Satellite Navigation
https://satellite-navigation.springeropen.com/

COMMUNICATIONS Open Access

Advances of SBAS authentication technologies

Ying Chen[1], Weiguang Gao[2*], Xiao Chen[3,4], Ting Liu[3], Cheng Liu[1], Chengeng Su[1], Jun Lu[1], Wei Wang[1] and Shenglin Mu[3,4]

Abstract

Satellite Based Augmentation System (SBAS) provides the corrections and integrity information to users, but as its signal format is opened to the public and Global Navigation Satellite System (GNSS) spoofing technology becomes more realistic, more feasible and cheaper. It's foreseeable that there will be risks of spoofing threats against SBAS in the future. SBAS signal authentication technology provides a system-level solution to spoofing threats by adding special markers to SBAS signals so that receivers can verify whether the SBAS signals are from the on-orbit Geostationary Earth Orbit (GEO) satellites or whether the signal information has been forged and tampered with. First, this article introduces the existing anti-spoofing methods that can be applied to SBAS, especially the Elliptic Curve Digital Signature Algorithm (ECDSA) and Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocols. Then it discusses four possible solutions in a combination with the existing SBAS Interface Control Document (ICD). Two main Key Performance Indicators (KPIs), Time Between Authentication (TBA) and Authentication Latency (AL), obtained in the four main scenarios are compared. By analyzing the EGNOS Authentication Security Testbed (EAST) test simulation results of European Geostationary Navigation Overlay Service (EGNOS) in Europe, the impact of SBAS after joining the authentication service is obtained.

Keywords: SBAS, Authentication, TESLA, ECDSA

Background

Satellite Based Augmentation System (SBAS), as a wide augmentation system, broadcasts the differential corrections and integrity information to users for improving the accuracy, availability and integrity of its services in a wide range (RTCA MOPS 229). Applied in the field of safe-of-life, SBAS can meet the navigation needs of civil aviation from the en-route phase to precision approach phase of an aircraft. As SBAS Dual Frequency and Multiple Constellation (DFMC) technology has been developed (TAN, 2008), its services can play an important role in the field of high integrity demands such as aviation, navigation, and railway. In addition to being vulnerable to the natural disturbance and electromagnetic interference in complex environmental conditions, SBAS is subject to malicious spoofing attacks due to its open signal format which makes receivers capture deceptive signals in an unconscious state, leading to integrity risks. Improving the security of SBAS services becomes an important task in the SBAS technology development.

SBAS authentication technology provides a solution to this problem by adding special markers to SBAS signals (Psiaki & Humphreys, 2016) so that the receivers can verify whether the SBAS signals are from the on-orbit Geostationary Earth Orbit (GEO) satellites and whether the signal has been forged or tampered with. The technology ensures the integrity of signals/navigation messages and provides authentication services. Without affecting the usage of SBAS services, it provides users with more secure navigation messages by increasing navigation messages integrity verification and signal source identification so as to tackle spoofing attacks.

*Correspondence: gwg9821@163.com
[2] Beihang University, Beijing, China
Full list of author information is available at the end of the article

Evolution of navigation signal authentication

The basic principle of authentication is that the message sender conducts cryptographic operation on the original message to generate an "authentication symbol" and sends it to the receiver along with the original message. Then the receiver validates message integrity and authenticates identity by verifying the symbol.

The Global Positioning System (GPS) authentication was first proposed by Scott in 2003 (Scott, 2003). To reduce the software and hardware costs, it would be easier to generate GPS spoofing signals in the future. Applying a cryptographic algorithm to civil GPS navigation messages and spreading codes was proposed to protect GPS signals from spoofing attacks, and further three levels of protection measures were put forward, i.e., message authentication, public spreading code authentication, and encrypted spreading code authentication. In 2004, the potential market for Galileo Navigation Satellite System (Galileo) authentication service was outlined by Pozzobon et al., who indicated Galileo authentication would be used for open services, life safety services, and public regulatory services (Pozzobon et al., 2004). Subsequently, two methods, Elliptic Curve Digital Signature Algorithm (ECDSA) and Timed Efficient Stream Loss-Tolerant Authentication (TESLA), were proposed for navigation message authentication (Wullems et al. 2005). An authentication method based on GPS-L1C message, which mixes ECDSA and TESLA in the navigation message to authenticate users with low requirements for synchronization, was came up by a research team in the University of Texas. In 2017, Galileo provided the Galileo signal authentication service for the first time, which featured the Open Service Navigation Message Authentication (OS-NMA) message structure integrated into the Galileo I/NAV message sequence with TESLA protocol, and standardized generation and verification of Message Authentication Code (MAC) and keychain (Chiara et al. 2017).

There are two types of navigation signal authentication, i.e., Navigation Message Authentication (NMA) and Spreading Code Authentication (SCA). For NMA, a cryptographic marker is added to the navigation message, and the receiver uses the marker to authenticate the signal source. For SCA, the unpredictable chips are inserted in an unencrypted public spreading code, and then the receiver verifies the unpredictable chips in the received code sequence with a cryptographic algorithm to authenticate the identity of the signal source. SBAS provides users with integrity message and message tampering is the major threat it faces, so NMA is adopted as the signal authentication method for SBAS. The SBAS system provides users with Global Navigation Satellite System (GNSS) corrections and integrity messages. Spoofing is carried out by generating false signal that are highly similar to the real SBAS signal and tampering the message. A system-level spoofing countermeasure based on SBAS NMA has been provided against this kind of SBAS message tampering (Chiara et al. 2016, 2017).

NMA schemes for SBAS authentication

The SBAS signal authentication adopts NMA method (Fernandez-Hernandez et al., 2014). In order to protect the navigation message data, the Digital Signature (DS) or MAC is authenticated at the user terminal. There are two types of SBAS message authentication methods, i.e., DS and TESLA (Neish et al. 2018, 2019a, 2019b, 2019c).

DS is based on asymmetric cryptography. The sender uses its private key to sign the message, while the receiver uses a public key to verify the signature of the message (Yuki, 2016).

DS adopts ECDSA, which uses Elliptic Curve Cryptography (ECC) to simulate the digital signature algorithm. It has high security, but its encryption and decryption speed is low.

TESLA protocol is a broadcasting authentication protocol based on MAC designed by Perring et al. (2000). This protocol uses symmetric cryptographic mechanism to enable the broadcasting authentication of messages and achieves the asymmetry of broadcasting authentication by delaying the release of the authentication key in the one-way keychain, which prevents message forgery ensuring the security of messages.

Security level for SBAS authentication

The length of the key depends on the Security Level (SL) of the authentication service which refers to the difficulty for the password algorithm to be cracked by force. For example, the 128-bit security level means that it would take 2^{128} attempts to break. For symmetric ciphers, the security level is generally equal to the length of the key. For asymmetric ciphers, the security level is generally less than the length of the key. For example, for the ECDSA algorithm with a security level of 128-bit, the length of the private key is 256-bit, and the length of the public key is 512-bit. Considering the round expectancy of SBAS service, a security level of 128-bit is selected.

Comparison of the two KPIs from diverse schemes

Time Between Authentication (TBA) and Authentication Latency (AL), as Key Performance Indicators (KPI) of SBAS authentication, were proposedby several researchers. (Chiara et al., 2017; Enge & Walter, 2014; Fernandez-Hernandez et al., 2014; Neish et al., 2019a, 2019b):

TBA, understood as the time between authentication verification events, is a relevant design parameter which balances the robustness and performance. When authentication message is transmitted frequently, it needs significant bandwidth and potentially degrades the performance; on the other hand, when authentication message is transmitted infrequently, it forces the receiver to coast during a longer time using non-authenticated information (Figs. 1, 2).

AL, understood as the maximum time between the reception of a message and its authentication, is also a relevant parameter given that, unlike GNSS ephemerides, SBAS messages are continuously changing. AL is directly related to Time To Alert (TTA). The ideal authentication delay should not exceed 6 s, because the TTA is 6 s. AL and TBA are interrelated and their relationship depends on the scheme, as shown in Fig. 3.

Considering the channel (I/Q) and the authentication protocols (TESLA/ECDSA), four schemes were developed, as shown in Fig. 3.

Status of SBAS signal authentication

In 2016 the European Union (EU) proposed the European Geostationary Navigation Overlay Service (EGNOS) signal authentication plan (Chiara et al. 2016), then developed the EGNOS Authentication Security Testbed (EAST) (Chiara et al. 2017), preliminarily designed the authentication protocol, the authentication message broadcasting scheme and the key performance indicators, and continuously evaluated the authentication method. Alternatives for SBAS authentication include ECDSA digital signature and TESLA protocols (Chiara et al. 2017; Neish et al. 2018), in which ECDSA adopts the Elliptic Curve Schnorr (EC-Schnorr) standard.

The United States has not yet explicitly proposed the Wide Area Augmentation System (WAAS) authentication service plan, while a team from Stanford University has been actively promoting the formulation of SBAS signal authentication standard. They adopted the same alternatives as those used in Europe, including the ECDSA and TESLA protocols (Neish et al. 2019a, 2019b), in which ECDSA adopted the National Institute of Standards and Technology (NIST) standard.

Compared with Europe and the US, China is at early stage in the development of the SBAS signal authentication technology. The Civil Aviation University of China and the China Academy of Sciences Institute of

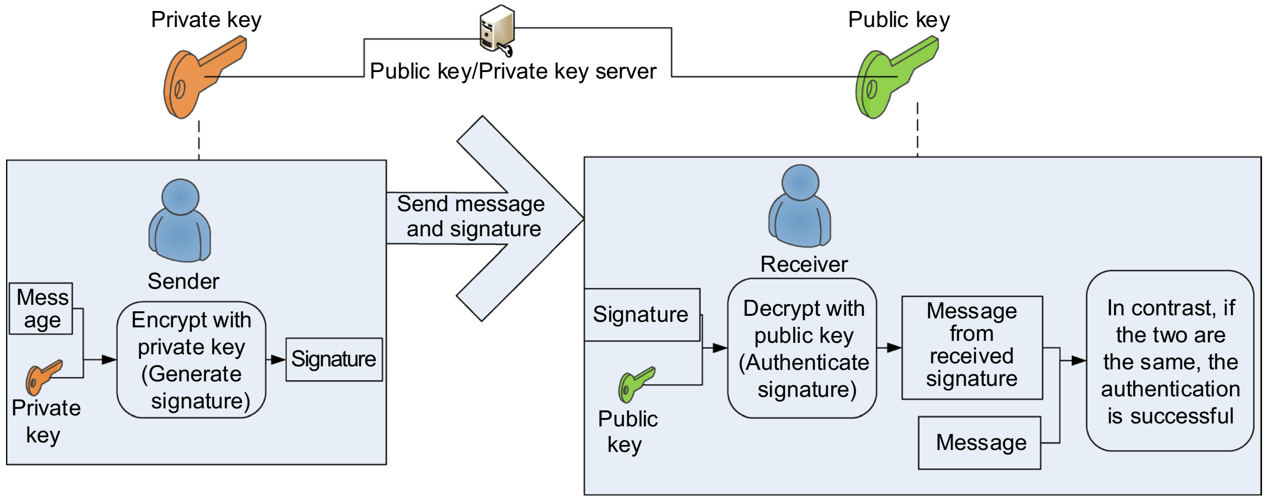
Private key
Public key/Private key server
Public key
Send message and signature
Sender
Message
Private key
Encrypt with private key (Generate signature)
Signature
Receiver
Signature
Public key
Decrypt with public key (Authenticate signature)
Message from received signature
Message
In contrast, if the two are the same, the authentication is successful

Fig. 1 Schematic diagram of authentication based on digital signature

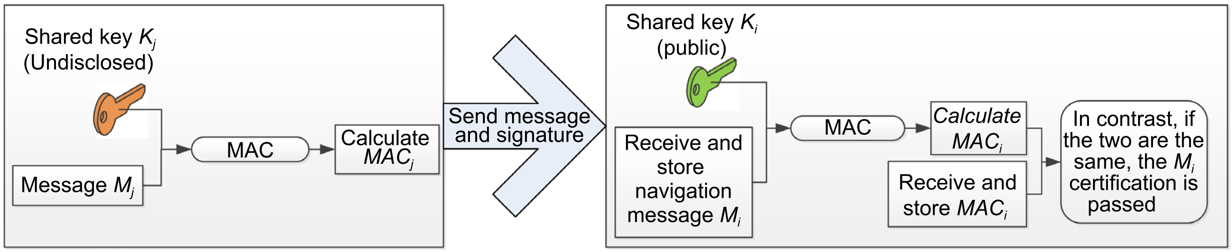
Shared key K_j (Undisclosed)
Message M_j
MAC
Calculate MAC_j
Send message and signature
Shared key K_i (public)
Receive and store navigation message M_i
MAC
Calculate MAC_i
Receive and store MAC_i
In contrast, if the two are the same, the M_i certification is passed

Fig. 2 message authentication code principle

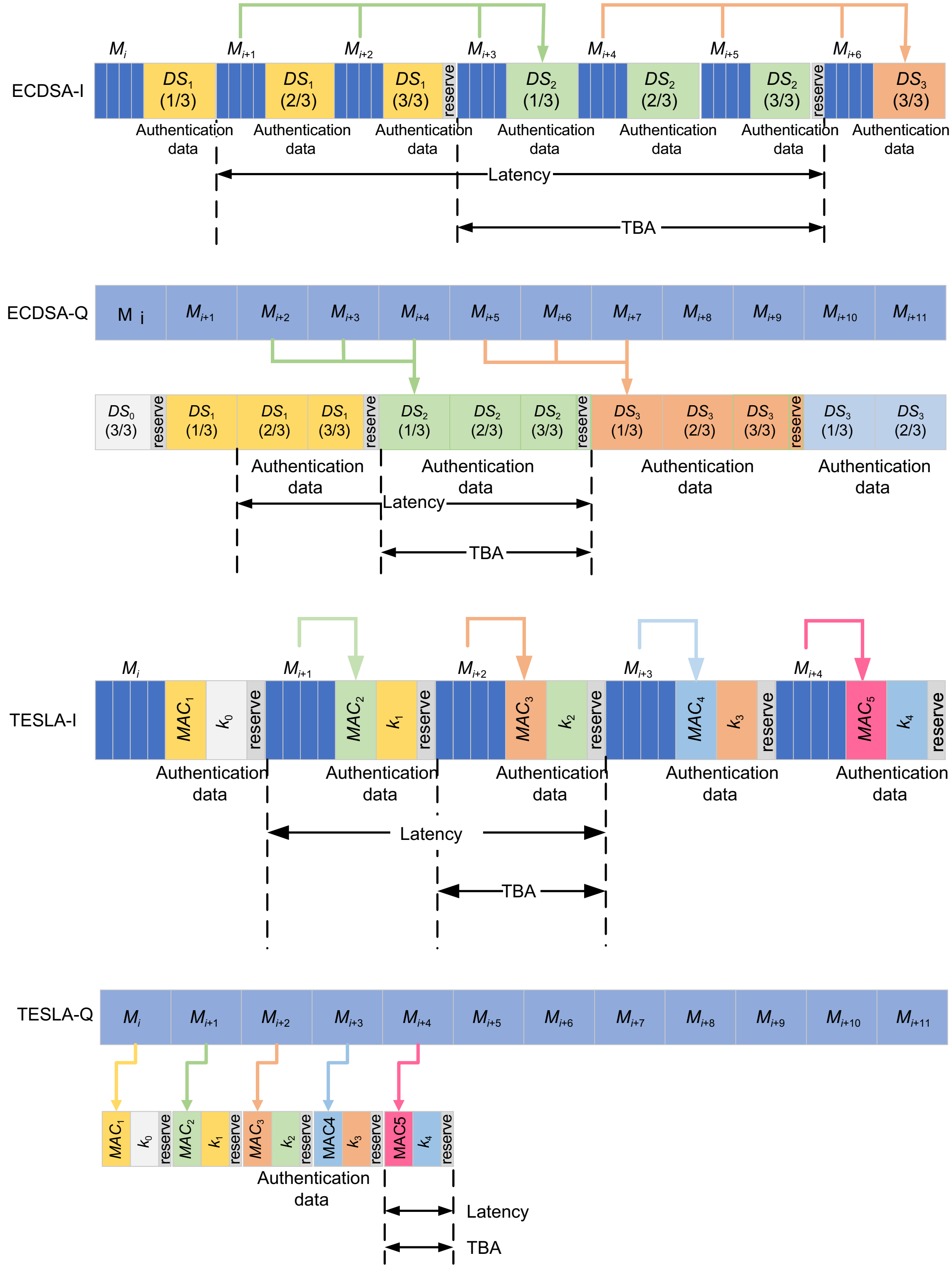

Fig. 3 Simplified scheme of the implementations of SBAS message authentication

Optoelectronics have carried out the research on NMA authentication (Liu 2015, 2018; Mu et al. 2020). The existing SBAS signal authentication protocol proposed in Europe and the United States are based on the traditional bent-pipe systems such as WAAS and EGNOS, while the Chinese BeiDou Satellite Based Augmentation System (BDSBAS) adopts on-board signal generation system, which is somewhat different from WAAS and EGNOS. In 2019, BDSBAS authentication message and simulation experiments were carried out by Mu et al. of the China Academy of Sciences. The message was designed based on China's commercial cryptography system standard SM2 (GM/T 32918-2016) and ECC algorithm (Standardization Administration, 2016a, 2016b), and the simulation verification of Over The Air Rekeying (OTAR) broadcasting process was carried out.

Simulation results and analysis

The simulation trials based on the EGNOS EAST platform were carried out by Fernandez-Hernandez et al. (Fernandez-Hernandez et al. 2014), and the results on the performances of SBAS authentication in the I/Q-channel schemes, as well as SBAS authentication were presented.

Simulation results of authentication performance in I/Q-channel schemes

According to the 128-bit security level, ECDSA authentication message (512-bit) requires three 216-bit message frames, but TESLA only needs one 216-bit message frame. At this time, the maximum TBA of TESLA is six seconds, and the maximum TBA of ECDSA is 18 s. Table 1 shows the simulation results of the SBAS message authentication schemes.

Table 1 Performance comparison of different Schemes

Schemes	C/N_0 (AER = 1%) (dB·Hz)	Avg. TBA (AER 1%) (s)	Max. TBA (s)	Max. AL (s)
L5-I ECDSA	28.5	13.52	18	20–29
L5-I TESLA	28.3	5.9	6	11
L1-I ECDSA	28.5	12.89	18	20–29
L1-I TESLA	28.3	4.89	6	11
Q ECDSA I/Q 1:1	31.3	3.03	3	4
Q TESLA I/Q 1:1	31	1.01	1	1
Q ECDSA I/Q 3:1	29.1	5.05	5	8
Q TESLA I/Q 3:1	29.3	2.02	2	4

For L1-ECDSA, a 1% Authentication Error Rate (AER) is achieved with a Carrier-to-Noise ratio (C/N_0) of 28.5 dB·Hz. In these conditions, the average TBA is 13.52 s, the authentication period is 18 s (three message frames), and the maximum AL is from 20 to 29 s. The maximum delay suggests that due to the 1% of authentication failures, three digital signature message frames may have an additional digital signature frame.

The 6s TTA required by SBAS is just satisfied in the Q channel scheme. Using I/Q power 1:1 allocation will reduce the performance. A power apportionment of 75%/25% for the I/Q channels will reduce the Q channel power by about 1 dB, but still meets the 6s TTA requirement.

The simulation results of SBAS To study the impact of SBAS authentication on the original SBAS service, the simulation trials were implemented by Fernandez-Hernandez et al. (2014, 2018). The simulations with L1 and L1/L5 scenarios, were conducted in European air service area (Fernández-Hernández et al., 2018).

Table 2 summarizes the impact of TESLA and ECDSA schemes on the service performances such as Vertical Position Errors (VPE), Vertical Protection Level (VPL), continuity, and availability of SBAS under different Page Error Rate(PER) conditions. When PER = 0, the presence or absence of authentication has no effect on all performance indicators. For PER = 1×10^{-3}, since the loss of each message may cause identity authentication failure, the continuity risk of SBAS messages after joining the authentication protocol is significantly higher, but the availability remains above 99%. It can be seen that joining the authentication service will have an impact on the SBAS message but still meet the availability performance.

Conclusion

This article introduces two different SBAS message authentication methods, ECDSA and TESLA, and four different feasible schemes combined with the current SBAS Interface Control Document (ICD). Combined with the simulation results of European EGNOS in EAST, the results of several performance indicators with or without certification are analyzed. It can be seen that after joining the authentication service, the performance of SBAS is less affected. SBAS messages are protected against spoofing.

Starting from improving the design of signals, SBAS authentication provides user terminals with the technical means to cope with spoofing and interference, enhancing the security of the SBAS augmentation service and promoting its applications in the fields of safe-of-life, such as aviation, navigation, and high-speed train. However, there are still many problems and challenges to be addressed in the authentication of SBAS.

In terms of system design, the SBAS signal authentication improves the security of SBAS service, but may

Table 2 Summary of SBAS performance with and without ECDSA and TESLA authentication, for cases with PER = 0 and PER = 1×10^{-3}

Items	Results for PER = 0		Results for PER = 1×10^{-3}		
	No authentication	ECDSA/TESLA	No authentication	ECDSA	TESLA
L1-I					
VPE 95%	2.86 m	2.90 m	2.86 m	2.94 m	2.93 m
VPL 99%	17.37 m	17.57 m	17.38 m	17.93 m	17.91 m
Continuity risk	$< 8 \times 10^{-6}$	$< 8 \times 10^{-6}$	$< 8 \times 10^{-6}$	7.7×10^{-3}	5.9×10^{-3}
Availability (PL < AL)	99.71%	99.63%	99.71%	99.80%	99.19%
AER	N/A	0	N/A	0.5%	0.3%
L5-I					
VPE 95%	1.66 m	1.72 m	1.66 m	1.72 m	1.72 m
VPL 99%	9.98 m	10.33 m	9.98 m	10.39 m	10.43 m
Continuity risk	$< 8 \times 10^{-6}$	$< 8 \times 10^{-6}$	$< 8 \times 10^{-6}$	5.8×10^{-3}	7.1×10^{-3}
Availability (PL < AL)	99.89%	99.85%	99.89%	99.17%	99.45%
AER	N/A	0	N/A	0.5%	0.3%

reduce its service performances such as integrity and continuity so that the demand for Category I of Precision Approach (CAT-I) may not be met. Several aspects need to be improved in the future, such as the selection of authentication protocols, optimal configuration of authentication parameters, processing of bit errors at the user terminals, and integrated applications of Automatic Dependent Surveillance-Broadcast (ADS-B)/SBAS. Overall performance evaluation for SBAS also needs to be carried out to ensure the balance between the SBAS augmentation service and authentication service.

In order to add authentication processing in the current SBAS processing at user terminals, we need to study the strategies of processing different authentication results to ensure the real-time use of integrity alarm information (< 6 s). Meanwhile, SBAS MOPS must be taken into consideration in aviation applications.

Concerning the compatibility and interoperability of GNSS/SBAS authentication, SBAS authentication only ensures the security of the augmentation service. However, the security of GNSS system is the cornerstone of the security for GNSS positioning service. European Galileo plans to provide OS-NMA authentication, and American Air Force Research Laboratory (AFRL) will launch Navigation Technology Satellite-3 (NTS-3) to implement technical trials of GPS signal authentication based on Chips-Message Robust Authentication (CHIMRA) signals. In the future, it is necessary to implement signal authentication of GNSS and the design of compatibility and interoperability of GNSS/SBAS authentication.

In the development of SBAS authentication standards we should consider the SBAS operation process and cryptographic algorithm standards in different countries, and have sufficient trials.

Acknowledgements
Not applicable.

Authors' contributions
Conceptualization: YL, WG, XC, TL, CL and GS; Methodology: XC, TL, JL and CL; Writing original draft: XC and SM; Editing: XC, WW and YL; Review: YL, XC, WG and JL. All authors read and approved the final manuscript.

Funding
This research is supported by the National Natural Science Foundation of China (61601009, 41974041) and the Young Talent Supporting Program of the China Association for Science and Technology (2019QNRC001).

Availability of data and materials
Not applicable.

Declarations

Competing interests
The authors declare that they have no competing interests.

Author details
[1] Beijing Institute of Tracking and Telecommunication Technology, Beijing 100094, China. [2] Beihang University, Beijing, China. [3] Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China. [4] University of Chinese Academy of Sciences, Beijing 100049, China.

Received: 28 December 2020 Accepted: 18 March 2021
Published online: 28 June 2021

References

Chiara, A. D., Broi, G. D., Pozzobon, O., Sturaro, S., Caparra, G., Laurenti, N., & Chatre, E. (2016a) Authentication Concepts for Satellite-Based Augmentation Systems, ION GNSS+ 2016, Portland.

Chiara, A. D., Broi, G. D., Pozzobon, O., Sturaro, S., Caparra, G., Laurenti, N., & Chatre, E. (2016b). Authentication concepts for satellite-based augmentation systems. In *Proceedings of the 29th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2016)* (pp. 3208–3221).

Chiara, A. D., Broi, G. D., Pozzobon, O., Sturaro, S., Caparra, G., Laurenti, N., & Fernandez-Hernandez, I. (2017). SBAS authentication proposals and performance assessment. In *Proceedings of the 30th international technical* *meeting of the satellite division of the institute of navigation (ION GNSS+ 2017)* (pp. 2106–2116).

Draft IWG SBAS L5 DFMC Interface Control Document (SBAS L5 DFMC ICD), E-OC-7260-ESA, 1 Draft 036, March 2015.

EGNOS Grant Plan 2019. (2018). GSA-EGN-PM-PL-244825 v1.0. https://www.gsa.europa.eu/sites/default/files/content/egnos_2019_grant_plan.pdf

Enge, P., Walter, T. (2014). Digital message authentication for SBAS (and APNT). In *ION GNSS+ 2014, Tampa, FL*.

Fernández-Hernández, I., Châtre, E., Chiara, A. D., Broi, G. D., Pozzobon, O., Fidalgo, J., & Rijmen, V. (2018). Impact analysis of SBAS authentication NAVIGATION. *Journal of the Institute of Navigation, 65*(4), 517–532.

Fernández-Hernández, I., Rijmen, V., Seco-Granados, G., Simón, J., Rodríguez, I., & Calle, J. D. (2014). Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service. In *Proceedings of the 27th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2014)* (pp. 2810-2827)..

Fernández Hernández, I. (2014a). GNSS authentication: design parameters and service concepts. In: *Proceedings of the European navigation conference*.

Fernández Hernández, I. (2014b). GNSS authentication: design parameters and service concepts. In: Proceedings of the European navigation conference.

ICAO, Annex 10-Volume 1 Aeronautical Telecommunications - Radio Navigation Aids.

Kerns, A. J., Wesson, K. D., & Humphreys, T. E. (2014). A blueprint for civil GPS navigation message authentication. In *2014 IEEE/ION position, location and navigation symposium-PLANS 2014* (pp. 262–269). IEEE.

Liu R. (2015). Information Authentication Based Beidou II Civil Signal Anti-spoofing Method. Civil Aviation University of China, 2015.

Liu T. (2018). Design of Navigation Message Authentication Scheme and Analysis of Performance. In *Proceeding of the 29th Conference of Spacecraft TT&C Technology in China, Shanghai, 2018*.

Lo, S., DeLorenzo, D., Enge, P., Akos, D., & Bradley, P. (2009). Signal authentication. *Inside GNSS, 4*(5), 30–39.

Minimum Operational Performances standards for global positioning system/wide area augmentation system airborne equipment (SBAS L1 MOPS), RTCA DO-229D, 2006.

Mu, S., Chen, Y., Liu, T., Liu, C., & Chen, X. (2020). Design of message authentication and OTAR broadcast strategy for BDSBAS. *Journal of Beijing University of Aeronautics and Astronautics*. https://doi.org/10.13700/j.bh.1001-5965.2020.0222.

Neish, A., Walter, T., & David Powell, J. (2019). Design and analysis of a public key infrastructure for SBAS data authentication. *Navigation, 66*(4), 831–844.

Neish, A., Walter, T., & Enge, P. (2019). Quantum-resistant authentication algorithms for satellite-based augmentation systems. *Navigation, 66*(1), 199–209.

Neish, A., Walter, T., & Powell, J. D. (2017) SBAS Data authentication: a concept of operations.

Neish, A., Walter, T., & Enge, P. (2018). Parameter selection for the TESLA keychain. ION GNSS. Vol. 1.

Neish, A., Walter, T., & Powell, J. D. (2019). SBAS data authentication: a concept of operations. In *Proceedings of the 32nd international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2019)* (pp. 1812–1823).

Perrig, A., Canetti, R., Tygar, J. D., & Song, D. (2000). Efficient authentication and signing of multicast streams over lossy channels. In *Proceeding 2000 IEEE symposium on security and privacy. S&P 2000* (pp. 56–73). IEEE.

Pozzobon, O., Wullems, C., Kubik, K., et al. (2004). Secure tracking using trusted gnss receivers and galileo authentication services. *Positioning, 3*(08), 200.

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS Spoofing and Detection. *Proceedings of the IEEE, 104*(6), 1258–1270.

Scott, L. (2003). Anti-spoofing and authenticated signal architectures for civil navigation systems. In: Proceedings of the ION GNSS meeting (pp. 1542–1552).

Standardization Administration (2016a) GB/T 32918.1——2016, SM2 Public key cryptographic algorithm SM2 based on elliptic curves, Part 1: General.

Standardization Administration (2016b) GB/T 32918.1——2016, SM2 Public key cryptographic algorithm SM2 based on elliptic curves, Part 2: Digital signature algorithm.

Tan, S. (2008). Development and thought of compass navigation satellite system. *Journal of Astronautics., 29*, 391–396.

Walter, T., Neish, A., Clark, B (2019) Recommended removal of the authentication time to detect key performance indicator for SBAS Authentication of the 15th joint working groups meeting of the navigation systems panel, Montreal, October 15–24. JWGs/5-WP/67.

Wesson, K., Rothlisberger, M., & Humphreys, T. (2012). Practical cryptographic civil GPS signal authentication NAVIGATION. *Journal of the Institute of Navigation, 59*(3), 177–193.

Wullems, C., Pozzobon, O., & Kubik, K. (2005). Signal authentication and integrity schemes for next generation global navigation satellite systems. In *European navigation conference (ENC-GNSS 2005)*.

Yuki, H. (2016). ANGO GIJUTSU NYUMON. The Third Edition. Post&Telecom Press, Vol. 12.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.