remote sensing

MDPI

Review

Satellite Navigation Signal Authentication in GNSS: A Survey on Technology Evolution, Status, and Perspective for BDS

Xiao Chen [1,2], Ruidan Luo [1], Ting Liu [1,*], Hong Yuan [1] and Haitao Wu [1]

[1] Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China
[2] School of Electronic, Electrical and Communication Engineering, University of Chinese Academy of Sciences, Beijing 100049, China
* Correspondence: liuting101015@aircas.ac.cn

Abstract: As the Global Navigation Satellite System (GNSS) is widely used in all walks of life, the signal structure of satellite navigation is open, and the vulnerability to spoofing attacks is also becoming increasingly prominent, which will seriously affect the credibility of navigation, positioning, and timing (PNT) services. Satellite navigation signal authentication technology is an emerging technical means of improving civil signal anti-spoofing on the satellite navigation system side, and it is also an important development direction and research focus of the GNSS. China plans to carry out the design and development of the next-generation Beidou navigation satellite system (BDS), and one of its core goals is to provide more secure and credible PNT services. This paper first expounds on the principles and technical architecture of satellite navigation signal authentication, then clarifies the development history of satellite navigation signal authentication, and finally proposes the BDS authentication service system architecture. It will provide technical support for the construction and development of the follow-up Beidou authentication service.

Keywords: satellite navigation; Beidou navigation satellite system; credible navigation; signal authentication; anti-spoofing

Citation: Chen, X.; Luo, R.; Liu, T.; Yuan, H.; Wu, H. Satellite Navigation Signal Authentication in GNSS: A Survey on Technology Evolution, Status, and Perspective for BDS. *Remote Sens.* **2023**, *15*, 1462. https://doi.org/10.3390/rs15051462

Academic Editor: Yunbin Yuan

Received: 31 January 2023
Revised: 26 February 2023
Accepted: 3 March 2023
Published: 5 March 2023

1. Introduction

With the Global Navigation Satellite System (GNSS) being widely used in power grids, finance, transportation and communication networks, and other livelihoods and key infrastructures, human life is becoming increasingly dependent on the navigation, positioning, and timing (PNT) services provided by satellite navigation [1]. However, the structure of satellite navigation signals is open, and there is a security risk of spoofing attacks, which makes the credibility of GNSS services increasingly prominent [2]. In recent years, GNSS spoofing incidents have occurred frequently [3,4]. How to solve the problem of the anti-spoofing of GNSS services and improve the credibility of user PNT services will be an important developmental direction in the future.

For the GNSS anti-spoofing problem, the common method is to add more sensors [5,6], more antennas, and more complex algorithms [7,8] into the user terminal to improve the user's anti-spoofing ability. Satellite navigation signal authentication technology is an anti-spoofing technology on the GNSS system side [9]. By adding cryptographic markers to satellite navigation signals, the receiver can verify whether the satellite navigation signals are from real satellites and whether the signals/messages have been tampered with [10]. At present, the construction of four major global navigation satellite systems has been completed. The addition of navigation signal authentication services requires appropriate modifications to the existing satellite navigation systems. On the one hand, it involves the existing system architecture, Interface Control Document (ICD), and cryptographic standards of various countries, and it is necessary to take into account the existing system design. On the other hand, GNSS has been applied on a large scale, and the navigation signal

authentication service cannot affect the existing navigation and positioning service. The Galileo System announced the navigation authentication service plan in 2016, providing Open Service Navigation Message Authentication (OSNMA) [11,12] at the Galileo-E1B. The test signals are now available, and formal services will be provided in 2023 [13]. The Japanese Quasi-Zenith Satellite System (QZSS) [14] and the Navigation with Indian Constellation (NavIC) [15] have both performed the on-orbit testing and verification of navigation message authentication technology. In addition, the United States has proposed the concept of Chips Message Robust Authentication (CHIMERA), and plans to carry out technology tests in 2023 on Navigation Technology Satellite-3 (NTS-3) [16].

In view of anti-spoofing, EU scholars summarized the technical methods of signal authentication in 2017, evaluated different authentication protocols, and looked forward to the authentication services of the GNSS system in the future [17]. In 2021, The Resilience Technical Subgroup of the U.S.-EU Working Group C (WGC-RESSG) summarized the existing the Satellite-Based Augmentation System (SBAS) authentication protocol, in order to add SBAS message authentication in the next version of the Dual Frequency Multi Constellation (DFMC) standard [18]. China's Beidou navigation satellite system (BDS) has completed the system construction in 2020 [19], and plans to conduct the design and development of the next-generation Beidou navigation system in 2022. One of its core goals is to provide more secure and credible PNT services [20]. The main contribution of this article is to design a service architecture for next-generation BDS authentication and analyze the corresponding technical challenges.

The paper is organized as follows: Section 2 expounds the principles and technical architecture of satellite navigation signal authentication and focuses on the analysis of the satellite navigation signal authentication technology and navigation message authentication protocol, as well as the new capabilities brought by the navigation signal authentication service. Section 3 sorts out the development process of satellite navigation signal authentication technology from the three stages. Section 4 designs the BDS authentication service system architecture, and puts forward the technical challenges faced from the aspects of security, key management, authentication system design, authentication performance evaluation, etc., which will provide technical support for the construction and development of the BDS authentication service system. The conclusions of this research are in Section 5.

2. Principles and Technical Architecture of the Satellite Navigation Signal Authentication

Satellite navigation signal authentication uses cryptographic methods to improve the anti-spoofing of civil GNSS signals and provides users with more credible PNT services. First of all, this section introduces the principle of satellite navigation signal authentication. Then, it describes the technical architecture of navigation signal authentication based on space segment, ground section and user segment, Finally, it analyzes the new capabilities brought by satellite navigation signal authentication, as well as the advantages and limitations in anti-spoofing.

2.1. Principles

Satellite navigation signal authentication technology aims to add encrypted authentication marks to satellite navigation signals to prevent satellite navigation signals from GNSS spoofing attacks. It is a new GNSS anti-spoofing technology that combines information security and navigation signal design. The sender (navigation satellite) uses cryptography technology to generate an "authentication symbol", which is embedded in the existing satellite navigation signal and broadcast to users. The receiver (GNSS user terminal) verifies the "authentication symbol" to confirm whether the received navigation signal is from a real satellite in orbit, and whether the navigation message has been forged or tampered with [21]. Satellite navigation signal authentication technology has the following characteristics:

(1) One-way broadcast.

The satellite navigation signal uses the navigation satellite broadcast signal to provide PNT services for terrestrial users, and its signal characteristics have the characteristics of one-way broadcast. Therefore, satellite navigation signal authentication technology should be based on the broadcast system authentication framework.

(2) Signal disclosure transmission.

Satellite navigation signals use the public signal structure to broadcast signals, and their signal authentication needs to have the characteristics of public signal transmission.

(3) Compatible with existing signal structure.

The authentication of satellite navigation signals will not affect existing GNSS services, so its authentication signal design should be compatible with an existing signal structure.

2.1.1. Satellite Navigation Signal Authentication Type

Satellite navigation signals include the carrier, pseudocodes, and message. The newly added authentication mark can be added to the navigation message [22] and spreading spectrum codes [23]. Figure 1 shows the generation of the navigation message including authentication message and the spreading spectrum code including authentication code. Therefore, the satellite navigation signal authentication type is divided into Navigation Message Authentication (NMA) and Spreading Code Authentication (SCA) [24].

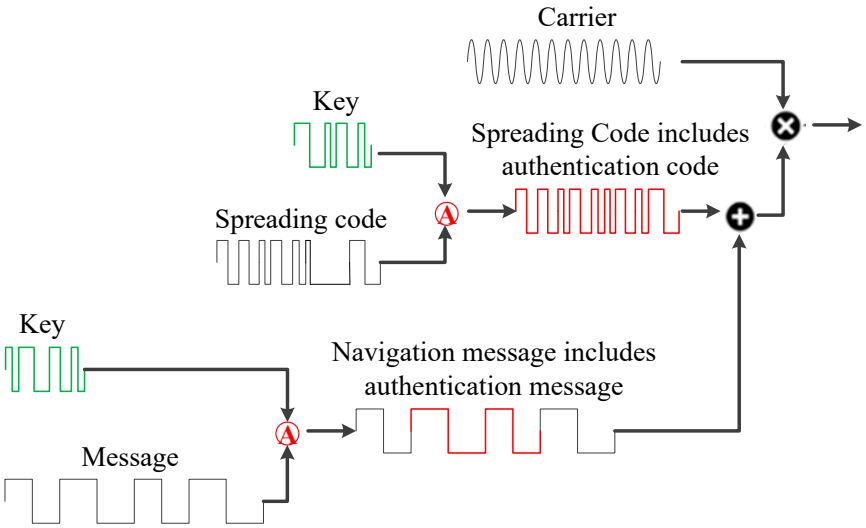

Figure 1. Satellite Navigation Signal Authentication.

(1) NMA

NMA uses message bit-level authentication to realize navigation source authentication. Its advantage is that the modification of the existing signal system is small and the signal modulation method is not changed—it is just used to upgrade the software of the user receiver. The engineering realization cost is small. The Galileo E1 OSNMA structure is shown in Figure 2. Galileo reserved a 40-bit message in the early ICD, and the ICD announced in 2021 clarified that the 40-bit message is the navigation authentication message [25].

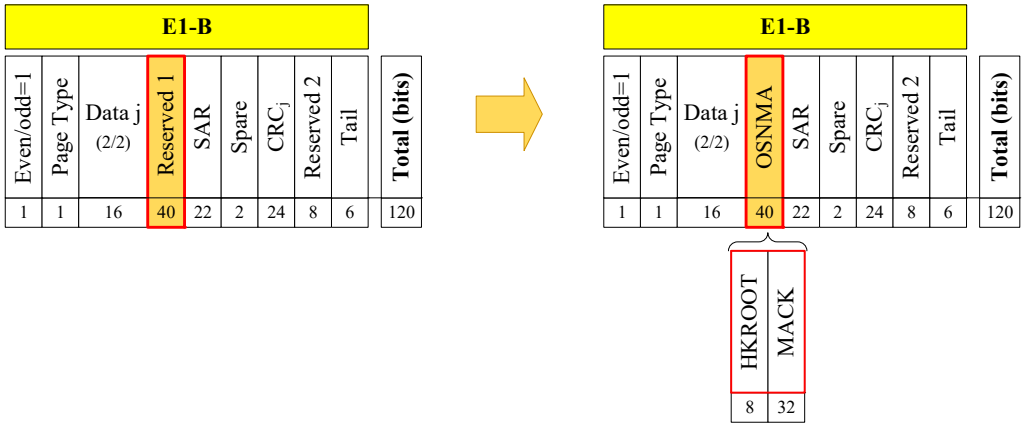

Figure 2. GALILEO NMA message structure [25].

(2) SCA

SCA adopts the characteristics of unpredictable authentication spreading chips, and implements authentication processing in the power domain, which can provide spoofing protection in the pseudorange domain. The typical SCA is the CHIMERA signal, as shown in Figure 3. Based on the TMBOC (Time-Multiplexed Binary Offset Carrier) signal, the 1 ms sector is divided into 31 segments via a combination of time division and time hopping, and different authentication channels (fast channel and slow channel) are assigned for each segment. The authentication codes are randomly replaced for 29 BOC(1,1) in each segment of 33 chips, and the 4 BOC(6,1) chips are never modified [26].

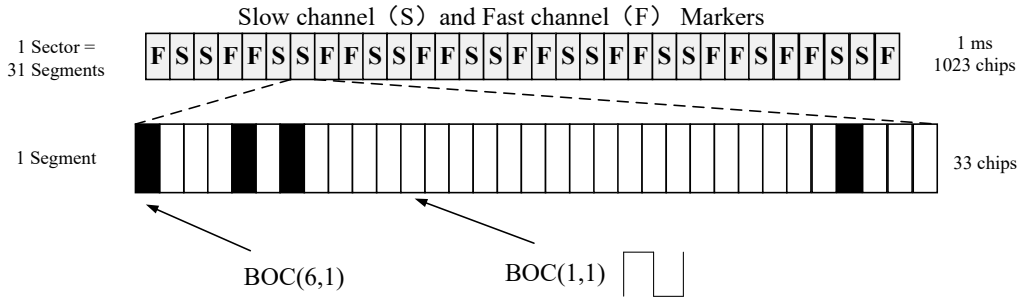

Figure 3. CHIMERA spreading code [26].

Compared with NMA, SCA can provide spoofing protection in the pseudorange domain, and it has higher security. However, the SCA authentication chip needs to be delayed to the user receiver; the receiver needs to buffer the sampled data so the implementation cost of the receiver is relatively costly. Table 1 shows the comparison of NMA and SCA.

Table 1. Comparison of NMA and SCA.

Type	Indicators	Receiver Processing	Feature
NMA [25]	Galileo-OSNMA Time Between Authentication: 10 s	Message bit authentication using Message Authentication Code (MAC)	The project implementation is less difficult, the security level is not as good as SCA, and it can be processed in real time at the terminal.
SCA [26]	NTS3-CHIMERA Time Between Authentication for slow channel: 180 s	Power Domain Authentication Using Sampled Data for Spreading Code Correlation Processing	The pseudorange can be authenticated. The authentication requires data caching, and the project implementation is costly.

Time Between Authentication for fast channel: 1.5 s or 6 s	

2.1.2. Satellite Navigation Message Authentication Type

The navigation message authentication protocol includes Digital Signatures (DS) and the Timed Efficient Stream Loss-Tolerant Authentication (TESLA).

Digital signatures are implemented based on asymmetric cryptography (also known as public key cryptography). The sender uses the private key to sign the message, and the receiver uses the public key to verify the signature of the message [27]. Digital signatures commonly use the Elliptic Curve Digital Signature Algorithm (ECDSA), which has the characteristics of high security and complex algorithm strength. In addition, European scholars proposed EC Schnorr's digital signature algorithm [18]. The digital signature schematic is shown in Figure 4 below.

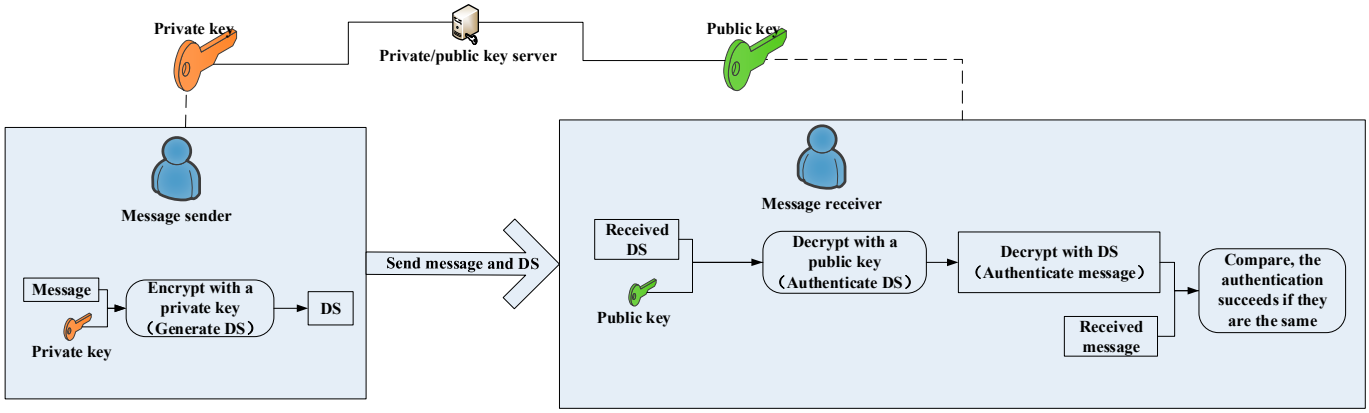

Figure 4. Digital Signature Schematic.

The TESLA protocol is a broadcast authentication protocol that can be applied to satellite navigation broadcast signals with limited bandwidth [28,29]. The TESLA protocol, designed by Perring et al., is an MAC-based broadcast authentication protocol [30,31]. The protocol uses a symmetric cryptography method, and the key is to use the delayed key release to ensure the security of the broadcast key.

The TESLA protocol generates a set of keychains through the hash function. The generation order of the keychain is Key_i, Key_{i-1},..., Key_1, Key_0, while the keychain system uses Key_0, Key_1,..., Key_{i-1}, Key_i. The advantage is that when the key is not received or not received at a certain moment, the key can be obtained via the key hash of the subsequent epoch. Then, according to the key Key_i and the navigation message M_i at the current moment, the Hash-based Message Authentication Code (HMAC) algorithm is used to generate the message authentication code MAC_i. The GNSS system broadcasts the navigation message M_i, the message authentication code MAC_i, and the Key_{i-1} of the previous epoch to the user; that is, the symmetric key used to generate the MAC is sent after the broadcast MAC is delayed by δ time. The user receives the GNSS message M_i for storage and the delayed symmetric key Key_i, then generates delay MAC_i', and compares it with the MAC_i of the GNSS broadcast. If the two are consistent, the authentication is passed. Key chain generation and the key usage of TESLA are shown in Figure 5 below.

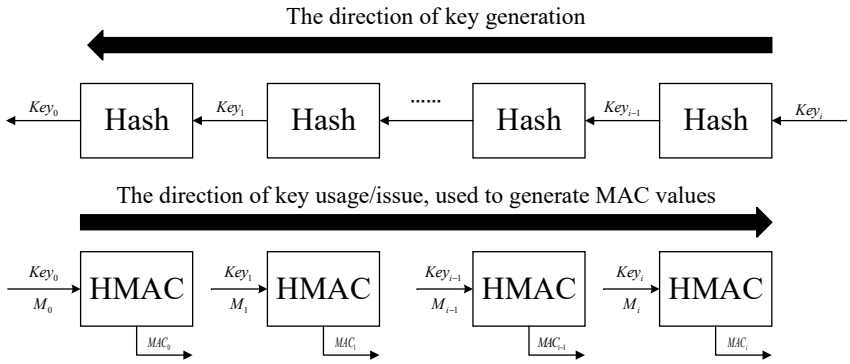

Figure 5. Key chain generation and key usage of TESLA.

Compared with the ECDSA algorithm, TESLA has a lower computational load and communication load, and is suitable for satellite navigation systems with limited message bandwidth. TESLA's one-way keychain generation and transmission improve the stability of authentication services. ECDSA has a variety of international standards, and the implementation process is simple, but ECDSA occupies more data bits. The comparison between TESLA and the digital signature is shown in Table 2.

Table 2. Comparison of TESLA and ECDSA.

Protocol	Cryptographic Algorithm	Calculated Amount	Authentication Information Truncation	Key Distribution Requirements	Key Length under the Same Security Level
TESLA [28–31]	Hash, HMAC	Small	Yes	Yes	Short
DS [18,27]	DS	Big	No	No	Long

2.2. Technical Architecture

The satellite navigation system consists of the space segment, ground segment, and user segment. Based on the existing satellite navigation system, the satellite navigation signal authentication will be extended to the space segment, the ground segment, the user terminal, and the network auxiliary segment. The space segment adds the authentication spreading code/authentication messages to the broadcast downlink satellite navigation signal, the user segment authenticates the received satellite navigation signal, and the network auxiliary segment uses the communication base station (terrestrial communication/satellite communication) to provide network auxiliary authentication information. If there is a GNSS spoofing signal in the actual environment, the user segment can identify whether the current signal is a spoofing signal through the authentication of the message/spreading spectrum code. The architecture of the satellite navigation signal authentication is shown in Figure 6.

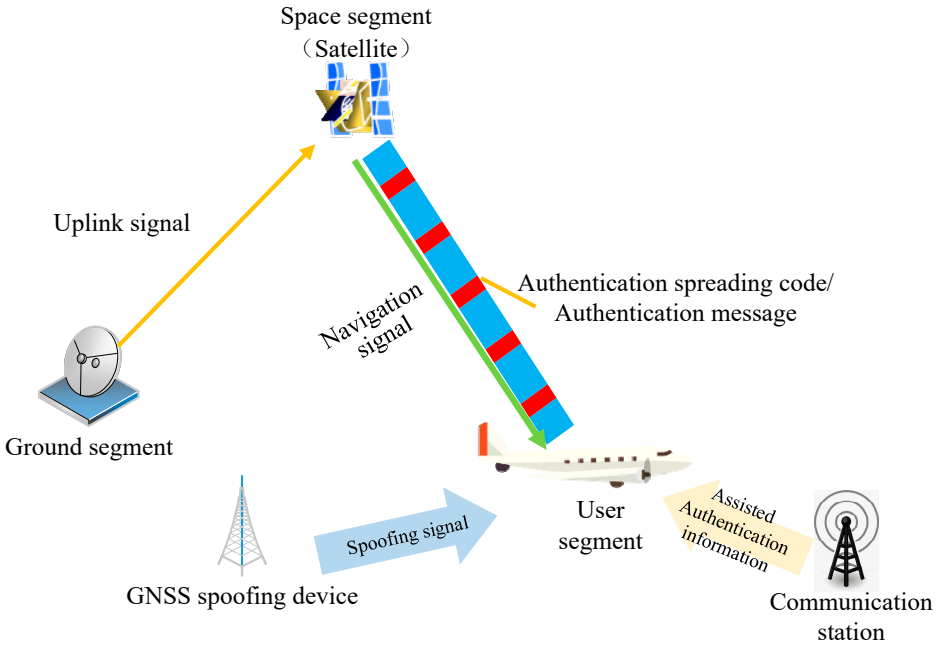

Figure 6. Satellite navigation signal authentication architecture.

2.3. Incremental Capability

Navigation signal authentication technology will bring a new service to the GNSS, which neither improves the accuracy nor augments the integrity and continuity, just focuses on improving the anti-spoofing capability of GNSS civil signals to provide users with more credible PNT services. Signal authentication is a system-side anti-spoof technology which can resist generative spoofing. The orange part in Figure 7 represents the incremental capability.

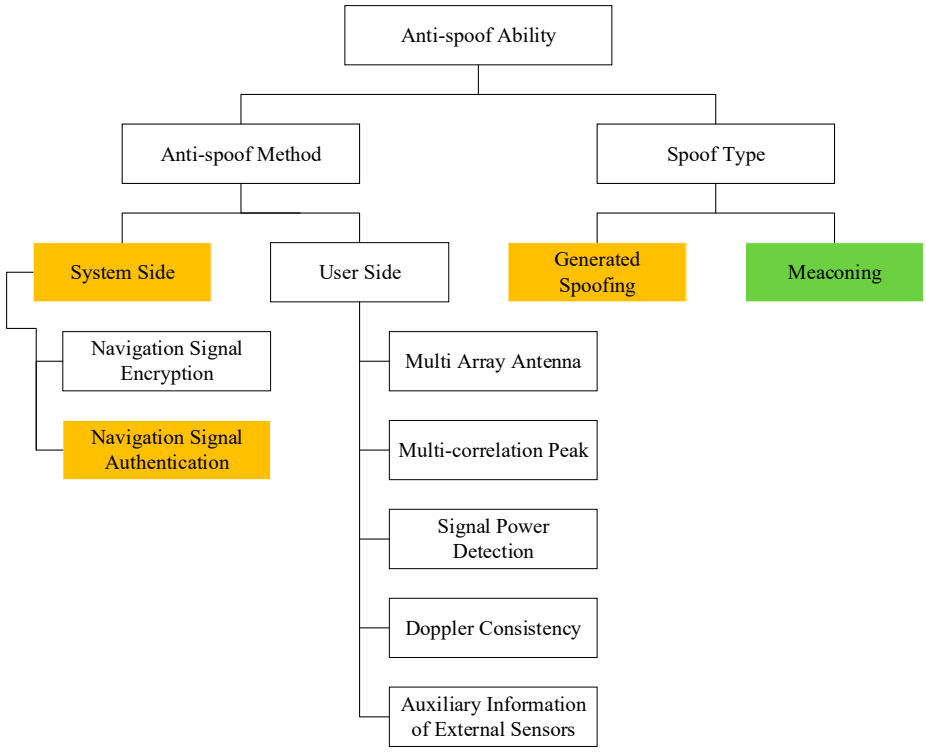

Figure 7. Ability of satellite navigation signal authentication technology.

(1) Anti-spoofing method

The anti-spoofing capability can be divided into system-side and user-side anti-spoofing technology according to the anti-spoofing method. The system-side anti-spoofing technology provides signal services with anti-spoofing capability, including navigation encryption signal technology [32] and navigation signal authentication technology [17]. The user-side anti-spoofing technology includes the direction of arrival (DOA) detection based on multi-array antennas [7,8], multiple correlation peaks [33,34], signal power [35,36], Doppler consistency [37,38], baseband processing algorithms, and the auxiliary information of external sensors [4,5]. Table 3 lists the comparison of the common anti-spoof algorithms. Compared with the existing user-side anti-spoofing algorithms, navigation signal authentication has a better anti-spoofing effect.

Table 3. Comparison of common anti-spoofing algorithms.

Anti-Spoofing Method	Description	Effect
Navigation signal encryption [32]	Encrypted signals serve authorized users, making it difficult for attackers to predict signals	High
Navigation signal authentication [17]	It is difficult for spoofed attackers to predict the authentication message/spreading code	High
DOA detection based on multi-array antennas [7,8]	The spoofing signal is generally emitted from a single transmitting antenna, and its satellites come from the same direction, while the real satellites of the signal come from different directions	High
Multiple correlation peaks [33,34]	The superposition of the spoofed signal and the real signal will bring multiple correlation peaks, and it will also cause distortion of the correlation peaks	Medium
Signal power [35,36]	The spoofing signal has more power, and the signal power changes during the spoofing implementation	Medium
Doppler consistency [37,38]	It is difficult for spoofing signals to keep the carrier Doppler shift consistent with the pseudocode Doppler shift	Medium
Auxiliary information of external sensors [4,5]	Spoofing signals cannot deceive sensors such as inertial navigation, chip-scale atomic clocks, and lidar	High

(2) Anti-spoofing capability

According to the GNSS cheating attacker type, it is divided into generated spoofing and meaconing. The anti-spoofing effect of the satellite navigation signal authentication is detailed, as shown in Table 4 [17].

Generated spoofing means that the attacker generates a spoofing signal with the exact same structure as the real GNSS signal [39], which utilizes the known vulnerabilities of the civilian signal ICD to generate a false GNSS spoofing signal and broadcast it to the target receiver. The prerequisite for satellite navigation signal authentication is that the spoofing attacker cannot break the cryptographic algorithm, so that the authentication message/spreading code cannot be forged. Therefore, satellite navigation signal authentication can solve the generative spoofing attack to civilian users.

Meaconing means that the attacker receives the navigation signal [40], performing proper delay and power amplification on the real GNSS signal, and then broadcasts the meaconing signal to the target receiver. The meaconing does not change the message and spreading code, so the satellite navigation signal authentication effect is not good for this method.

In addition to the above two common spoofing methods, Security Code Estimation and Replay (SCER) [41] has also been proposed in recent years. This method is to receive the real signal and estimate the encrypted or authenticated message in real time as much as possible. Then, the encrypted or authenticated message in the signal is reassembled and sent. SCER predicts the authentication message based on the security code estimation

method, which is effective for security codes with a low symbol rate (navigation message), but less effective for security codes with a high symbol rate (spreading code).

Table 4. Signal authentication anti-spoofing effect [17].

	Spoofing	NMA	SCA
Generated spoofing	Primary generated spoofing (low-cost software radio or commercial signal simulator)	High	High
	Intermediate generated spoofing (receive GNSS signal first and then generate spoofing signal)	High	High
	SCER	Low	High/Medium
	Advanced generated spoofing (multiple intermediate generative spoofing)	High/Medium	High
Meaconing	Simple meaconing (same delay for each satellite channel)	Low	Low
	Multichannel meaconing (the delay of each satellite channel is inconsistent)	Low	Low

3. Development History of Navigation Signal Authentication Technology

Satellite navigation signal authentication technology has undergone three stages of development: concept, technical research, technical trials, and on-orbit testing.

3.1. Concept

The concept of satellite navigation signal authentication was first proposed in the report, "Vulnerability Assessment of Transportation Infrastructure Based on GPS", issued by the Center for Transportation Systems in the United States in 2001, which comprehensively studied the anti-jamming and anti-spoofing methods of the Global Positioning System (GPS) and proposed several strategies to mitigate GPS spoofing. Although the report believes that "the best anti-spoofing technology will be based on the multiantenna array measurement method", it proposes an anti-spoofing method for encrypted authentication signals for the first time [42].

3.2. Technical Research

Research on satellite navigation signal authentication technology focuses on the GNSS, SBAS, and the high-precision augmentation system.

- GNSS

In 2003, Logan Scott of the United States first proposed the concept of civil GPS and Wide Area Augmentation System (WAAS) signal authentication by adding encrypted content to the message and spreading code of the GPS/WAAS signal to protect it from spoofing attacks. Three authentication methods are further defined: navigation message authentication, public spreading code authentication, and private spreading code authentication [43]. Along with the design and demonstration of the Galileo system, European scholar Pozzobon put forward the concept of providing navigation authentication services in the Galileo system and the potential market for Galileo navigation authentication in 2004 [44]. In 2005, Pozzobon further proposed the DS and TESLA protocol of NMA, and conducted the simulation experiment of message authentication [45]. At the same time, European Kuhn proposed a navigation authentication design that hides the encrypted signal in the thermal noise signal [46], and the receiver caches the pending authentication to verify after receiving the key. Since 2012, Andrew of the University of Texas has used GPS L2C and L5 signals to carry out NMA message design and has proposed a hybrid scheme based on ECDSA and TESLA [47]. Since 2019, relevant Chinese scholars have also carried out technical research on message authentication protocols [48,49]and spreading code authentication protocols for BDS-2 and BDS-3 [50,51].

- SBAS

In 2016, the European Union launched the EAST (EGNOS Authentication Security Test-bed) project, which aims to evaluate the SBAS authentication scheme and its impact on SBAS performance [52]. In 2019, the Elasticity Technology Group of US-EU Joint Working team jointly promoted the European Geostationary Navigation Overlay Service (EGNOS), WAAS, and other SBAS systems to provide navigation message authentication services [26], carried out ECDSA-I, ECDSA-Q, TESLA-I, and TESLA-Q simulation, and plans to add the message authentication service to the future DFMC standard [53]. In 2021, the United States, Europe, and Japan jointly launched the standardization of SBAS message authentication, and Stanford University in the United States designed the authentication message and Over the Air Rekeying (OTAR) parameters [54,55]. In 2021, China launched the Beidou Satellite-Based Augmentation System (BDSBAS) navigation message authentication design based on the Chinese commercial cryptographic standard [56,57]. In 2022, Europe and the United States submitted the first draft of the Standards and Recommended Practices (SARP) for SBAS authentication to promote SBAS authentication services, which involves the SBAS-L1 and SBAS-L5 frequencies.

- High-Precision Augmentation System

For GNSS high-precision authentication services, Japanese scholars demonstrated the Precise Point Positioning-Real Time Kinematic (PPP-RTK) authentication service design of the QZSS Centimeter Level Augmentation Service (CLAS) at the Institute of Navigation, in 2019 [58]. The CLAS adopts the message authentication method based on the TESLA protocol. Subsequently, in 2021, the ESA proposed a framework for providing authentication services in Galileo High Accuracy Service (HAS) [59], and evaluated the performances of two authentication protocols, digital signature and TESLA.

3.3. Technical Trials and On-Orbit Tests

- Galileo

In 2017, the European Union officially announced that Galileo will provide navigation authentication services. The E1 frequency (E1B) provides the OSNMA, and the E6 frequency provides the commercial service authentication [60]. At the end of 2021, the ESA officially announced that Galileo's public signal message authentication service OSNMA provides testing services. Galileo adopts cross-authentication technology. In addition to broadcasting its own satellite authentication messages, it also broadcasts other satellite authentication messages, which will improve the authentication efficiency of the entire constellation. The service will be officially provided in 2023 [61–63].

- GPS

In 2018, the United States officially announced that the CHIMERA signal would be broadcast on the NTS-3 satellite. The signal is based on the GPS-L1C signal and adopts a combined NMA and SCA authentication signal design. On the basis of NMA, an unpredictable chip is added to the spreading code of the civil signal, and the receiver checks the unpredictable code position and level of the spreading code to verify the authenticity of the spreading code. The security of the pseudorange measurement process is improved [16,64].

- QZSS

Since 2018, a team from the University of Tokyo in Japan has used the QZSS L1S signal to carry out satellite navigation signal authentication design and on-orbit testing. It adopted digital signature-based message authentication technology to carry out GPS L1C/A message and Galileo message authentication tests [14].

- NavIC

In 2022, India announced the progress of NavIC signal authentication on-orbit testing at the International Committee on Global Navigation Satellite Systems (ICG) conference.

It adopted message authentication technology based on the TESLA protocol and carried out message authentication tests based on L5 and S frequency [15].

Table 5 shows the status of signal authentication for the GNSS system. At present, the main GNSS suppliers carry out satellite navigation signal authentication research and construction to augment the capability of the national satellite navigation system based on their respective satellite navigation systems (the European Union for the Galileo E1 and E6 signals, the United States for the GPS L1C BOC signals, Japan for the QZSS L1 signals, and India for the NavIC signals).

Table 5. Status of GNSS signal authentication.

System	Service Type	Signal	Authentication Type	Authentication Protocol	Status
Galileo	Open service [61,62]	E1	NMA	TESLA	On-orbit testing
	Authorization service [63]	E6	SCE + SCA	---	On-orbit testing
	PPP-RTK service [59]	E6	NMA	TESLA or ECDSA	Simulation verification
GPS	Open service [16,64]	L1C	NMA + SCA	ECDSA	Simulation verification
QZSS	Open service [14]	L1	NMA	ECDSA	On-orbit testing
	PPP-RTK service [58]	L6	NMA	TESLA	On-orbit testing
NavIC	Open service [15]	L5, S	NMA	TESLA	On-orbit testing
SBAS	Open service [52–57]	SBAS-L1 SBAS-L5	NMA	TESLA	Simulation verification

4. Key Technologies and Challenges for the Construction of the Authentication Service System for the BDS

From the perspective of BDS signal authentication system construction, the authentication architecture for BDS is proposed and it is discussed from the aspects of security, key management, authentication system design, authentication performance evaluation technology, and terminal authentication processing technology.

4.1. Authentication Architecture for BDS

Facing the construction of the next-generation BDS, a BDS signal authentication service system is built that integrates high–medium–low mixed constellation, and standard positioning service and augmented services. The architecture is shown in Figure 8. The BDS medium orbit and high orbit broadcasts navigation and augmentation signals, and adds signal authentication functions in the existing signal system framework to provide message integrity and signal source identity verification capabilities; low-orbit satellites can broadcast both navigation signals and communication signals. Its navigation authentication signal is similar to that of the medium and high orbits, and the communication signal has a two-way communication link with the terminal, which can provide large-capacity communication resources.

Beidou navigation satellites will provide both navigation message authentication and a spreading code authentication service; BDSBAS will provide message authentication. Low-orbit navigation augmentation satellites can broadcast navigation ranging signals, and high-precision navigation messages, and transmit communication signals. Thus, on the one hand, the low-orbit navigation satellite provides two-way communication authentication, and on the other hand, it assists the BDS satellites or the BDSBAS satellites to complete the broadcast signal authentication and realize positioning authentication based on the spot beam. In addition, a third-party navigation signal authentication service can be provided using the terrestrial communication network.

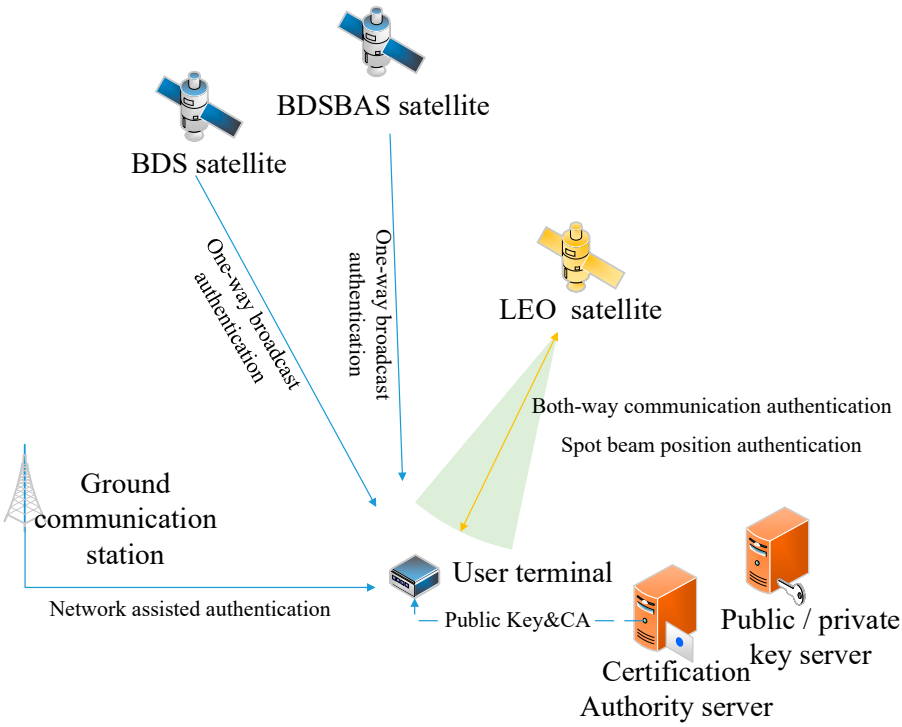

Figure 8. Authentication service architecture for BDS.

4.2. Security

The security of its authentication service is the prerequisite of satellite navigation signal authentication. The security refers to the ability to deal with spoofing attacks, which can be divided into two types according to the attack methods: one is to directly crack the cryptographic algorithm, which involves the security of the cryptographic algorithm itself; the other is to predict or estimate the authentication security code (authentication message or authentication spreading code), which involves the security of the authentication protocol.

(1) Cryptographic Algorithm Security

A cryptographic algorithm is a specific rule that uses a key to transform information into plaintext and ciphertext. Navigation signal authentication involves cryptographic algorithms, including digital signature algorithms, hash algorithms, and encryption algorithms. The security of cryptographic algorithms is determined by the length of the cryptographic algorithm key. For example, these include the ECDSA-P256, SHA256, AES128, and other cryptographic algorithms promulgated by the National Institute of Standards and Technology (NIST) [65,66]; and the SM2 public key cryptography algorithm, the SM3 cryptographic hash algorithm, and SM4 block cipher algorithm of the Chinese commercial cryptography standard [67–70].

The existing navigation signal authentication adopts the authentication protocol based on the cryptographic algorithm. For example, the navigation message authentication protocol includes the digital signature and the TESLA. The security of the digital signature algorithm is guaranteed by standard algorithms, such as ECDSA, SM2, etc. The security of the TESLA protocol involves a digital signature algorithm, message authentication code algorithm, and hash algorithm. The existing cryptographic algorithm standards all meet the security requirements.

With the continuous progress of quantum computing technology and quantum algorithms, more powerful attack methods are provided for key breaking. The well-known Shor quantum algorithm and Grover quantum algorithm pose a threat to the security of classical cryptosystems, especially for public key cryptosystems based on mathematical problems such as the factorization of large numbers and discrete logarithms, which have

brought about unprecedented challenges. Table 6 shows the impact of quantum computers on classical cryptography.

Table 6. The impact of quantum computers on classical cryptography.

Cryptographic Algorithm	Type	Functional	Quantum Computing Impact
AES, SM4 [66,70]	Symmetric cipher	Encryption and decryption	Need to increase key length
SHA-2, SHA-3, SM3 [27,69]	Hash	Hash Function	Need to increase output length
RSA, ECDSA, DSA, SM2 [27,65,67,68]	Public key cryptography	Digital signature, key distribution	No longer safe

Therefore, considering the security of the BDS signal authentication cryptographic algorithm, how to choose the appropriate cryptographic algorithm, cryptographic security level and key update cycle while taking into account new future cryptographic algorithms, such as post-quantum cryptography to resist future quantum computing attacks will become an important direction of future research.

(2) Authentication Protocol Security

The satellite navigation signal adopts a one-way broadcast signal system, and its authentication protocol includes an asymmetric cryptosystem and TESLA [71].

The authentication protocol based on an asymmetric cryptographic system uses CA (Certification Authority) digital certificate to achieve identity authentication, and asymmetric cryptographic algorithm to realize message authentication. Authentication protocols are determined by asymmetric cryptographic algorithms, such as the ECDSA algorithm and the EC Schnorr algorithm, which is determined by cryptographic algorithm and key management security.

The TESLA protocol implements identity authentication based on CA digital certificates and implements message authentication based on a symmetric cryptographic algorithm combined with delayed key transmission. It requires that certain time synchronization requirements must be met between the satellite and the terminal. Attacks against the TESLA protocol include attacks on the keychain (such as keychain pre-computation attacks, keychain brute force attacks, and keychain replay attacks), message authentication code brute force attacks, and time synchronization attacks on transceivers. The security of TESLA protocol consists of TESLA key and MAC truncation length, TESLA keychain length (the replacement keychain period), and TESLA time synchronization requirements. Table 7 shows the security design of the TESLA protocol of a typical satellite navigation system.

Table 7. Security design of TESLA protocol for typical satellite navigation system.

System	Key Length	MAC Length	Keychain Update Cycle	Time Synchronization Requirements
Galileo [13]	128 bits	40 bits	168 h (1 week)	≤30 s
SBAS-BigMAC [28]	30 bits	115 bits	-	need
SBAS-LittleMAC [28]	30 bits	15 bit	-	need
NavIC [15]	116 bits	30 bits	-	≤48 s

Therefore, considering the security of the BDS signal authentication protocol; balancing TESLA key; MAC truncation length; TESLA keychain length (replacement of the keychain period) and building a time synchronization, trusted mechanism will be one of the important directions of future research. In addition, the security of providing two-way communication authentication based on low-orbit navigation satellites also needs to be studied.

4.3. Design and Analysis of a Public Key Infrastructure for BDS Data Authentication Key Management

Key management involves the management process of the key life cycle, such as key generation, distribution, update and revocation. It is also related to the administrative management system of keys. The functions of key management are as follows: Firstly, when using authentication services, a chain of trust for keys needs to be built. Secondly, keys are regularly replaced to prevent them from being intercepted and exploited by malicious attackers. Thirdly, when keys are leaked, they can be changed in time. Considering one-way communication and the small bandwidth of satellite broadcasting, the key management scheme includes three-level key management based on a Merkle tree, two-level key management based on ECDSA, and three-level key management based on the TESLA protocol. The details are shown in Table 8.

(1) Three-level key management based on a Merkle tree.

Key management needs to build a chain of trust to ensure the authenticity of the key. Galileo OSNMA adopts the key management scheme based on a Merkle tree, and initially completes the on-orbit test [61,62]. The third-level key is the TESLA key, the second-level key is the TESLA public key to authenticate the root key, and the first-level key is the Merkle tree root, as shown in Figure 9.

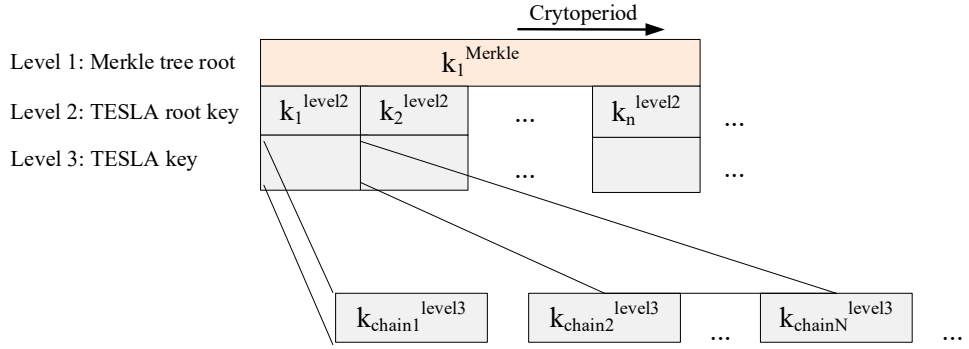

Figure 9. Three-level scheme based on the Merkle tree.

(2) Second-level key management based on ECDSA.

The ECDSA scheme is an alternative scheme for SBAS authentication, and its key management scheme adopts second-level key management. The second-level keys are the public and private keys for message authentication, and the first-level key is the system CA public key [72]. The scheme is as shown in Figure 10.

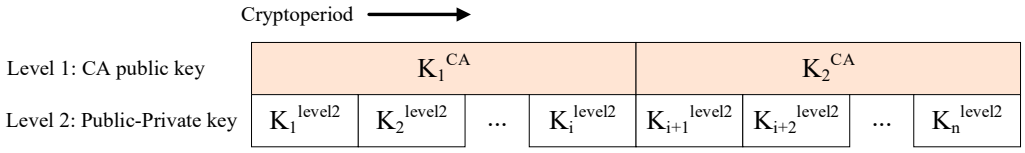

Figure 10. Second-level scheme based on ECDSA [72].

(3) Three-level key management based on TESLA.

The TESLA protocol is an alternative scheme for SBAS authentication, and its key management scheme adopts three-level key management. The third-level key is the TESLA key, the second-level key is the TESLA public key to authenticate the root key, and the first-level key is the CA public key [72]. The scheme is as shown in Figure 11.

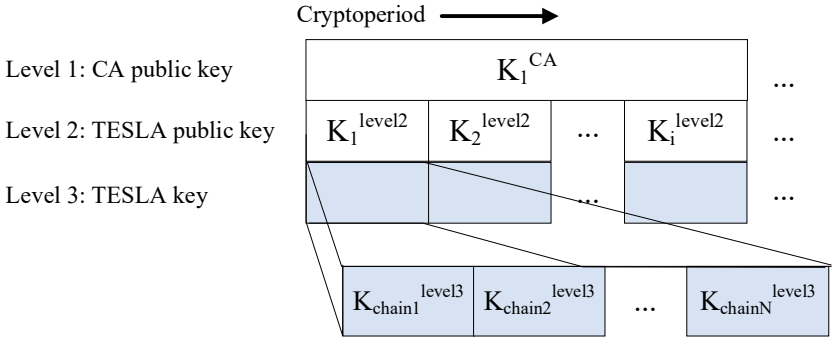

Figure 11. Three-level scheme based on the TESLA protocol [72].

Table 8. Key management scheme.

System	Key Management	First-Level	Second-Level	Third-Level	Receiver Built-In Key
Galileo [25,26]	Three-level scheme based on the Merkle tree	Merkle tree root key	TESLA public key	TESLA shared key	Built-in Merkle tree root key
SBAS [72]	Second-level scheme based on ECDSA	CA public key	Message authentication public and private key	--	Built-in CA public key
SBAS [72]	Three-level scheme based on TESLA protocol	CA public key	TESLA public key	TESLA shared key	Built-in CA public key

The key management for the BDS signal authentication service involves a series of technical challenges: one is to design a corresponding hierarchical key system for different authentication protocols, and the selection of a key hierarchical management structure is closely related to its application scenarios; the other is to research the key distribution scheme combining different methods such as over-the-air key update, receiver built-in, and network distribution to simplify the key distribution process under the premise of ensuring security; the third challenge is a key distribution strategy and optimization algorithm and the fourth challenge is the key revocation policy in the case of key leakage.

4.4. Authentication Mechanism

The authentication mechanism design includes navigation message authentication and navigation spreading code authentication.

(1) Navigation message authentication.

The design of navigation message authentication needs to have the following characteristics: firstly, the authentication message is compatible with the existing message format of BDS and its augmentation system. Secondly, the authentication message can meet the characteristics of a one-way broadcast of Beidou navigation signals and low message bandwidth. Thirdly, Chinese cryptographic standards should be selected as the priority for being independent and controllable.

- BDS

The standard positioning service of BDS includes B1C and B2a. Taking BDS B1C as an example [73,74], the authentication message bits are reserved in advance for Galileo E1, and B1C needs to design a new authentication message frame—subframe 3 adds page 5. The B1C message frame broadcast period is 18 s, and the authentication period is 90 s, which is much longer than the Galileo authentication period (10 to 30 s). The Beidou constellation adopts the cross-authentication method and the authentication message frame offsets the transmission mechanism, which is expected to increase the authentication period to 18 s. The cross-authentication method is that Beidou satellites not only provide their own authentication information, but they also provide the authentication

information of adjacent satellites. The authentication message frame offset transmission mechanism refers to the time-sharing broadcast of each satellite message authentication frame (subframe 3, page 5); that is, each satellite broadcasts a different message frame at the same time, which is different from the existing Beidou satellite broadcast strategy. There are huge challenges from the perspective of project implementation. The details of the authentication message offset transmission are as follows in Figure 12.

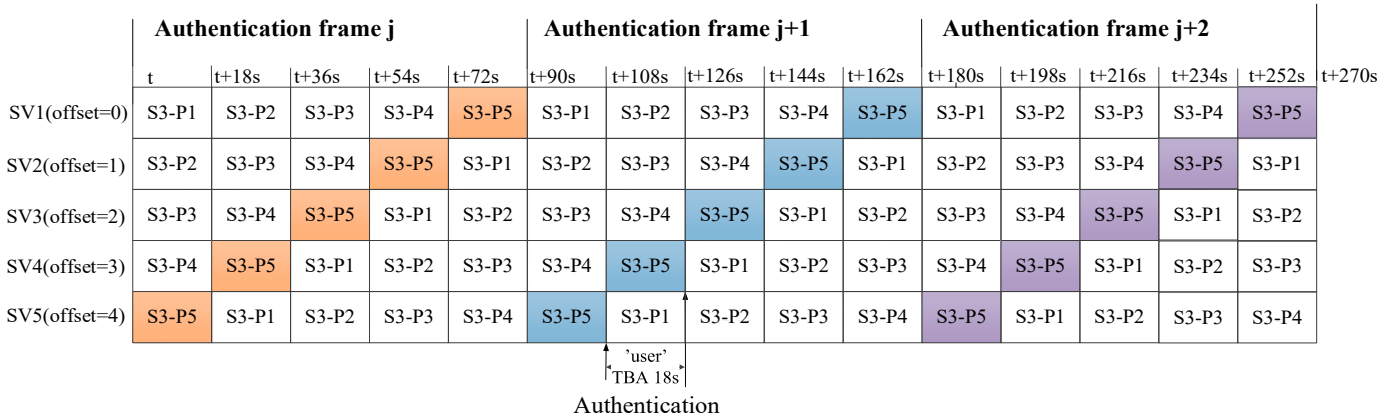

Figure 12. Satellite offset transmission.

- BDSBAS

BDSBAS message authentication needs to meet the relevant documents of the International Civil Aviation Organization (ICAO) [52]. At present, it has been designated as a TESLA authentication scheme internationally, and it plans to provide authentication services at the SBAS L1 and L5 frequency in the future [54,55]. The addition of the SBAS authentication design is limited by the constraints imposed by SARPs on the authentication system. The SBAS message format is shown in Figure 13.

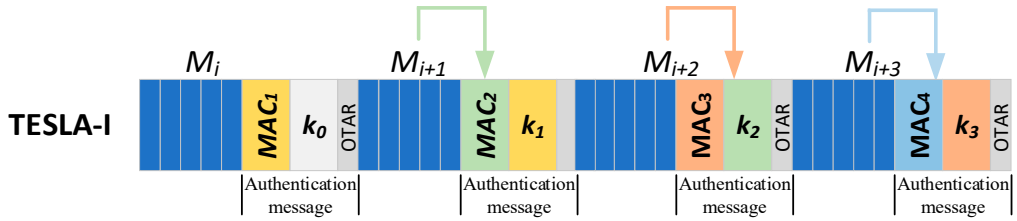

Figure 13. SBAS message format [52].

(2) Spreading Code Authentication.

The spreading code authentication is constructed by adding an unpredictable spreading code to the spreading code sequence. Figure 3 is a GPS CHIMERA authentication spreading code design [24], and the Beidou navigation spreading code authentication design needs to have the following requirements: First, it can be compatible with the existing Beidou signal structure and will not affect the existing signal processing. Second, it is designed to take into account both fast channel authentication and slow channel authentication.

4.5. Authentication Performance Evaluation

The authentication performance evaluation results represent the service performance of the BDS authentication service. It is necessary to build a complete authentication performance indicator system to comprehensively represent the security, robustness,

authentication, and other performances of the authentication service. The authentication performance indicators are shown in Figure 14.

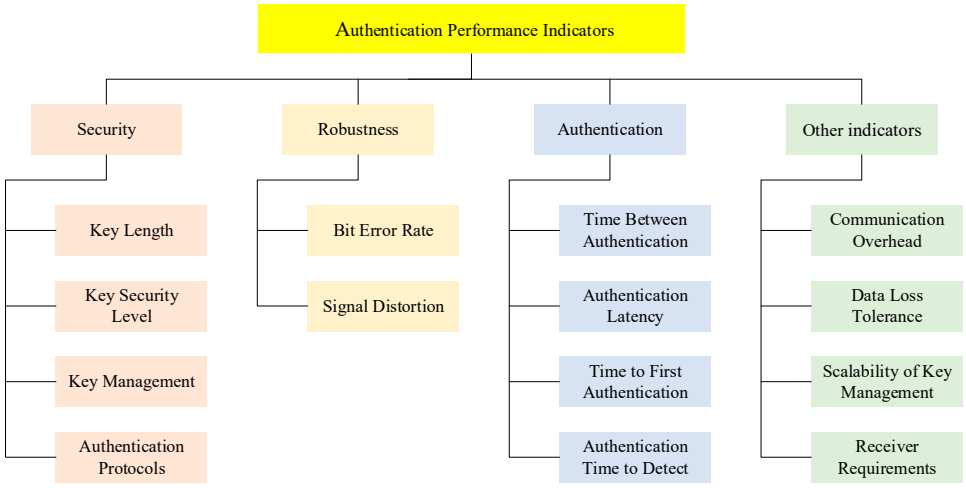

Figure 14. Authentication performance indicators.

(1) Security.

Security describes the ability to resist spoofing attacks, including key length, key security level, key management and authentication protocols [71]. The NMA is embodied in the unpredictable message bit/symbol, and the SCA is embodied in the unpredictable spreading code, that is, the entropy of the authentication signal.

(2) Robustness.

Robustness describes the maximum bit error rate or signal distortion that can be tolerated under channel transmission [21]. The NMA is reflected in the maximum message bit error rate, which will lead to the failure of the entire frame of message authentication; the SCA is embodied in the maximum signal distortion, which will cause signal correlation peak attenuation, resulting in missed alarms and false alarms in authentication.

(3) Authentication.

Authentication describes the ability of the receiver to perform message/spreading code authentication, including the time between authentication, authentication latency, time to first authentication, and authentication time to detect [18], etc.

(4) Other indicators.

Other indicators include communication overhead, data loss tolerance, the scalability of key management, and receiver requirements. Communication overhead refers to the communication bandwidth required for authentication messages/spreading codes; data loss tolerance refers to the ability to restore authentication services or to minimize service impact in the event of data loss; the scalability of key management refers to being faced with the scalability of key distribution, storage, and update under a large number of users; receiver requirements refer to the cost of additional authentication services for receivers, such as SCA, which will increase receiver storage resources.

4.6. Terminal Processing

Since the authentication message/spreading code lags behind the to-be-authenticated signal, there is a risk of spoofing attacks during this time. Terminal processing technology refers to how the user terminal handles the authentication signal.

(1) Message Authentication Processing.

Taking SBAS navigation message authentication as an example, SBAS requires the integrity alarm time to be 6 s, and the authentication message will lag the integrity

message [28,53]. The authentication MAC will be delayed by at least 1 s, and the key corresponding to the MAC will be delayed by 6 s. For terminal processing, it is faced with the problem of whether to perform authentication processing or to use integrity first. Authentication first will cause the integrity alarm to time out. If the integrity is used first, the user's integrity parameter may be forged. Therefore, the processing of message authentication is still a problem that needs to be studied.

(2) Spreading Code Authentication Processing.

Compared with the navigation message authentication process, which stores only the navigation message, the spreading code authentication process needs to buffer the signal sample data [16,63]. Taking the CHIMERA signal as an example, slow channel authentication needs to cache data for at least 180 s. According to the 20 MHz sampling rate and 2-bit quantization, a 7.2 Gbit buffer is needed, and the buffer capacity of the receiver cannot meet the requirement at present. Fast authentication requires the data to be cached for at least 3 s, requires a 120 Mbit cache, and requires low-orbit satellite/5 G network assistance, which involves the co-processing of navigation and communication, which is still under study.

5. Conclusions

The satellite navigation signal authentication technology will provide more credible PNT services. Based on summarizing and reviewing the existing satellite navigation signal authentication, this paper designs a service architecture for next-generation BDS authentication and analyzes the corresponding technical challenges. The main conclusions are as follows:

(1) Navigation signal authentication technology is a method used to improve the anti-spoofing ability of the GNSS on the system-side, which can solve the generated spoofing.
(2) In the future, authentication services will become the GNSS standard to improve the credible service capabilities of the GNSS.
(3) For the construction of the next-generation BDS, this paper designs a Beidou authentication service system integrating high, medium, and low constellations; standard positioning and augmentation services; and navigation and communication. It involves system security, key management, authentication mechanism, authentication performance evaluation and terminal processing.

In summary, satellite navigation signal authentication is an emerging technology in the current GNSS development stage, which can provide users with more credible PNT services. During the gradual construction of the next-generation BDS in China, it is of great significance to seriously consider the " assured and credible" capabilities provided by navigation signal authentication and its application prospects and to identify and overcome corresponding key technologies.

Author Contributions: Conceptualization, X.C. and R.L.; methodology, X.C. and R.L.; investigation, X.C., R.L. and T.L.; resources, H.Y. and H.W.; writing—original draft preparation, X.C.; writing—review and editing, X.C., R.L., T.L., H.Y. and H.W.; visualization, X.C. and T.L.; supervision, T.L., H.Y. and H.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Defence Science and Technology Innovation Special Zone of China (Grant No.: CX2022-04-03-02) and the Key Deployment Project of National Defense Science and Technology Innovation of Chinese Academy of Sciences (Grant No.: 2021-KJC-Y-0617).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. EUSPA EO and GNSS Market Report 2022. Available online: https://www.euspa.europa.eu/euspa-market-report-2022-0 (2022, 1, (1), 1-216.).
2. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M., Jr. Assessing the spoofing threat: development of a portable GPS civilian spoofer. In Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008), Savannah, GA, USA, 16–19 September 2008; pp. 2314–2325.
3. Bhatti, J.; Humphreys, T.E. Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *Navigation* **2017**, *64*, 51–66.
4. Wang, K.; Chen, S.; Pan, A. Time and Position Spoofing with Open Source Projects. In Proceedings of the Black Hat Europe 2015, Amsterdam, The Netherlands, 10–13 November 2015.
5. Moafipoor, S.; Bock, L.; Fayman, J.A. Resilient Sensor Management for Dismounted Assured-PNT. In Proceedings of the 2020 International Technical Meeting of the Institute of Navigation, San Diego, CA, USA, 21–24 January 2020; pp. 1135–1147.
6. Khanafseh, S.; Roshan, N.; Langel, S.; Chan, F.-C.; Joerger, M.; Pervan, B. GPS spoofing detection using RAIM with INS coupling. In Proceedings of the Position, Location and Navigation Symposium-PLANS, Monterey, CA, USA, 5–8 May 2014; pp. 1232–1239.
7. Yang, Q.; Zhang, Y.; Tang, C.K. A combined antijamming and antispoofing algorithm for GPS Arrays. *Int. J. Antennas Propag.* **2019**, *2019*, 8012569.
8. Lee, Y.S.; Yeom, J.S.; Noh, J.H.; Lee, S.J.; Jung, B.C. A novel GNSS spoofing detection technique with array antenna-based multi-PRN diversity. *J. Position. Navig. Timing* **2021**, *10*, 169–177.
9. de Castro, H.V.; van der Maarel, G.; Safipour, E. The possibility and added-value of authentication in future Galileo open signal. In Proceedings of the 23th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION 2010), Portland, OR, USA, 21–24 September 2010.
10. Fernandez-Hernandez, I.; Rijmen, V.; Seco-Granados, G.; Simón, J.; Rodríguez, I. 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), Tampa, FL, USA, 8–12 September 2014; pp. 2810–2827.
11. Walker, P.; Rijmen, V.; Fernandez-Hernandez, I.; Bogaardt, L.; Seco-Granados, G.; Simón, J.; Calle, D.; Pozzobon, O. Galileo Open Service Authentication: A Complete Service Design and Provision Analysis. In Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2015), Tampa, Florida, USA, 14–18 September 2015; pp. 3383–3396.
12. Fernandez-Hernandez, I.; Rijmen, V.; Seco-Granados, G.; Simon, J.; Rodríguez, I.; David Calle, J. A Navigation Message Authentication Proposal for the Galileo Open Service. *Navig. J. Inst. Navig.* **2016**, *63*, 85–102.
13. Nicola, M.; Motella, B.; Pini, M.; Falletti, E. Galileo OSNMA Public Observation Phase: Signal Testing and Validation. *IEEE Access* **2022**, *10*, 27960–27969.
14. Manandhar, D.; Shibasaki, R. Authenticating GALILEO Open Signal using QZSS Signal. In Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2018), Miami, FL, USA, 24–28 September 2018; pp. 3995–4003.
15. Pravin, P. *Navigation Message Authentication (NMA) for NavIC SPS*; ICG-16, Abu Dhabi, United Arab Emirates: 2022.
16. Anderson, J.M.; Carroll, 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 Proceedings of the 31th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS + 2018, Portland, OR, 25–29 September 2018.
17. Margaria, D.; Motella, B.; Anghileri, M.; Floch, J.-J.; FernandezHernandez, I.; Paonni, M. Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives. *IEEE Signal Process. Mag.* **2017**, *34*, 27–37.
18. Fernández-Hernández, I.; Walter, T.; Neish, A.M.; Anderson, J.; Mabilleau, M.; Vecchione, G.; Châtre, E. SBAS message authentication: a review of protocols, figures of merit and standardization plans. In Proceedings of the 2021 International Technical Meeting of the Institute of Navigation, Auditorium UPC, Barcelona, Spain, 25–28 January 2021; pp. 111–124.
19. Cai, H.; Meng, Y.; Geng, C.; Gao, W.; Zhang, T.; Li, G.; Shao, B.; Xin, J.; Lu, H.; Mao, Y.; et al. BDS-3 performance assessment: PNT, SBAS, PPP, SMC and SAR. *Acta Geod. Et Cartogr. Sin.* **2021**, *50*, 427–435.
20. The State Council Information Office of the People's Republic of China. 2022. Available online: http://www.scio.gov.cn/zfbps/32832/Document/1732789/1732789.htm (accessed on 4 November 2022).
21. Fernandez-Hernandez, I. *Snapshot and Authentication Techniques for Satellite Navigation*; Aalborg University: Aalborg, Denmark: 2015.
22. Curran, J.T.; Paonni, M. Securing GNSS: An End-to-end Feasibility Analysis 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), Tampa, FL, USA, 8–12 September 2014; pp. 2828–2842.
23. Gkougkas, E.; Pany, T.; Eissfeller, B. Sensitivity Analysis of Potential Future Authentication Components for Open Service GNSS Signals. In Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS + 2018), Miami, FL, USA, 24–28 September 2018.
24. Shen, C.; Guo, C. Study and Evaluation of GNSS Signal Cryptographic Authentication Defenses. *GNSS World China* **2018**, 43, 7–12.

25. European Union. *GALILEO Open Service Navigation Message Authentication (OSNMA) Receiver Guidelines for the Test Phase*; European Union Issue 1.0; 2021.
26. Air Force Research Laboratory Space Vehicles Directorate Advanced GPS Technology. Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface. 16 April 2019. CHAPMAN D C. Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Seg-ment/User Segment Interface (IS-AGT-100)[R]: Advanced GPS Technologies Program, 2019.
27. Hiroshi, Y. *Angō Gijutsu Nyūmon*, 3rd ed.; Post & Telecom Press: Beijing, China, 2016. (In Chinese)
28. Neish, A.; Walter, T.; Powell, J.D. 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), Miami, FL, USA, 16–20 September 2019; pp. 1812–1823.
29. Neish, A.; Walter, T.; Enge, P. Parameter selection for the TESLA keychain. In Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2018), Miami, FL, USA, 24–28 September 2018; pp. 2155–2171.
30. Perrig, A.; Canetti, R.; Tygar, J.D. Efficient authentication and signing of multicast streams over lossy channels. In Proceedings of the 2000 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 14–17 May 2000; pp. 56–73.
31. Caparra, G.; Sturaro, S.; Laurenti, N.; Wullems, C. Evaluating the Security of One-Way Key Chains in TESLA-Based GNSS Navigation Message Authentication Schemes. In Proceedings of the 2016 International Conference on Localization and GNSS (ICL-GNSS), Barcelona, Spain, 28–30 June 2016; pp. 1–6.
32. Zhao, X.; Liu, C. GPS Military Signal Security Protection and Password Management. *Mod. Navig.* **2020**, *11*, 14–19.
33. Li, J.Z.; Zhu, X.W.; Ouyang, M.J.; Li, W.Q.; Chen, Z.K.; Dai, Z.Q. Research on multi-peak detection of small delay spoofing signal. *IEEE Access* **2020**, *8*, 151777–151787.
34. Khan, A.M.; Ahmad, A. Global navigation satellite systems spoofing detection through measured autocorrelation function shape distortion. *Int. J. Satell. Commun. Netw.* **2022**, *40*, 148–156.
35. Dehghanian, V.; Nielsen, J.; Lachapelle, G. GNSS spoofing detection based on receiver C/N0 estimates. In Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation, Nashville, TN, USA, 17–21 September 2012; pp. 2875–2884.
36. Elezi, E.; Cankaya, G.; Boyaci, A.; Yarkan, S. A detection and identification method based on signal power for different types of electronic jamming attacks on GPS signals. In Proceedings of the 2019 IEEE 30th Annual International Symposium on Personal,Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 8–11 September 2019; pp. 1–5.
37. He, L.; Li, H.; Lu, M.Q. Global navigation satellite system spoofing detection technique based on the doppler ripple caused by vertical reciprocating motion. *IET Radar Sonar Navig.* **2019**, *13*, 1655–1664.
38. He, L.; Li, H.; Lu, M.Q. Dual-antenna GNSS spoofing detection method based on doppler frequency difference of arrival. *GPS Solut.* **2019**, *23*, 1–14.
39. Bian, S.; Hu, Y.; Ji, Bing. Research status and prospect of GNSS anti-spoofing technology. *Sci. Sin. Inf.* **2017**, *47*, 275–287.
40. Zhao X，Chen X，Guo, X. A Repeater Spoofing Method for GNSS Clock of receiver. *Telecommun. Eng.* **2020**, *60*, 1415–1419.
41. Arizabaleta, M.; Gkougkas, E.; Pany, T. A Feasibility Study and Risk Assessment of Security Code Estimation and Replay (SCER) Attacks. In Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2019), Miami, FL, USA, 16–20 September 2019.
42. Volpe, J.A. *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*; National Transportation System Center, USA, 2001.
43. Scott, L.D. *Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems*; Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), Portland, USA, 2003; pp 1543-1552.
44. Pozzobon, O.; Wullems, C.; Kubik, K. Secure Tracking using Trusted GNSS Receivers and Galileo Authentication Services. *J. Glob. Position. Syst.* **2004**, *3*, 200–207.
45. Wullems, C.; Pozzobon, O.; Kubik, K. Signal authentication and integrity schemes for next generation global navigation satellite systems. In Proceedings of the European Navigation Conference (ENC-GNSS 2005), Munich, Germany 19–22 July 2005.
46. Kuhn, M.G. An Asymmetric Security Mechanism for Navigation Signals. In Proceedings of the Information Hiding: 6th International Workshop, IH 2004, Toronto, Canada, 23–25 May 2004.
47. Wesson, K.; Rothlisberger, M.; Humphreys, T. Practical cryptographic civil GPS signal authentication. *Navigation* **2012**, *59*, 177–193.
48. Wu, Z.; Zhang, Y.; Liu, R. BD-II NMA&SSI: An Scheme of Anti-Spoofing and Open BeiDou II D2 Navigation Message Authentication. *IEEE Access* **2020**, *8*, 23759–23775.
49. Yuan, M.; Lv, Z.; Chen, H.; Li, J.; Ou, G. An Implementation of Navigation Message Authentication with Reserved Bits for Civil BDS Anti-Spoofing. In Proceedings of the China Satellite Navigation Conference (CSNC), Shanghai, China, 23-25 May 2017; pp. 69–80.
50. Wang, S.; Liu, H.; Tang, Z.; Ye, B. Binary phase hopping based spreading code authentication technique. *Satell. Navig.* **2021**, *2*, 4. https://doi.org/10.1186/s43020-021-00037-z
51. Yan, T.; Li, T.; Tian, Y.; Wang, Y.; Bian, L.; Meng, Y. Spreading code authentication method for GNSS signals based on chip-level amplitude modulation. *Chin. Space Sci. Technol.* **2023**, *43*, 69–78.

52. Chiara, A.D.; Broi, G.D.; Pozzobon, O.; Sturaro, S.; Caparra, G.; Laurenti, N.; Fidalgo, J.; Odriozola, M.; Lopez, G.M.; Fernandez-Hernandez, I. 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), Portland, OR, USA, 25–29 September 2017; pp. 2106–2116.
53. Chen, Y.; Gao, W.; Chen, X.; Liu, T.; Liu, C.; Su, C.; Lu, J.; Wang, W.; Mu, S. Advances of SBAS authentication technologies. *Satell. Navig.* **2021**, *2*, 12.
54. Anderson, J.; Lo, S.; Neish, A.M.; Walter, T. On SBAS Authentication with OTAR Schemes. In Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2021), St. Louis, MO, USA, 20–24 September 2021.
55. Walter, T.; Anderson, J.H.; Lo, S. SBAS Message Schemes to Support Inline Message Authentication. In Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2021), St. Louis, MO, USA, 20–24 September 2021.
56. Chen, X.; Tian, X.; Luo, R. Design of message authentication based on TESLA protocol for BDSBAS. *J. Beijing Univ. Aeronaut. Astronaut.* **2021**. Available online: https://doi.org/10.13700/j.bh.1001-5965.2021.0669 (accessed on 4 November 2022).
57. Mu, S.L.; Chen, Y.; Liu, T.; Liu, C.; Chen, X. Design of message authentication and OTAR broadcast strategy for BDSBAS. *J. Beijing Univ. Aeronaut. Astronaut.* **2021**, *47*, 1453–1461. (In Chinese)
58. Hirokawa, R.; Fujita, S. A Message Authentication Proposal for Satellite Based Nationwide PPP-RTK Correction Service. In Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2019), Miami, FL, USA, 16–20 September 2019.
59. Fernández-Hernández, I.; Hirokawa, R.; Rijmen, V.; Aikawa, Y. PPP/PPP-RTK Message Authentication. In Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2021), St. Louis, MO, USA, 20–24 September 2021.
60. Cancela, S.; Calle, D.; Arroyo, G. Designing and evaluating next generation of resilience receivers. In Proceedings of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS + 2017, Portland, OR, USA, 25–29 September 2017.
61. European Union. *GALILEO Open Service Navigation Message Authentication (OSNMA) User ICD for the Test Phase*; European Union Issue 1.0, 2021.
62. European Union. *Agency for the Space Programme, GALILEO Open Service Navigation Message Authentication (OSNMA)*; European Union Issue 1.0, 2021.
63. Fernández-Hernández, I.; Winkel, J.; O'Driscoll, C.; Cancela, S.; Terris-Gallego, R.; López-Salcedo, J.A.; Seco-Granados, G.; Chiara, A.D.; Sarto, C.; Blonski, D.; Blas, J.D. Semi-Assisted Signal Authentication for Galileo: Proof of Concept and Results. *IEEE Trans. Aerosp. Electron. Syst.* **2023**. https://doi.org/10.1109/TAES.2023.3243587
64. Hinks, J.; Gillis, J.T.; Shawn, P.L.; Myer, G.; Rushanan, J.J.; Stoyanov, S. Signal and Data Authentication Experiments on NTS-3. In Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2021), St. Louis, MO, USA, 20–24 September 2021; pp. 3621–3641.
65. NIST. *FIPS Pub 186-4: Digital Signature Standard (dss)*; Technical report; Digital Signature Standard (DSS). In National Institute of Standards and Technology, Gaithersburg, MD, USA, 2013.
66. NIST. *Announcing the Advanced Encryption Standard (aes)*; FIPS Standard; Federal Information Processing Standards Publication: 2001; Volume 197, pp. 1–51.Available online: https://doi.org/10.6028/NIST.FIPS.197 (accessed on 30 January 2023).
67. General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China, Information security techniques. *SM2 Elliptic Curve Signature Algorithm, Part 1: General Rules*; Standards Press of China: Beijing, China, 2017.
68. General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China, Information security techniques. *SM2 Elliptic Curve Signature Algorithm, Part 2: Digital signature algorithm*; Standards Press of China: Beijing, China, 2017.
69. General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China, Information security techniques. *SM3 Cryptographic Hash Algorithm GB/T 32905—2016*; Standards Press of China: Beijing, China, 2017.
70. General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China, Information security techniques. *SM4 Block Cipher Algorithm GB/T 32907-2016*; Standards Press of China: Beijing, China, 2017.
71. Fernández-Hernández, I.; Ashur, T.; Rijmen, V. Analysis and Recommendations for MAC and Key Lengths in Delayed Disclosure GNSS Authentication Protocols. *IEEE Trans. Aerosp. Electron. Syst.* **2021**, *57*, 1827–1839.
72. Neish, A.; Walter, T.; Powell, J.D. Design and analysis of a public key infrastructure for SBAS data authentication. *Navigation* **2019**, *66*, 831–844.

73. *BeiDou Navigation Satellite System Signal in Space Interface Control Document Open Service Signal B1C*, Version 1.0; China Satellite Navigation Office 2018.
74. Jia, X.; Su, R.; Liang, W.; Shen, F.; Zheng, C.; Wang, X.; Xu, L. Research on Civil GNSS Signal Authentication Service Design. In *China Satellite Navigation Conference (CSNC 2021) Proceedings*, *Nanchang*, *China*, *2–25 May 2021*; Yang, C., Xie, J. Eds.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2021; Volume 773.