# Method of GNSS Security Augmentation Based on LEO Satellite

Tao Yan(✉), Ying Wang, Xiao Liu, Lang Bian, and Yansong Meng

China Academy of Space Technology (Xi'an), Xi'an 710000, China
iamyantao@126.com

**Abstract.** In order to improve the service performance of the global navigation satellite system (GNSS), a variety of augmentation systems have been developed, including satellite-based and ground-based augmentation methods. The purpose of augmentation systems usually includes integrity augmentation, accuracy augmentation and availability augmentation. With the emerging user fields, especially those related to life safety or economic debt, more dependence on GNSS, leads to a high demand for the robustness and security of GNSS civil signals. The received power of GNSS signal on ground is weak and the civil signal structure is open, which is easy to become the target of jamming and spoofing. Therefore, it has become a trend to enhance the security of GNSS civil signals. At present, there are two ways to enhance the security. One is to introduce security authentication features into civil signals, including navigation message authentication and spread spectrum code authentication. This method has little effect on non-authenticated users, but the security authentication is not real time. The other method is based on the location authentication of LEO satellite multi spot-beam features represented by iridium next satellite. The method has high real-time performance, but the accuracy is limited by the beam pattern. In this paper, a GNSS security augmentation method based on LEO satellite is proposed. Using the credible ranging signal broadcasted by LEO satellite, the positioning result of GNSS civil signal is authenticated to achieve security augmentation. This proposed method has the advantages of high real-time performance and high precision. Theoretical analysis shows the effectiveness and feasibility of this method.

**Keywords:** Security augmentation · LEO satellite · Signal authentication · GNSS signals

## 1 Introduction

In order to improve the service performance of the satellite navigation system, a variety of navigation augmentation methods have been developed to enhance the integrity, accuracy and availability of satellite navigation. In recent years, GPS and other GNSS technologies have been widely used in mobile positioning services, road transportation, aviation, shipping, timing service, geodesy, atmospheric sensing and other fields, and the vulnerability of GNSS civil signals has attracted widespread attention. Most of these emerging applications are related with security or responsibility, that is, the location or speed information of users can be used to implement life safety related or

J. Sun et al. (Eds.): CSNC 2020, LNEE 651, pp. 634–642, 2020.
https://doi.org/10.1007/978-981-15-3711-0_56

legal/economic decisions. Therefore, enhancing the security of GNSS is becoming an important requirement for these users [1].

GNSS civil signals are extremely vulnerable. On the one hand, the received power of GNSS signal is very low, usually only about −158 dBW, which makes it easy to be interfered and spoofed by the enemy; on the other hand, all GNSS civil signal interface specifications are open, and the receiver can receive any input conforming to the specifications and treat it as the real signal from GNSS satellite, which leads to spoof the GNSS receiver very easy. Therefore, for the security of GNSS civil signals, the threat of spoofing signal is more serious [2]. In recent years, there have been many GPS interference events [3, 4].

In order to enhance the security of GNSS, one direction way is to enhance the robustness of GNSS itself and improve the anti-spoofing ability of civil signals. The common method is to modify the GNSS civil signal structure, on the premise of maintaining backward compatibility with the current signal, to provide the authentication ability of the navigation signal. At present, Galileo, GPS and QZSS teams have studied the civil anti-spoofing signal structure, and Galileo plans to provide navigation message (NMA) authentication function on its E1 OS signal. The United States researches on adopting chimera authentication scheme on GPS L1C signal [5–8]. Another direction is to develop auxiliary technologies or backup systems. Iridium next proposes a scheme based on LEO multi spot beam overlapping pattern anti-spoofing to enhance the security of positioning and timing [9].

All of the above methods can effectively enhance the security of satellite navigation. However, in order to ensure the security, the method of introducing the security authentication feature into GNSS civil signals usually delays the key transmission, resulting in the delay of security authentication. The method based on the multi spot beam feature of LEO satellite has high real-time performance, but the accuracy is limited by the beam pattern. Aiming at the problem of enhancing the security of GNSS, this paper proposes a GNSS security augmentation method based on LEO satellite, which uses the bi-directional authentication ability of LEO satellite to receive the trusted ranging signal broadcasted by LEO satellite, and authenticates the positioning result of GNSS civil signal to realize the security augmentation. This method has the advantages of high real-time and high precision.

This paper is organized as follows. In Sect. 2, the GNSS civil signal authentication method is analyzed. In Sect. 3, the anti-spoofing scheme of Iridium next based on LEO multi spot beam overlapping pattern is introduced. In Sect. 4, a method of enhancing the security of GNSS based on LEO is proposed. In Sect. 5, the performance of the proposed method in this paper is analyzed. Finally, the summary is made in Sect. 6.

## 2 GNSS Civil Signal Authentication Methods

GNSS signal authentication methods include NMA and SCA, which can be used in combination.

## 2.1 Navigation Message Authentication (NMA)

NMA is carried out at the information level, using the digital signature authentication scheme, selecting the bits in the navigation message that change with time to generate message authentication code (MAC) [7], or referred to as reference authentication navigation data (RAND) [6], and RAND usually uses the bits in the message that change with time. An example of RAND is as following. RAND includes ROW data (17 bits), TOC data (16 bits), AF1 data (16 bits), AF0 data (22 bits), and PRN ID (8 bits). TOW and PRN ID data are necessary, because the receiver needs time reference and satellite ID to obtain authentication key.

At the satellite end, the RAND message is first hashed to generate hash message (A), then encrypted with a private key to generate a digital signature data, which is broadcasted simultaneously with the navigation message. At the receiver end, the receiver receives the message and the digital signature data. Through public key decryption, hash message (A) is obtained. The receiver also receives the navigation message data, and can generate the RAND data, and then get a hash message (B) according to the same hash algorithm. Theoretically, the generated hash message (B) is the same as the received hash message (A) through decryption; otherwise the navigation data bits of the signal are modified. That is, if the signal is not modified, "hash message A" and "hash message B" are the same, which ensures the authenticity of the message. If the two hash messages are different, the signal is not true.

In order to complete the authentication of the receiver, the key should be exploited. Therefore, the distribution and transmission of the key is a problem. Based on the hybrid symmetric/asymmetric key method, Galileo OS NMA adopts the TESLA (timed efficient streamed loss tolerant authentication) scheme [10] to delay the key dissemination to users. These keys form a one-way key chain, which can verify the effectiveness of the key.

NMA is only the authentication at the message level, which can only ensure that the received message is traceable the real source. Therefore, for the regenerative forwarding spoofing attacking, the received message will be demodulated and broadcasted, and the receiver cannot find out the spoofing attacking. Therefore, the authentication at the measurement level is required.

## 2.2 Spreading Code Authentication (SCA)

For SCA scheme, the unpredictable long period spreading code sequence is inserted into the open spreading code to realize the authentication at the measurement level. According to the different ways of introducing security code, there are several methods as follows.

For scheme one, the spread spectrum security codes (SSSC) at a certain frequency are inserted into the open PRN code period [7]. The SSSC is unpredictable. In the digital signature broadcasted later, it contains the seed value of SSSC. After the receiver authenticates the navigation message, it gets the seed value, generates the SSSC, correlates with the signal sampling value, and realizes the spreading code authentication.

For scheme two, the navigation signal is divided into data channel and pilot channel. The spreading code of data channel is open, and the code of pilot channel is the module 2 sum of open code and secret code. The message of data channel contains the digital signature of the information needed to generate the secret code.

Scheme three is different from the previous two schemes. In this scheme, only a part of chip in one code period is encrypted. The encrypted information broadcasted in the message contains the position and value of the marked sequence. Chimera authentication scheme for GPS L1C signal adopts the scheme [8]. In this scheme, the use of non-authenticated users is not affected.

Both the NMA and SCA authentication methods involve the dissemination of the key. In order to prevent the key from being obtained in advance by the spoofer, and then generate the spoofing signal, they generally delay the dissemination of the key. Therefore, there is a delay of several seconds in the signal authentication.

## 3 Anti-spoofing Method Based on LEO Satellite Multi Spot Beam Overlapping Pattern

LEO satellite adopts multi spot beam scheme, which provides a scheme of anti-spoofing based on multi spot beam overlapping pattern. The complex multi spot beam overlapping pattern combines with the characteristics of communication burst signal to form a unique mechanism, which provides location-based authentication and is extremely difficult to be spoofed. In addition, the Doppler signature generated by LEO satellite motion is also significantly stronger than GPS, making it more difficult to be spoofed.

Iridium next satellite broadcasts the STL signal. It can provide effective anti-spoofing ability by using multi spot beam overlapping pattern. The phased array antenna of each satellite of Iridium satellite forms 48 spot beams, covering a circular area with a diameter of 4700 km, and each beam radius is about 350 km. The core of the anti-spoofing mechanism based on spot beam overlapping pattern is to estimate the position of the receiver by using the overlapped spot beam [11]. At a given time, the user receiver is located in multiple overlapping spot beams, which are from a single satellite or multiple satellites. The position of the user receiver can be estimated as the centroid of the spot beam center at the multiple overlapping points, or the center of the overlapping area. Moreover, the estimation error can be further reduced by averaging two or more position estimation. Obviously, the more spot beams the satellite transmits in each unit area, the more accurate the position estimation of the user's receiver will be.

If at any time, the position and attitude of the satellite relative to the earth are known, the direction of the transmitting antenna beam relative to the satellite is known, and the feature of the antenna beam is known, then at time $t_0$, the projection pattern of the spot beam on the ground can be calculated. The center position of the point beam can be sent to the user's receiver via satellite or acquired through the ground network.

By using the uniquely identified spot beam information, when the user receiver detects at least one spot beam, it can identify which satellite's spot beam the user receiver is located in. Once the spot beam of the user receiver is determined, the user receiver can determine its position in the spot beam projection. Therefore, when the error introduced by GNSS spoofing signal is larger than the range of the spot beam estimation, the spoofing attack can be identified.

The anti-spoofing mechanism based on spot beam overlapping can be divided into single satellite multi spot beam overlapping scheme and multi satellite multi spot beam overlapping scheme. The schematic diagram of single satellite multi spot beam overlapping scheme is shown in Fig. 1. The receiver receives the signal of a satellite and is located in at least one point beam area. The receiver obtains the satellite's orbit, attitude or spot beam pattern and direction information from the message. By using the orbit model data and orbit correction data, the center position of the spot beam is calculated. When the receiver is located in multiple beam overlapping areas, the position estimation area is further reduced, as shown in Fig. 1.

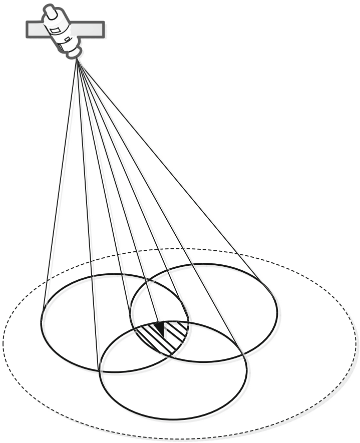

**Fig. 1.** The overlapping of multiple spot beams

In order to further improve the accuracy of position estimation, the information of multi spot beam pattern changing with time can be used. At time $t_0$, the receiver is located in the multiple spot beam overlapping area of the satellite. After time $\Delta t$, the spot beam overlapping area moves, and the receiver is located in the overlapping area of the two spot beam overlapping areas. If multiple satellites can be seen at the same time, the position estimation accuracy is higher by using multi satellite multi spot beam overlapping pattern.

Based on the anti-spoofing method of LEO multi spot beam overlapping pattern, the real-time position estimation can be carried out. However, limited by the coverage of spot beam (about 500 km), the estimation accuracy of spot beam overlapping area is in the order of tens of kilometers. Through long time estimation, the accuracy can be further improved.

## 4 GNSS Security Augmentation Based on LEO Satellite Ranging Signal

The security of GNSS civil signal is low and is easy to be spoofed. The user receives the GNSS civil signal, but it is difficult to verify its real source.

For the security augmentation method based on the ranging signal of LEO satellite, the LEO satellite, especially the LEO mobile communication satellite, has two-way link signal, the terminal and the LEO communication satellite can use the two-way connection and the key for two-way authentication, to determine the authenticity of each other. At the same time, LEO satellite broadcasts the ranging signal, which provides a reliable ranging signal source.

Taking the LEO communication satellite as an example, the specific implementation scheme is as shown in Fig. 2: the GNSS receiver uses the received GNSS civil signal to get a positioning result $\mathbf{P_G}$; through the two-way link signal, carries out two-way authentication to determine the authenticity of LEO satellite signal, receives the trusted ranging signal broadcasted by the LEO satellite, and obtains the trusted clock data and ranging value $\rho$ between the terminal and the satellite. LEO satellite ephemeris is also obtained from the signal, and the position $\mathbf{P_L}$ of LEO satellite can be calculated. The distance $\tilde{\rho}$ between the terminal to be certified and LEO satellite is calculated by using the GNSS positioning result $\mathbf{P_G}$ and the trusted LEO satellite position $\mathbf{P_L}$. If the difference between the distance $\tilde{\rho}$ and the ranging value $\rho$ exceeds the threshold value, the existence of spoofing signal can be decided.

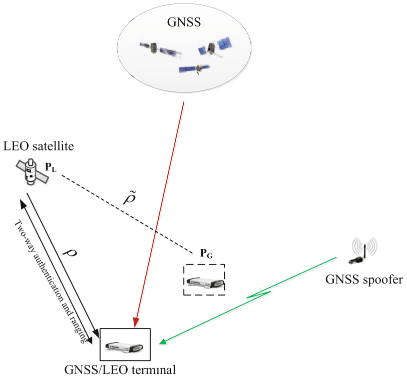

**Fig. 2.** GNSS security augmentation method based on LEO satellite

## 5 Performance Analysis

The parameters are as follows: $R = 6378$ km is the radius of the earth, $h$ is the orbit height of the LEO satellite, $r$ is the real distance from the terminal to LEO satellite, $\Delta r$ is the maximum measurement error between the pseudo range measurement value $\rho$ and the true range $r$, and $\theta$ is the real elevation angle from the user to the LEO satellite.

Figure 3 shows the schematic diagram of the analysis conditions. In the figure, S represents the position of LEO satellite, O represents the geocenter, S′ represents the subsatellite point, P represents the real position of the terminal, $\mathrm{P_1}$ and $\mathrm{P_2}$ represent the farthest position of the terminal under the measured pseudo range error $\Delta r$, and the terminal is on the ground.

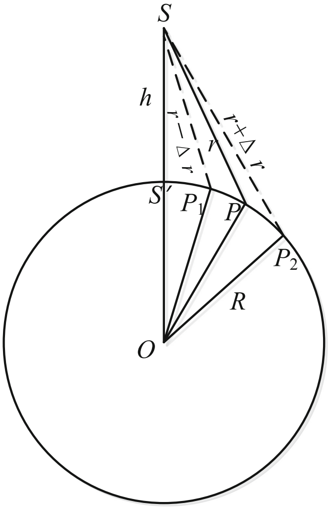

**Fig. 3.** Geometrical relationship between LEO and terminal

According to the trigonometric formula, we have

$$r = \sqrt{(R\cdot\,\sin(\theta))^2 + (h^2 + 2Rh)} - R\cdot\,\sin(\theta) \tag{1.1}$$

When $r - \Delta r \geq h$, we have

$$\begin{aligned} \angle SOP_1 &= \arccos\left(\frac{(h+R)^2 + R^2 - (r-\Delta r)^2}{2R(h+R)}\right) \\ \angle SOP &= \arccos\left(\frac{(h+R)^2 + R^2 - r^2}{2R(h+R)}\right) \\ \angle SOP_2 &= \arccos\left(\frac{(h+R)^2 + R^2 - (r+\Delta r)^2}{2R(h+R)}\right) \end{aligned} \tag{1.2}$$

The distances from P, $P_1$ and $P_2$ to the subsatellite point are as follows:

$$\begin{aligned} \widehat{S'P_1} &= R\cdot\arccos\left(\frac{(h+R)^2 + R^2 - (r-\Delta r)^2}{2R(h+R)}\right) \\ \widehat{S'P} &= R\cdot\arccos\left(\frac{(h+R)^2 + R^2 - r^2}{2R(h+R)}\right) \\ \widehat{S'P_2} &= R\cdot\arccos\left(\frac{(h+R)^2 + R^2 - (r+\Delta r)^2}{2R(h+R)}\right) \end{aligned} \tag{1.3}$$

When $r - \Delta r < h$, $\widehat{SP_1}=0$.

As long as the position error of GNSS caused by spoofing signal is greater than $\Delta P = \max\left\{\widehat{PP_1}, \widehat{P_2P}\right\}$, it can be detected and the security can be enhanced.

When LEO orbit height $h$ = 1100 km and pseudo distance measurement error $\Delta r$ is equal to 3 m and 30 m respectively, the change curve with elevation angle is shown in Fig. 4. It can be seen that when the measurement error of LEO pseudo range is 3 m, as long as the positioning error caused by spoofing signal exceeds 2.4 km, the spoofing attack can be identified. In fact, most of the spoofing attack can be identified when the error exceeds 100 m in the case that elevation of LEO satellite is lower than 85°. When the error of LEO pseudo range measurement is 30 m, as long as the positioning error caused by deception signal is more than 7.5 km, the spoofing attack can be identified. In fact, most of the spoofing attack can be identified if it is more than 360 m.

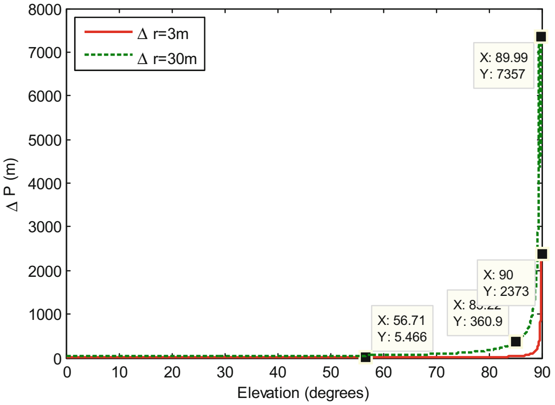

**Fig. 4.** Positioning bias induced by spoofing signal vs. elevation

Compared with the multi spot beam overlapping method, this proposed method has stronger anti-spoofing ability and better real-time performance. With the increase of the ephemeris accuracy and the number of satellites, the security augmentation ability can be further improved.

## 6 Conclusions

The vulnerability of GNSS civil signal has gradually attracted people's attention. It is a consensus to enhance the security of GNSS civil signal. The current security augmentation methods, one is to introduce security authentication features into GNSS civil signals, but there is a delay in security authentication; the other is based on the LEO satellite multi spot beam location authentication method, which has high real-time performance but limited location estimation accuracy. In this paper, the GNSS security augmentation method based on LEO satellite is proposed. By using the bi-directional authentication function of LEO satellite, the trusted ranging based on LEO ranging signal is realized, and the positioning result of GNSS civil signal is certified, and the real-time security is enhanced. Simulation and theoretical analysis show that when the error of LEO pseudo range measurement is 30 m, as long as the positioning deviation caused by GNSS spoofing signal is more than 7.5 km, and in the case that elevation of LEO satellite is lower than 85°, as long as it is more than 360 m, this method can identify spoofing attack. Improving the precision of pseudo range measurement can further improve the security and enhance the performance.

## References

1. Margaria, D., Motella, B., Anghileri, M., Floch, J.J., Fernández-Hernández, I., Paonni, M.: Signal structure-based authentication for civil GNSSs. IEEE Signal Process. Mag. **34**(5), 27–37 (2017)
2. Petovello, M.: What is navigation message authentication? InsideGNSS, January/February 2018, pp. 26–31 (2018)
3. Goff, S.: Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup. Inside GNSS, 24 July 2017 (2017). http://www.insidegnss.com/node/5555
4. Scott, L.: Spoofing Incident Report: An Illustration of Cascading Security Failure. InsideGNSS, 9 October 2017 (2017). http://www.insidegnss.com/node/5661
5. Walker, P., Rijmen, V., Fernández-Hernández, I., Bogaardt, L., Seco-Granados, G., Simón, J., Calle, D., Pozzobon, O.: Galileo open service authentication: a complete service design and provision analysis. In: ION GNSS+ 2015, Tampa, Florida, 14–18 September, 2015, pp. 3383–3396 (2015)
6. Manandhar, D., Shibasaki, R.: Signal authentication for anti-spoofing based on QZSS L1S. In: ION PNT 2017, Honolulu, Hawaii, 1–4 May 2017, pp. 938–947 (2017)
7. Scott, L.: Anti-spoofing and authenticated signal architectures for civil navigation systems. In: Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), Portland, OR, 2003 (2003)
8. Anderson, J.M., Carroll, C.K.L., DeVilbiss, N.P., Gillis, J.T., Hinks, J.C., O'Hanlon, B.W., Rushanan, J.J., Scott, L., Yazdi, R.A.: Chips-Message robust authentication (Chimera) for GPS civilian signals. In: ION GNSS+ 2017, Portland, Oregon, 25–29 September 2017, pp. 2388–2416 (2017)
9. Satelles Satellite Time and Location White Paper (2016). https://www.satellesinc.com/technology-2/resources/Satelles-White-paper-Final.pdf
10. Development, Supply and Testing of a Galileo Open Service Authentication User Terminal (OS-NMA) for the GSA. European Global Navigation Satellite Systems Agency (2016)
11. Whelan, D.A., Gutt, G.M., Brumley, R.W., Eglington, M.L., Martens, C.J., Haddad, A.T., Schmalzried, R.R.: Geolocation Leveraging Spot Beam Overlap. United States Patent, Patent No.: US 9625573 B2, 2017 (2017)