Research on Civil GNSS Signal Authentication Service Design

Xiaomin Jia(✉), Ranran Su, Wentao Liang, Fei Shen, Chong Zheng, Zheng Wang, Xuan Wang, and Linfeng Xu

Beijing Satellite Navigation Center, Beijng, China

Abstract. GNSS authentication enhances the signal with signatures to help users to validate that the received signal is from a reliable source. Over the past years GPS and Galileo has been advancing system level implementation and test towards an operational GNSS authentication enhancement, so as to tackle the rise of spoofing risks that poses increasingly severe threats to civilian user community. Started with a briefing on GNSS authentication technology categories and the authentication services adopted by GPS and Galileo, main design requirements and a performance metric framework of GNSS authentication are presented for practical market application. The paper then puts forward one solution for BDS civil signal authentication based on BDS characteristics, which introduces the TESLA protocol originally used for navigation message authentication (NMA) into the field of spread code authentication (SCA) to reduce communication overhead and allows for fast and independent authentication. The preliminary design and performance analysis of the mechanism on BDS new-generation signals is presented.

Keyword: GNSS authentication · Spoofing · Authentication performance metrics · BDS · Navigation message authentication (NMA) · Spread code authentication (SCA)

1 Introduction

In a GNSS simulator exhibition at the ION GNSS+ 2017 conference held in US, the location and time of cell phones of many attendees were spoofed to somewhere in Europe in Jan. 2014, due to improper termination of the output port [1].

The incident highlights the pressing problems faced by GNSS. First, With the advancement of simulator and SDR, it is becoming trivially easy to spoof a GNSS Receiver. Second, spoofing causes increasingly severe damage due to the rapid popularization of smart devices which use GNSS-based PNT services. Moreover, benefit drivers behind spoofing are strengthening. Secure PNT is critical to safety-of-Life applications, critical infrastructure, financial applications, etc. [2].

GNSS authentication for open signal has been proposed and studied in literature [2–9] as a system-level anti-spoofing enhancement, which improves the security of GNSS services by adding extra cryptographic signatures or marks to signals. In recent

C. Yang and J. Xie (Eds.): *China Satellite Navigation Conference (CSNC 2021) Proceedings*, LNEE 773, pp. 208–218, 2021.
https://doi.org/10.1007/978-981-16-3142-9_19

years, GPS, Galileo, and ICAO have accelerated development and test of civil GNSS authentication to provide secure civil PNT services.

This paper presents an analysis and characterization of design considerations and performance metrics of GNSS authentication. The paper then proposes a BDS civil GNSS authentication scheme based on BDS signal features, and details the design concepts, authentication protocol and message structure, then gives a preliminary performance analysis.

2 Technical and Service Perspective

GNSS authentication mainly applies at data and spreading code level, and can be distinguished into three categories, Navigation Message Authentication (NMA), Spreading Code Authentication (SCA) and the combination of SCA and NMA [2].

GNSS authentication [2, 8] is introduced to achieve signal origin authentication, signal integrity authentication, as well as a certain level of resistance to replay attacks. Replay attacks lead to errors of measurements and thus wrong PNT resolution. GNSS authentication can increase the unpredictability of signal [8, 9], thus preventing some types of replay attacks. NMA facilitates authentication of both the origin and integrity of data by adding signatures or MACs to the navigation data [2]. It can achieve a certain level of symbol unpredictability [3, 10, 11], but is still vulnerable to some replay attacks [9]. SCA replaces part of spreading code stream with cryptographically generated chips (hereafter "auth chips") for origin authentication. It better tackles replay attacks [3], because spreading code operates at a higher chip rate and is hidden under thermal noise. It is difficult to estimate the auth chips and replay. SCA also provides more fine-grained signal unpredictability.

GPS plans to carry out SIS test of L1C authentication mechanism Chimera in NTS-3 program [12, 13]. L1C Chimera uses a combination of NMA and SCA. $L1C_D$ introduces digital signatures to the data, and $L1C_P$ inserts auth chips into the spreading code. Chimera has two variations, "slow channel" and "fast channel". In "slow channel", keys used to generate auth chips are derived from $L1C_D$ digital signatures, with an authentication period of 3 min. While in "fast channel", keys are generated by a dedicated key infrastructure and delivered to users through an external channel [5, 13], with an authentication period of 3 or 6 s.

Galileo provides OSNMA and CAS for Open Service and Commercial Service, respectively. OSNMA is expected to be operational in 2021 [14]. CAS is expected to provide initial service in 2021–2022 [15]. OSNMA applies NMA to E1B message, and use an authentication protocol based on Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol, adapted to Galileo [4]. About 40 bits per odd page are used to broadcast OSNMA message, with an effective data rate of 20 bps. CAS is based on Spreading code Encryption (SCE) [15], using a mechanism similar to SAS [9], which encrypts the pilot signal E6C and broadcasts the E6C spreading code verification sequence in a dedicated field of E6B data.

3 Design Considerations

Main design considerations for civil GNSS authentication include [2, 5, 6, 8, 15]:

1. Openness. Cryptography used should maintain the openness of the PNT service, as well as a public key distribution. Users need not to store private keys.
2. Backward compatibility. Users uninterested should not be affected.
3. Navigation performance. Authentication used should have no or minimum impact on the performance of navigation services in any environment.
4. Adaption to navigation signals. GNSS SIS is high-noise, low-bandwidth, one-way channel with high data error rate (BER) [2]. Feasible authentication calls for low communication overhead and adaption to those channel conditions.
5. Security. Cryptography used should be sufficient to prevent prediction or forging of messages or signals, providing information or signal unpredictability to deal with replay attacks, ensuring security for one to several decades.
6. Scalability. The authentication mechanism should support multiple configurations, with scalability to system upgrades and increasing security threats.
7. Receiver overhead. Allow receivers to quickly complete authentication and issue alarms, with low storage and computation overhead and minimized security requirements, avoiding storage of private keys.
8. Independence. Authentication should be able to work independently based on space signals, supporting standalone or low-end users.
9. System implementation. Careful balancing of the constraints and capability of SIS, satellite and ground facilities is needed to make changes to data or code.

4 Performance Metrics Framework

A GNSS authentication service should provide users with secure PNT while maintaining navigation performance. Therefore, performance metrics need to measures both the navigation performance and security of real-time authentication.

Table 1 shows the performance metric framework and their impacting factors [5, 6, 8]. Figure 1 depicts the relationship between performance metrics. This section expands the analysis of NMA metrics on the basis of literature [8], adding SCA-related performance metrics and analysis.

4.1 Navigation Performance Metrics

The main navigation performance metrics examined are Accuracy, Availability and Time to First Authenticated Fix (TTFAF) when authentication is used by users [6]. SCA causes a certain level of spreading code correlation power loss to the users and the degree of loss can be examined with the Correlation Loss metric [5].

Table 1. Performance metrics and authentication schemes

Type	Metric	NMA	SCA
Navigation Performance metrics	$Accuracy_{Auth}$	$UERE_{Auth}$: Authenticated navigation data less than total navigation data or an older version of navigation data is used for authentication DOP_{Auth}: User has more troubles receiving authentication data than standard data, satellites authenticated in view less than satellites in view	$UERE_{Auth}$: SCA brings correlation loss, impacting measurements under high-noise environments DOP_{Auth}: Correlation loss impacts signal reception under certain environments or satellites authenticated in view less than satellites in view
	$Availability_{Auth}$	User has more troubles receiving authentication data than standard data, satellites authenticated in view less than satellites in view	Correlation loss impacts signal reception under certain environments or satellites authenticated in view less than satellites in view
	TTFAF	Time to receive authenticated data longer than that of standard data	Time to receive all auth chips for one authentication
	L_{corr}	–	DF
Authentication metrics	AER	Number of bits of authenticated data and authentication data, system BER	Number of chips and data bits generated or used in authentication calculation
	TBA	Depends on authentication mechanism, impacted by data rate and message structure	
Critical design parameters	DF	–	Depends on authentication mechanism, should be configurable
	NNA	= Number of bits of authenticated and authentication data, impacted by authentication mechanisms, should be configurable	–

(*continued*)

Table 1. (*continued*)

Type	Metric	NMA	SCA
Security metrics	SKS	Determined by authentication mechanism and cryptography used	Determined by authentication mechanism and cryptography used
	MPT	Determined by authentication mechanism, impacted by data rate and message structure	Determined by authentication mechanism, impacted by insertion rule
	USR		–
	DF	–	Depends on authentication mechanism, should be configurable

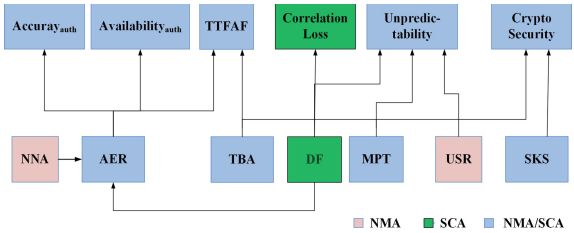

Fig. 1. Performance metrics and their relevance

1) $Accuracy_{Auth}$: the user position accuracy when only the authenticated signals are used. Can be approximated by the following formula.

$$Accuracy_{Auth}[m] = UERE_{Auth}[m] * DOP_{Auth} \tag{1}$$

2) $Availability_{Auth}$: the percentage of time that the user can correctly receive at least 4 authenticated satellite signals in a specific environment.

When the number of authenticated satellite signals that a receiver can receive under any conditions or the authenticated part (data or spreading code) of the signal is inconsistent with the standard service, the accuracy or availability of the service will be affected. For NMA, a successful authentication requires the receiver to correctly receive both the authenticated data and the authentication data (after data decoding and error correction). While for SCA, it requires the received authentication spreading code chips errorless or correlation passed (depending on the verification rule), these requirements also affect the accuracy and availability.

2) TTFAF: the time taken by a receiver to complete the first position fix using the authentication signals of at least 4 satellites. System TTFAF can be approximated

statistically. Whereas user TTFAF depends on which time slot the SIS is at out of the authentication period when the receiver is started and the length of the authentication period.

3) Correlation loss: the correlation power loss caused by insertion of auth chips to the spreading code, and depends on the auth chips insertion rule and proportion (denoted by Duty Factor, DF). Literature [16] gives the formula of the average correlation loss L_{corr} when puncture is used for insertion. DF is described below.

$$L_{corr}(dB) = 20 * log_{10}[1 - DF] \tag{2}$$

4.2 Authentication Metrics

To examine the impact of authentication solutions on navigation service performance and security, literature [8] proposed two authentication performance metrics, Authentication Error Rate (AER) and Time Between Authentications (TBA).

1. AER: refers to the error probability of the authentication signal under no attack. For NMA, AER [5] mainly depends on the number of bits of data participating in authentication (including the authenticated and authentication data) in a single authentication period and the system BER. Literature [8] gives AER calculation formula for NMA. NNA is the total number of bits participating in authentication. For SCA, AER mainly considers the impact of spreading code verification, and is determined by the chip error rate and the verification rule used. If a chip-by-chip comparison verification is used, AER calculation is similar to NMA. If the correlation adjudication is used for verification, AER will be relatively small.

$$AER = 1 - (1 - BER)^{NNA} \tag{3}$$

   For a combined use of NMA and SCA, AER calculation requires a more rigorous modelling that takes the relationship between the two-level working flow into account, which is left to later work.
2. TBA: refers to the time interval for a single signal to complete two consecutive authentications. TBA depends on authentication solution.

4.3 Security Metrics

Security metrics consider cryptographic security and resistance against replay attacks. Signal unpredictability helps to improve detection of replay attacks. MPT [8], USR [8] and DF can be used to examine signal unpredictability of a solution.

1. Symmetric key strength (SKS): represents the equivalent symmetric key length that the authentication cryptography can provide, expressed in bits [5, 8].
2. Maximum Predictable Time (MPT): refers to the maximum predictable time that the signal is transmitted.

3. Unpredictable Symbol Rate (USR): represents the proportion of unpredictable symbols, for NMA solutions.
4. DF: DF is proposed in [5] to measure correlation loss. We propose the use of DF to measure the proportion of unpredictable chips for SCA solutions as well.

(MPT, USR) or (MPT, DF) can simultaneously examine the proportion and distribution of unpredictability of a signal for NMA or SCA solutions.

5 Preliminary Design of an Authentication Proposal for BDS

This section proposes a preliminary design of an authentication mechanism for BDS civil signal BDSSA (BDS Signal Authentication).

Among BDS new generation civil signals [17–23], The B1C, B2a, and B2b-I (MEO/IGSO satellites) signals provide global open service, and the BDSBAS-B1C and BDSBAS-B2a signals provide regional SBAS service, while the PPP-B2b-I and PPP-b2b-Q signals are used for regional PPP service.

For open service, B1C is the primary signal, authenticating B1C may serve more users. However, B2a has a higher data rate, allowing for a smaller TBA. Moreover, users who need authentication generally are high-end users, who either already support B2a or are not sensitive to the cost of adding it. We characterize both signals for a thorough analysis and comparison. For SBAS service, ICAO is formulating a data authentication mechanism [24], which BDSBAS-B1C authentication will follow with. For PPP service, this paper characterizes PPP-B2b-I.

5.1 BDSSA Design Features

Based on the above analysis, BDSSA mainly adopts the following principles.

1. Bit Commitment.

To sustain the openness of civil service to allow for broader usage of authentication and backward compatibility, and to make sure receivers need not to store private keys or implement private algorithms, the cryptography adopted should be public, supporting public key distribution [3–6].

Bit commitment (or delayed key transmitting) algorithms transmit the cipher text first, and then send the key after a certain delay, which guarantees the security of key before the cipher text is received. Security is realized by keeping a certain time interval between cipher text and key transmission to prevent forging of the signal [5, 13]. In this way, bit commitment algorithms achieve publicity and public distribution of keys. GPS Chimera [5] and Galileo OSNMA [4] both leverage bit commitment principle. In addition, the bandwidth requirement of bit commitment algorithms is much less than that of digital signature algorithms, thereby reducing NNA and TBA. OSNMA reduces the communication bandwidth requirements significantly by using and adaption of a bit commitment algorithm TESLA [4].

2. One-way key chain

BDSSA adopts a one-way function to generate the key chain for authentication generation, thus keys distributed can be verified by the one-way function, further reducing the meta-information required for key transmission while improving security. One-way function has the feature that the next variable can be calculated quickly through the current variable, but the computational complexity of inverse calculation of the current variable through the next variable is extremely high [8].

3. Time liaison

The BDS system time is introduced into the BDSSA authentication calculation to further improve cryptography security and prevent pre-computing attacks.

5.2 BDSSA Protocol

BDSSA authenticates the spreading code. BDSSA employs the design concept of TESLA protocol [4], which is only used for data authentication, into the spreading code authentication domain, using bit commitment to facilitate security while reducing communication overhead of transmitting keys, especially through SIS. An independent SCA mechanism relying only on BDS SIS is achieved and TBA is reduced as much as possible at the same time.

In order to increase successful verification rate under high-noise conditions, BDSSA adopts a one-keychain-for-all-satellite design feature similar to OSNMA [4], in which all satellites use keys from one single key chain. In a given authentication period, different satellites use consecutive keys in the order of PRN numbers. Receivers only need to receive one key broadcast on one satellite to complete verification of the auth chips of all satellites in view. The single key chain significantly reduces the key verification overhead, while reducing AER [4].

For the independent use of the authentication service by standalone receivers, the BDSSA key is broadcast through navigation data. For receivers that support external channels such as 5G, an A-BDSSA variation of BDSSA can be enforced, in which BDSSA key is distributed through a high-speed external channel, significantly reducing TBA and improving the ability to prevent replay attacks.

5.3 BDSSA Message Structure

The B1C signal B-CNAV1 subframe 3 allows for definition of new page types, each page containing 234 bits. The B2a and PPP-B2b-I supports definition of new message types, each containing 234 bits and 456 bits, respectively.

The BDSSA message type is structured as shown in Fig. 2. Each BDSSA page contains two fields, KROOT and ASK. KROOT is used to broadcast the root key of the key chain and configuration parameters. KROOT data is broadcast in multiple pages. PNUM represents the total number of pages (denoted as packages) used for KROOT data, PIDX represents the package index, and OPType indicates the type of data distributed in the KDATA domain. KDATA domain distributes the root key and its digital signatures,

or the configuration parameters, etc. Configuration parameters include key length, DF, code insertion rules, etc. ASK is used to broadcast keys, and 1–4 keys can be broadcast according to the configuration of cryptographic parameters. B1C and B2a supports a key length of 98–196 bits, and PPP-B2b-I supports a key length of 98–394 bits.

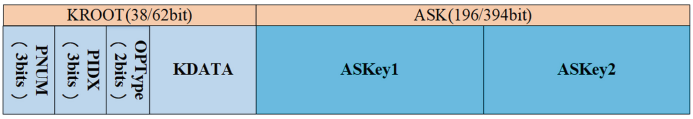

Fig. 2. BDSSA message structure

5.4 Preliminary Performance Analysis

This section gives a preliminary analysis of main performance metrics of BDSSA on B1C, B2a, and PPP-B2b-I. Two key length configurations are used, 98 and 196 bits, respectively. The preliminary results of some metrics are shown in Table 2.

Table 2. Preliminary performance analysis

Metric	SKS = 98			SKS = 196		
	B1C	B2a	PPP-B2b-I	B1C	B2a	PPP-B2b-I
TBA	≥90 s	≥15 s	≥8 s	≥90 s	≥15 s	≥8 s
AER	See analysis					
DF	Configurable, depending on the distribution and DF of auth chips					
MPT	Configurable, depending on the distribution and DF of auth chips					
USR	≤5.2%	≤15.6%	≤11.4%	≤5.2%	≤15.6%	≤11.4%

Constrained by signal message structure, BDSSA message works as independent pages or messages, and cannot be evenly distributed across pages/messages. Therefore, TBA depends on the fastest repetition period of the page/message type. Within one single page/message, reducing key length (SKS) is beneficial to reducing the system and receiver implementation overhead, but does not improve TBA.

AER depends on the number of auth chips inserted in a single authentication period and the number of authentication data bits. The number of authentication data bits in one BDSSA authentication period is a constant value (234 or 456). The number of auth chips depends on the DF. A smaller DF Helps to reduce AER. The accurate AER calculation needs careful treatment of both the influence of the message and the spreading code at the same time.

6 Conclusion

It is of great significance for BDS to provide security enhancement for civilian services. This paper carefully analyzes the design considerations of civil GNSS authentication for both NMA and SCA, and a performance metric framework including navigation performance metrics, security metrics and authentication performance metrics is constructed.

This paper then presents a preliminary BDSSA authentication mechanism for the new generation BDS civil signals, and a preliminary performance analysis is shown. Analysis shows that through the use of bit commitment, one-way function, and time liaison, BDSSA can significantly reduce communication overhead while enforcing authentication. Independent use of B1C, B2a and PPP-B2b-I can achieve a TBA of 90s\15s\8s, respectively, which is sufficient to provide a certain level of anti-replay capability for critical infrastructure or financial applications.

Further research is needed for careful tuning of BDSSA design, system & receiver implementation and verification based on simulation.

References

1. O'Driscoll, C.: What is navigation message authentication? InsideGNSS, Jan/Feb, pp. 26–31 (2018)
2. Wullems, C., Pozzobon, O., Kubik, K.: Signal authentication and integrity schemes for next generation global navigation satellite systems. European Navigation Conference GNSS, Munich, Germany (2005)
3. Scott, L.: Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems. ION GNSS, Portland, OR, pp. 1543–1552 (2003)
4. Fernández-Hernández, I., Rijmen, V., Seco-Granados, G., Simón, J., Rodríguez, I., Calle, J.D.: A navigation message authentication proposal for the galileo open service NAVIGATION. J. Inst. Navigation **63**(1), 85–102 (2016)
5. 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: 30th ION GNSS+, Portland, Oregon, pp. 2388–2416 (2017)
6. 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. ION GNSS+ 2014, Tampa, FL, pp. 2810–2827 (2014)
7. Wang, S., Liu, H., Tang, Z., Ye, B.: Binary phase hopping based spreading code authentication technique. Satellite Navigation **2**(1), 1–9 (2021). https://doi.org/10.1186/s43020-021-00037-z
8. Fernández-Hernández, I.: GNSS Authentication: Design Parameters and Service Concepts. European Navigation Conference, Rotterdam, Netherlands (2014)
9. Pozzobon, O.: Keeping the spoofs out – Signal Authentication Services for future GNSS. InsideGNSS **May/June**(2011), 48–55 (2011)
10. Cancela, S., Navarro, J., Calle, D., Reithmaier, T., Dalla Chiara, A., Da Broi, G., Fernández-Hernández, I., Seco-Granados, G., Simón, J.: Field testing of GNSS user protection techniques. In: 32nd ION GNSS+ 2019, Miami, Florida, pp. 1824–1840 (2019)
11. O'Driscoll, C., Fernández-Hernández, I.: Mapping bit to symbol unpredictability in convolutionally encoded messages with checksums, with application to galileo OSNMA. In: 33rd ION GNSS+:3738–3750 (2020)

12. Way, Way Out in Front- Navigation Technology Satellite-3: The Vanguard for Space-Based PNT. https://insidegnss.com/way-way-out-in-front-navigation-technology-satellite-3-the-vanguard-for-space-based-pnt/. 28 June 2020
13. Cameron, A.: AFRL tests Chimera to battle spoofers and hackers. https://www.gpsworld.com/afrl-tests-chimera-to-battle-spoofers-and-hackers/. 24 July 2019
14. Galileo Open Service Navigation Message Authentication Is Available for Testing. https://insidegnss.com/galileo-open-service-navigation-message-authentication-is-available-for-testing/. 1 Dec 2020
15. Fernandez-Hernandez, I., Vecchione, G., Díaz-Pulido, F.: Galileo authentication: a programme and policy perspective. In: 69th International Astronautical Congress, Bremen, Germany:IAC-18.B2.4.1 (2018)
16. Scott, L.: Proving Location Using GPS Location Signatures: Why it is Needed and A Way to Do It. (ION GNSS+ 2013), Nashville, TN (2013)
17. BeiDou Navigation Satellite System Signal In Space Interface Control Document Open Service Signal B1C (1.0). http://www.beidou.gov.cn/xt/gfxz/201712/P020171226741342013031.pdf. 22 December 2020
18. BeiDou Navigation Satellite System Signal In Space Interface Control Document Open Service Signal B2a (1.0). http://www.beidou.gov.cn/xt/gfxz/201712/P020171226742357364174.pdf. 22 December 2020
19. BeiDou Navigation Satellite System Signal In Space Interface Control Document Open Service Signal B2b(1.0) .http://www.beidou.gov.cn/xt/gfxz/202008/P020200803362059116442.pdf. 22 December 2020
20. BeiDou Navigation Satellite System Signal In Space Interface Control Document Precise Point Positioning Service Signal PPP-B2b(1.0). http://www.beidou.gov.cn/xt/gfxz/202008/P020200803362062482940.pdf. 22 Dec 2020
21. BDSBAS-B1C. BeiDou Navigation Satellite System Signal In Space Interface Control Document Satellite Based Augmentation System Service Signal BDSBAS-B1C (1.0). http://www.beidou.gov.cn/xt/gfxz/202008/P020200803362065480963.pdf. 22 December 2020
22. Du, Y., Wang, J., Rizos, C., El-Mowafy, A.: Vulnerabilities and integrity of precise point positioning for intelligent transport systems: overview and analysis. Satellite Navigation **2**(1), 1–22 (2021). https://doi.org/10.1186/s43020-020-00034-8
23. Lu, J., Guo, X., Su, C.: Global capabilities of BeiDou Navigation Satellite System. Satellite Navigation **1**(1), 1–5 (2020). https://doi.org/10.1186/s43020-020-00025-9
24. Neish, A., Walter, T.: Securing GNSS – A Trip Down Cryptography Lane (2020). https://insidegnss.com/securing-gnss-a-trip-down-cryptography-lane/. 20 May 2020