GNSS Receiver Anti-spoofing Techniques

Anti-spoofing techniques can be classified into two major categories: the GNSS side and the receiver side. The GNSS side anti-spoofing techniques always need modifications of the GNSS structure, which can't be implemented promptly. This paper will discuss receiver side anti-spoofing techniques. In the following, anti-spoofing methods that take place in the signal processing module and information processing module are discussed respectively.

3.1 Anti-spoofing Methods in the Signal Processing Layer

In-band Power Monitoring The existence of spoofing signals will increase the in-band power, which will change the receiver's auto gain control (AGC) level. The spoofing interference can be alarmed by monitoring the abnormal variance of the AGC gain level [4]. This method needs the information of AGC gain, so when the receiver only deals with digital intermediate frequency signals, the method can't be implemented. To make up for this limitation, Jafarnia-Jahromi et al. [5] have proposed a pre-despreading authenticity verification method. The delay and multiply (DAM) property of Gold codes is used in this method to generate a new Gold code that carries all the incident signals' power. Then, the in-band power component is filtered by a comb filter. The filter output is used to detect spoofing interference. This algorithm can sense the spoofing signal effectively, but it can't discriminate between spoofing interference and spectrum matched interference.

CNR (Carrier Noise Ratio) Monitoring Most GNSS receivers employ CNR measurements as a parameter that characterizes the received signal quality. Under normal conditions, the received signal power changes smoothly with the satellite movement and surroundings change. However, when a higher power spoofing signal controls the receiver tracking loop, the received CNR may experience a sudden change that can indicate the presence of spoofing interference [6, 7]. Wen et al. [8] shows that when the distance between the spoofer antenna and the receiver changes from 8 to 100 m, the received CNR reduces by 22 dB. Thus for a moving receiver, if its CNR measurements change considerably, there may be spoofing interference.

Multi-antenna Methods Montgomery et al. [9] have proposed a spoofing detection technique that compares the calculated phase difference of two fixed GNSS antennas to the theoretical one. This technique requires a calibrated antenna array, and it takes about one hour to do the detection. Borio [10] designed a double antenna receiver and developed a phase only analysis of variance (PANOVA) method in order to detect the phase difference coherency of spoofed PRN signals. This method can effectively recognize spoofing signals when the SNR (signal noise ratio) is larger than 10 dB, otherwise the detection performance is poor. Psiaki et al. [11] have proposed a method using a dual-antenna differential carrier phase. This method detects spoofing based on the fact that the quantities of authentic signals' carrier-phase single-differences are multiplicity, while the spoofing ones are identical.

Synthetic Array Methods Nielsen et al. [12] has proposed a spoofing detection algorithm that employs the synthetic antenna array technique. This algorithm detects spoofing signals by computing the correlation coefficient of the channel gain. The satellite signals arrive by passing different transmitting channels, so the channel gains are uncorrelated. However, as all the spoofing signals pass through the same channel, the channel gains for these signals are identical. This method works effectively even in multipath environments because all the spoofing signals experience the same fading path. The drawback is that it is only applicable to moving receivers.

Signal Quality Monitoring (SQM) Methods SQM techniques are widely used to monitor GNSS correlation peak quality in multipath fading environments. The signal in the process of a spoofing attack on a receiver tracking loop is similar to the multipath component. Thus, the SQM techniques have been extended to detect spoofing attacks [13–15]. The ratio and delta SQM tests are employed to detect any abnormal asymmetry or flatness of GNSS correlation peaks. These techniques can only be used in line-of-sight propagation environments to detect spoof interference. In multipath environments, SQM methods might not be able to distinguish the spoofing signals or multipath reflections.

Code and Phase Rates Consistency Check For authentic signals, the Doppler frequency and the code rate are consistent, as they are both affected by the relative movement between GNSS satellite and the receiver. The relationship of these parameters is $f^a = -f_{RF}\dot{\tau}^a$, where f^a and $\dot{\tau}^a$ denote the Doppler frequency and code rate respectively, and f_{RF} is the radio frequency of the GNSS signal. Thus, this relationship can be used to detect spoofing [8]. This method is simple to implement. However, the spoofer can keep this relationship easily.

3.2 Anti-spoofing Methods in the Information Processing Layer

Received Navigation Data Check

Ephemeris Consistency Check. The ephemeris information, including eccentricity, orbital inclination, rate of right ascen and so on, will not change for about 2 h. Thus, we can compare the current received ephemeris with the save ones. If there are many differences, there may be a spoofing attack.

Satellites Clock Consistency Check. The data messages of every signal contain all the satellite's clock information. The information coming from different signals should be the same. Any abnormality may indicate a spoofing attack.

PNT Solution Check

Receiver Clock Variance Check. In normal cases, the receiver clock bias changes smoothly, which depends on the quality of the used crystal oscillator. However, in the spoofed case, when the receiver moves with respect to the spoofer antenna, the clock bias will change rapidly [16]. This is because all the spoofing signals experience a common delay from the spoofer to the receiver. In the PVT solving process, the common delay is reflected on the clock bias.

Multi-Receiver Position Consistency Check. Literatures [17–20] all proposed a multi-receiver system that detects spoofing by checking the position reported by the receivers. If the system is spoofed, all receivers will obtain the same position result. In order to detect spoofing successfully, it requires the distance between receivers to be at least as large as twice the position solution, and all the receivers to be spoofed.

Consistency Check with other Navigation System. Before the GNSS bearing, land radio navigation systems have been widely used, such as the Roland system and tactical air navigation system. Therefore, whether or not the receiver is attacked by spoofing can be checked by comparing the GNSS solution with another navigation system's solution [21].

Consistency Check with Inertia Measurement Unit (IMU). Stand-alone inertia equipment can independently provide many high solution navigation parameters, such as position, velocity and attitude. These parameters can be used to detect spoofing by comparing with GNSS ones [22, 23].

3.3 Summary

The requirement, complexity, valid scope and performance of the above-discussed anti-spoofing methods are tabulated in Table 1.

The three performance levels are defined as: (1) alarming means that the method can't discriminate spoofing interference or other type interference; (2) detecting means that the method can recognize spoofing, but can't mitigate it; (3) suppressing means that the method can detect and mitigate spoofing.

Table 1 Summary of GNSS receiver anti-spoofing methods

Anti-spoofing methods	Required capability	Complexity	Valid scope	Performance
AGC gain monitoring	AGC output	Low	Confined	Alarming
Pre-despreading method	None	Low	Generally	Alarming
CNR monitoring	CNR measuring	Low	Generally	Alarming
Direction of arrival monitoring	Antenna array	High	Confined	Suppressing
PANOVA method	Dual antenna	High	Confined	Detecting
Synthetic array method	Receiver moving	Low	Confined	Suppressing
SQM method	None	Low	Generally	Detecting
Code and phase consistency check	None	Low	Generally	Detecting
Received ephemeris consistency check	None	Low	Generally	Alarming
Satellites clock consistency check	None	Low	Generally	Alarming
Receiver clock variance check	None	Low	Generally	Alarming
Multi-receiver position consistency check	Multi-receiver	Medium	Confined	Detecting
Consistency check with other navigation system	Multi-navigation system processing ability	High	Confined	Detecting
Consistency check with IMU	IMU equipment	High	Confined	Detecting

4 Prospect of Future Research

According to the above discussions of anti-spoofing techniques, the current research findings are mainly focusing on alarming or detecting the spoofing interference, and some findings have applicability limitations. For example, some require extra equipment, and some are only effective in special scenarios. Therefore, techniques that can be generally used, and can mitigate or eliminate the interference rather than only detecting it, are required. We think the future researches of this scope will be expanded in the following aspects:

1. That research will occur on different anti-spoofing techniques fusion strategies. A stand-alone method may have limitations, while methods combining together can extend the sphere of application. For example, the power monitoring method combines the SQM method and can detect not only high power spoofing but also covert spoofing attacks, and the applicability is not only confined to line-of-sight scenarios. Thus, how to fuse anti-spoofing methods will be a trend to be researched.
2. That research will occur on multi-GNSS anti-spoofing techniques. With the development of GPS, GLONASS, Galileo and Compass, many receivers have the ability to deal with multi-GNSS signals, which can help to detect spoofing signals. Spoofing interferences' detection and suppression can be realized by comparing and checking the characters of multi-signals (e.g., signal power) and processing results (e.g., the state of clock errors).
3. That anti-spoofing technique research by combining exterior assistants will occur. GNSS receivers are generally used on mobile phones, cars, airplanes, and steamships, on which there are other facilities to provide location, velocity and attitude information. How to use these messages to enhance the safety of the receivers' services should be researched.
4. That research on interference source localization techniques will occur. Techniques, localizing and further destroying the interference source are the most effective methods to protect GNSS receivers. The CNR, pseudo-range and Doppler measurements from different receivers are candidates for source localization.

5 Conclusion

With the wide use of GNSS services all over the world, their security and robustness become more and more important. This paper summarizes the current anti-spoofing techniques around the signal processing layer and information processing layer. As discussed in Sect. 3, the methods, such as in-band power monitoring, CNR monitoring, PNT check and so on, that have low complexity can be used generally. However, most of these methods can't tell whether there is a threat or just a receiver failure. The multi-antenna technique can detect and mitigate spoofing threats effectively, but it needs extra equipment and space. In conclusion, low-cost and universal applicable GNSS receiver anti-spoofing techniques will be a research point.

References

1. UAVs Vulnerable to Civil GPS Spoofing. http://gpsworld.com
2. Recommended Minimum Performance Standards for CDMA 2000 Spread Spectrum Base Stations. C.S0010-C. Technical report, 3rd Generation Partnership Project 2 "3GPP2". http://www.docin.com/p-560878501.html
3. Zhang, Z.H., Gong, S.P., Dimitrovski, A.D., Li, H.S.: Time synchronization attack in smart grid: impact and analysis. IEEE Trans. Smart Grid. **4**(1), 87–98 (2013)
4. Akos, D.M.: Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). J. Navig. **59**(4), 281–290 (2012)
5. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G.: Pre-despreading authenticity verification for GPS L1 C/A signals. J. Inst. Navig. **61**(1), 1–11 (2014)
6. Dehghanian, V., Nielsen, J., Lachapelle, G.: GNSS spoofing detection based on receiver C/N0 estimates. In: Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation, pp. 2878–2884. The Institute of Navigation, Manassas, USA (2012)
7. Nielsen, J., Dehghanian, V., Lachapelle, G.: Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements. Int. J. Navig. Obs. **2012**, 1–9 (2012)
8. Wen, H., Huang, P.Y., Dyer, J., Archinal, A., Fagan, J.: Countermeasures for GPS signal spoofing. In: Proceedings of the 18th International Technical Meeting of The Satellite Division of the Institute of Navigation, pp. 1285–1290. The Institute of Navigation, Manassas, USA (2005)
9. Montgomery, P.Y., Humphreys, T.E., Ledvina, B.M.: Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In: Proceedings of ION International Technical Meeting, pp. 124–130. The Institute of Navigation, Manassas, USA (2009)
10. Borio, D.: PANOVA tests and their application to GNSS spoofing detection. IEEE Trans. Aerosp. Electron. Syst. **49**(1), 381–394 (2013)
11. Psiaki, M.L., O'Hanlon, B.W., Powell, S.P.: GNSS spoofing detection using two-antenna differential carrier phase. In: Proceedings ION GNSS+2014, pp. 2776–2800. The Institute of Navigation, Manassas, USA (2014)
12. Nielsen, J., Broumandan, A., Lachapelle, G.: GNSS spoofing detection for single antenna handheld receivers. Navigation **58**(4), 335–344 (2011)
13. Cavaleri, A., Motella, B., Pini, M., Fantino, M.: Detection of spoofed GPS signals at code and carrier tracking level. In: Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC '10), pp. 1–6. IEEE, Piscataway (2010)
14. Cavaleri, A., Pini, M., Presti, L.L., Fantino, M.: Signal quality monitoring applied to spoofing detection. In: Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation, pp. 1888–1896. The Institute of Navigation, Manassas (2011)
15. Kuusniemi, H., Bhuiyan, M.Z.H., Kröger, T.: Signal quality indicators and reliability testing for spoof-resistant GNSS receivers. Eur. J. Navig. **11**(2), 12–19 (2013)

16. Jafarnia, A., Daneshmand, S., Broumandan, A., Nielsen, J., Lachapelle, G.: PVT solution authentication based on monitoring the clock state for a moving GNSS receiver. http://plan.geomatics.ucalgary.ca/papers/pvt_authentication_enc2013_alij_27apr2013.pdf
17. Swaszek, P.F., Hartnett, R.J., Kempe, M.V., Johnson, G.W.: Analysis of a simple, multi-receiver GPS spoof detector. In: Proceedings of the 2013 International Technical Meeting of The Institute of Navigation. pp. 884–892. The Institute of Navigation, Manassas (2013)
18. Swaszek, P.F., Hartnett, R.J.: Spoof detection using multiple COTS eceivers in safety critical applications. In: Proceedings of the ION GNSS + 2013, pp. 2921–2930. The Institute of Navigation, Manassas (2013)
19. Swaszek, P.F., Hartnett, R.J.: A multiple COTS receiver GNSS spoof detector—extensions. In: Proceedings of the 2014 International Technical Meeting of The Institute of Navigation, pp. 316–326. The Institute of Navigation, Manassas (2014)
20. Heng, L., Makela, J.J., Dominguez-Garcia, A.D., Bobba, R.B., et al.: Reliable GPS-based timing for power systems: a multi-layered multi-receiver architecture. Power Energy Conf Ill (PECI) **2014**, 1–7 (2014)
21. Zhu, X.W., Wu, Y.W., Gong, H., et al.: Timing receiver toughen technique in complicated jamming environments. J. Nat. Univ. Defense Technol. 37(3), 1–10 (2015) (in Chinese)
22. Khanafseh, S., Roshan, N., Langel, S., Chan, F.C., Joerger, M., Pervan, B.: GPS spoofing detection using RAIM with INS coupling. In: Proceedings of IEEE/ION PLANS 2014, pp. 1232–1239. The Institute of Navigation, Manassas (2014)
23. Tanil, C., Khanafseh, S., Pervan, B.: Impact of wind gusts on detectability of GPS spoofing attacks using RAIM with INS coupling. In: Proceedings of the ION 2015 Pacific PNT Meeting, pp. 674–686. The Institute of Navigation, Manassas (2015)