Yuan *et al. Satellite Navigation* (2023) 4:6
https://doi.org/10.1186/s43020-023-00094-6

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

REVIEW

Open Access

Authenticating GNSS civilian signals: a survey

Muzi Yuan, Xiaomei Tang* and Gang Ou

Abstract

Civilian services of Global Navigation Satellite System are threatened by spoofing attacks since it is hard to determine the authenticity of a navigation signal with a detailed structure open to the public. Signal authentication effectively protects the security of the signal by attaching unforgeable information to one or several elements of the signal. Receivers can verify the authenticity of the signal by extracting and validating this information. Developing good signal authentication schemes requires understanding possible spoofing modes, signal element specialty, and performance evaluation methods. This paper is an overview of navigation signal authentication, where the theories and reported approaches are described in detail. A design/performance matrix that demonstrates the advantages and defects of the signal element and its authentication design is summarized. Recommendations are proposed to improve the robustness, security, efficiency, and implementation hardness for future designs of navigation signal authentication.

Keywords GNSS spoofing, Signal authentication, Signal structure design, Authentication scheme

Introduction

Civilian Global Navigation Satellite System (GNSS) signals are broadcasted with a detailed structure open to the public and processed passively in receivers. While this feature makes satellite navigation an open service with unlimited user capacity, it also brings the threats of spoofing attacks by allowing the construction of counterfeit signals. One of the main threats of civilian GNSS services is spoofing attacks by broadcasting counterfeit navigation signals. Victim receivers without detection capability will process the counterfeit signals as authentic (Psiaki and Humphreys, 2016). Spoofing attackers will manipulate the position and timing outputs of victim receivers through the forged spreading code phase and navigation message in the counterfeit signals. Since power grid, financial industries, vehicle autopilots, civil aviation, and other civilian infrastructures and life safety applications rely on credible position and timing information, these spoofing attacks could severely threaten their security and robustness. Several examples of spoofing attacks against civilian GNSS services were reported in both laboratory and field, such as spoofing against commercial off-the-shelf receivers (Humphreys et al., 2008), an unplanned dive in an Unmanned Aviation Vehicle (UAV) (Kerns et al., 2014), and misleads of yachts in the Black Sea (Bhatti and Humphreys, 2017). Hence, protecting receivers from spoofing attacks is a significant measure to improve the robustness and security of civilian GNSS services.

Spoofing protection aims to detect a spoofing signal, alert the receiver of a spoofing attack, and maintain creditable position and timing fixes as far as possible. Spoofing protecting approaches can be categorized as cryptographic defenses and non-cryptographic defenses. The former may require some modification in signal structure or communication links, while the latter does not. Non-cryptographic defenses use physical manifestations such as received power monitoring (Akos, 2012),

*Correspondence:
Xiaomei Tang
txm_nnc@126.com
School of Electronic Science, National University of Defense Technology, Changsha, China

Direction of Arrival (DOA) (Borio and Gioia, 2016), signal polarization (De Wilde et al., 2018), or Receiver Autonomous Integrity Monitoring (RAIM) (Blanch et al., 2010; Wang et al., 2016) to determine if the processing signal is authentic or counterfeit. Cryptographic defenses use cryptographic algorithms to conceal part of the information in signal generation, which is ready to be validated and infeasible to be forged. These two categories of defenses are both used in detecting different types of spoofing attacks, which can be categorized as meaconing, Security Code Estimation And Replay (SCER) (Humphreys, 2013), and synthesizing.

Meaconing attackers use the repeaters to receive and retransmit the whole spectrum of authentic signals (Coulon et al., 2020). Since all information in meaconing attack signals is the same as authentic signals, this type of spoofing has the potential to compromise all GNSS signals, including encrypted military signals. However, there are unignorable delays to authentic signals in meaconing signals, which enable receivers to detect this type of spoofing and recover the original signal by sensing the existence of multiple peaks in correlation results and selecting the signal with the most leading phase in the spreading code. SCER attackers first receive the authentic signals and estimate the unpredictable information, then regenerate the counterfeit signal from a manipulated message and this unpredictable information (Humphreys, 2013). Suppose attackers can get reliable estimations before the unpredictable symbol finishes broadcasting. In that case, it is possible to forge a counterfeit signal with accurate unpredictable information and a leading phase in the spreading code compared to authentic signals. In this case, cryptographic defenses with high estimation difficulty and a short estimation period are needed to protect the authentic signals. Synthesizing attackers build spoofing signals from the available details of signal structure in Interface Control Documents (ICDs) without receiving any original signal. All information in the spoofing signal can be manipulated except encrypted unpredictable elements. Cryptographic defenses can provide significantly adequate protection against this type of attack.

Several surveys introduced the principles and technologies in GNSS spoofing and detection (Broumandan et al., 2017; Gunther, 2014; Psiaki and Humphreys, 2016, 2021; Schielin et al., 2012; Scott, 2013). These works mainly concentrate on non-cryptographic defenses and only make a general and brief description of cryptographic defenses. Other reviews were written earlier (Margaria et al., 2017), and now researchers have developed new navigation signal authentication schemes based on encryption and signal structure. Since signal authentication is already under implementation in Global Positioning System (GPS) and Galileo navigation satellite system (Galileo), it is necessary to understand cryptographic-based authentication approaches in detail. This paper makes three principal contributions to navigation signal authentication. First, the fundamental theories and key performance indicators in authenticable signal design are described in detail. The second contribution is a survey of reported approaches and implementations of navigation signal authentication, described in a moderate detail. Besides, the performance of different authentication implementations is assessed to offer a convenient reference for signal designers, based on which recommendations are proposed to improve the robustness, security, efficiency, and implementation hardness for future designs of navigation signal authentication.

The remainder of this paper consists of three main sections plus a work summary. In "Navigation signal authentication: theory" section introduces the fundamental theories in authenticable signal design and provides its Key Performance Indicator (KPI) systems with the methods to evaluate them. In "Cryptographic-based authentication schemes" section overviews navigation signal authentication approaches under implementation or consideration. In "Performance comparison and trends" section compares authentication approaches in a design/performance matrix. The parameters of the approaches under implementation are chosen by documents proposing them. Other approaches under consideration are evaluated with the typical parameters for corresponding civilian signals. Besides, several suggestions on the possible paths for improving performance are proposed. In "Conclusion" section summarizes the contributions of this paper and gives its conclusions.

Navigation signal authentication: theory

The fundamental theory of cryptographic-based GNSS signal authentication is the design and detection of a bunch of unpredictable symbols. In order to detect the origin of a GNSS signal through authentication schemes, unforgeable information is attached to one or several elements of the authenticable signal. This unforgeable information is marked as a security code. There are two critical points in the construction of an authenticable GNSS signal. One is securing the generation of the security code and giving receivers the capability to verify them. The other is elaborately selecting the signal elements, which will be used to carry the authentication message, and designing the methods to attach the authentication message for satellites and extract them from the authentic signal for receivers. Besides, performance indicator systems are also important in the design and will be introduced in this section to enable the assessment and comparison of different authentication approaches.

Security code: generation and validation

The security code is part of the information carried by the navigation signal, which is easy to be validated but hard to be forged. The security codes are usually generated from cryptographic algorithms along with secret keys. Receivers will need prior knowledge such as the corresponding public keys or the same secret keys to validate these security codes. Cryptographic algorithms used to generate the authentication messages can be mainly categorized into three types: symmetric cipher, asymmetric cipher, and cryptographic hash. Each of them has features fit for different authentication scenarios.

Symmetric cipher algorithms use the same secret key to generate and verify the authentication message. This category of algorithms consists of block cipher algorithms (e.g., AES (Daemen and Rijmen, 2002), SM4 (SAC, 2016b)) and stream cipher algorithms (e.g., A5 (Jensen and Andersen, 2017), ZUC (Mukherjee et al., 2021)). Spreading code used in civilian GNSS signals can be regarded as a simple stream cipher (encrypted by linear feedback shift registers) with an open key. *Asymmetric cipher algorithms* use secret private keys to generate authentication messages and open public keys to verify them. Authentication messages generated from these algorithms are often called digital signatures since they are easy to sign but hard to be forged, like those signatures in real life. Elliptic Curve Digital Signature Algorithm (ECDSA) (Johnson et al., 2001) and SM2 (SAC, 2017) are the examples of standard asymmetric algorithms for authentication message generation. *Cryptographic hash algorithms* are a class of one-way functions (e.g., SHA-2 (Dang, 2015), SM3 (SAC, 2016a)) that are easy to calculate in the forward direction while infeasible to calculate reversely. Since the output of cryptographic hash algorithms can be arbitrarily truncated while maintaining the capability of verification, the bit length of the authentication message is flexible and may achieve higher efficiency.

To enable receivers to validate the authentication message, prior knowledge needs to be transmitted to receivers through various methods. An ordinary solution is establishing an encrypted channel between receivers and the distribution center. Then, secret keys are transmitted securely through this channel. Secret keys to generate encrypted military GNSS signals are distributed by this method. Unlike symmetric cipher, digital signatures signed by private keys can be validated via public keys. The public keys of asymmetric ciphers can be publicly unveiled, while the private keys are kept secret. Since asymmetric cipher approaches require no secure channel to maintain validation capability, they are often used to build the fundamental trust infrastructure.

In practice, the symmetric cipher is still required to improve efficiency when the secret channel is absent. In these scenarios, the secure distribution of secret keys to validate symmetric cipher or cryptographic hash messages through an open broadcast channel is often implemented with the help of delayed disclosure. A practical approach is Timed Efficient Stream Loss-Tolerant Authentication (TESLA) (Perrig et al., 2005), which generates a chain of secret keys through a one-way function such as cryptographic hash algorithms and uses them in reversed order. Figure 1 demonstrates the generation and the revealing of the chain. In the initiation process, K_0 will be revealed first as the validation root of the protocol. Receivers can easily verify the authenticity of the key by repeatedly applying a one-way function to this key and checking if the result equals the verification root.

Here generation root K_N is randomly and secretly chosen as the beginning of the chain. A one-way function $F_{\mathrm{ow}}(x)$ is applied repeatedly to the root K_N to generate keys so that the output of the last one-way function is the input of the following one-way function. Then, the tail of the chain K_0 is revealed as the validation root, and other keys will be revealed in the opposite order of generation. In practice, the authentication message of a segment of the navigation signal will be generated through a key in the TESLA chain, and this key will be transmitted in the navigation signal in the next segment. Receivers can validate the key and then validate the signal through this TESLA protocol (Becker et al., 2009).

Besides TESLA-liked approaches to distribute prior knowledge for authentication capability, key-distribution-based structures are also used in military or commercial GNSS services. Many group key management schemes are capable of the distribution of prior knowledge. These schemes are categorized into three types: centralized key management, decentralized group key management, and distributed group key management. *Centralized key management* schemes are governed by a single or multiple key management centers to distribute keys to users. Layered trees are often utilized to simplify the complexity and reduce the communication cost of these schemes. Logical Key Hierarchy (LKH) (Pande and Thool, 2016) is a typical scheme of this category. *Decentralized group key management* schemes and *distributed*

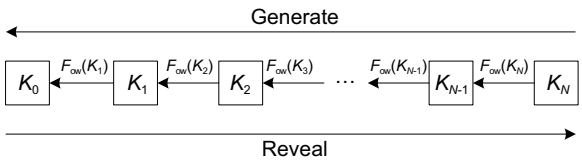

Fig. 1 Generating and revealing order of a typical one-way chain in TESLA protocol

group key management schemes reduce the computation and communication stress for center management by splitting users into different groups or making users generate keys through key-agreement algorithms such as Elliptic Curve Diffie-Hellman (ECDH) (Mohan Naik et al., 2020). In the GNSS scenario, centralized key management is the most suitable for key distribution. At the same time, the commercial service of Galileo Public Regulated Service (PRS) develops a centralized key management scheme for its distribution of spreading code keys (Turner et al., 2015), and the layered structure key management is proposed for open service authentication (Caparra et al., 2017).

When prior knowledge is successfully distributed, authentication messages can be derived or validated by cryptographic algorithms through these keys. Authentication messages derived through symmetric cipher or cryptographic hash are often called Message Authentication Codes (MACs), while others derived from asymmetric cipher are often called Digital Signatures (DSs).

Signal elements for authentication

Signal elements for authentication are the features of navigation signals that can carry authentication messages and be extracted by receivers using various approaches. A typical navigation signal set with the homologous clock in a Direct Sequence Spread Spectrum (DSSS) system can be modeled as Equation:

$$s(t) = \sum_{i=1}^{N_c} \sqrt{P_i(t)} D_i(t) C_i(t) f_{\mathrm{Sub}}^i(t) \exp \mathrm{j}[2\pi f_i(t) + \varphi_i(t)] \tag{1}$$

where $\mathrm{j} = \sqrt{-1}$ is the imaginary unit, N_c is the number of GNSS signal components in the set, $P_i(t)$ is signal power, $D_i(t)$ is the ± 1 navigation message, $C_i(t)$ is the ± 1 spreading code, $f_{\mathrm{Sub}}^i(t)$ is the subcarrier whose period's integer multiple equals to the chip width of the spreading code, $f_i(t)$ is the carrier frequency and $\varphi_i(t)$ is the phase of carrier.

Signal power $P_i(t)$ is mainly extracted through the Automatic Gain Control (AGC) module in the Radio Frequency (RF) front-end or C/N_0 estimation in the signal tracking loop. Besides, a fast but less robust extraction can also be done by observing the correlation value in the tracking loop. Authentication messages can be carried in the absolute or relative fluctuation in signal amplitude. Since the received signal power is relatively weak (such as -159 dB·W in B1C (SAC, 2020)), additional measures may be made to acquire a precise power estimation.

Navigation message $D_i(t)$ is extracted in a tracking loop and acquired through the demodulation and decode process. With the help of a low message rate (e.g., 100 Symbols Per Second (SPS) with 1/2 encoding in B1C (SAC, 2020)), the extraction precision of navigation message is relatively high, providing an advantage of robustness. However, since attackers will also have a relatively long estimation time window, this low rate of the unpredictable symbol also brings the threat of the SCER attack.

Spreading code $C_i(t)$ is mainly extracted through acquisition, pull-in, and tracking loops through code correlation. The results of extraction are often indicated in correlation power or hypothesis testing of the existence of a specific code serial. Security codes can be carried in spreading code by modifying the chips of periodical civilian spreading codes. The spreading code benefits from the high symbol rate of spreading codes and the relatively low power of navigation signals. It is difficult for attackers to construct SCER attacks against the security codes carried by spreading codes. However, at the same time, this feature also makes it difficult for authenticated users to demodulate the spreading code sequence directly. It needs to be indirectly observed through correlation operations, which sometimes brings about the need for key management and increases the complexity of the authentication scheme.

Subcarrier $f_{\mathrm{Sub}}^i(t)$ exists in split spectrum modulation such as Binary Offset Carrier (BOC) modulation and can be extracted by spectrum domain analysis or subcarrier tracking loop. As an element for authentication, the subcarrier has the features similar to spreading code and carrier.

Carrier frequency $f_i(t)$ and *carrier phase* $\varphi_i(t)$ are both extracted through pull-in or tracking process. Since the dynamic of receivers along with the security code also influences these two elements, further processes may be used to achieve a precise extraction. Another design point needs intention in utilizing carrier frequency and phase as authentication elements. A random bias may be introduced into the velocity measurement based on Doppler frequency observation because of the presence of security code modulated onto the frequency. Generally, to ensure the signal's consistency, if the security code impacts the carrier frequency, this impact will be transmitted to the relevant signal elements, such as the spreading code rate and the message rate. Considering the significant difference in the carrier frequency and the spreading code rate, the change in the spreading code rate and the message rate is usually tiny for the slight disturbance of the carrier frequency.

Signal time t can also be an element in constructing authentication, such as the Selective Availability (SA) technique (Swider et al., 2000) in past GPS. By introducing a tiny jitter in the clock frequency of the satellite, all elements in the GNSS signals will be influenced. If the

influence can be detected and authenticated, then the authenticity of the GNSS signal can be checked.

Authentication detection

There are two levels of the detection of navigation signal authentication: presence detection and authenticity validation. *Presence detection* is detecting whether the security code or the features carrying the security code are present in the GNSS signal's target elements. *Authenticity validation* requires the demodulation and extraction of the security code. Furthermore, it validates whether the cryptographic consistency is satisfied with the trust foundation.

Navigation Message Authentication (NMA) and Spreading Code Authentication (SCA) are different authentication schemes, and different terms are used to describe their authentication processes. The SCA scenario has a presence detection. However, the NMA scenario has an authenticity validation. The mainstream signal authentication methods use these two authentication processes, which can be called the authentication detection process.

Presence detection

The fundamental structure of the presence detection is the detector $f_d\left(r(n), K_p\right)$ designed for the signal elements involved in the authentication. This detector is a function with received samples $r(n)$ and prior knowledge K_p as input and detection observation as output. The authentication detection framework can be constructed through the detection theory since the probability density distribution of detector output differs when the security is present and absent.

Generally, the GNSS signal can be modeled as a combination of the predictable part without security code influence and the unpredictable part containing the security code, demonstrated as Eq. (2):

$$s(t) = F\left(s_p(t), s_u(t)\right) \tag{2}$$

where $s_p(t)$ is the predictable part and $s_u(t)$ is the unpredictable part. $F(s_1, s_2)$ is a combination function that assembles two signals. In most cases this combination is a summation. The detection problem of the unpredictable part is generally regarded as a choice between two hypotheses, $\mathcal{H}_0$ and $\mathcal{H}_1$, in processing noise-containing signals. Hypothesis $\mathcal{H}_0$ means that the unpredictable part does not exist. Hypothesis $\mathcal{H}_1$ indicates the presence of unpredictable parts. This model can be expressed in Eq. (3):

$$\begin{cases} \mathcal{H}_0 : s(t) = F\left(s_p(t), \tilde{s}_u(t)\right) + n(t) \\ \mathcal{H}_1 : s(t) = F\left(s_p(t), s_u(t)\right) + n(t) \end{cases} \tag{3}$$

where $n(t)$ is the additive white Gaussian noise, and $\tilde{s}_u(t)$ is the counterfeit unpredictable part generated by attackers or noise. The detector outputs under the two hypotheses will lead to two different probability density distributions $p\left(f_d\left(s(n), K_p\right)|\mathcal{H}_0\right)$ and $p\left(f_d\left(s(n), K_p\right)|\mathcal{H}_1\right)$. While a reasonable prior probability and hypothesis testing threshold is selected, signal authentication detection can be implemented under the condition of determining the false alarm probability.

Taking spreading code carried security code as an example, the typical authentication detector is the matched filter correlator $f_d(s(n), s_l(n)) = \sum s_l(n)s(n)$ (Laurenti and Poltronieri, 2020). Here $s_l(n)$ is the local authenticable replica for the signal to process the authentication. The probability density distribution of the detector output under the presence and absence of the security code modified spreading code can be represented as Eq. (4):

$$\begin{cases} p\left(f_d(s(n), s_l(n))|\mathcal{H}_0\right) \sim \mathrm{N}\left(0, \sigma_n^2\right) \\ p\left(f_d(s(n), s_l(n))|\mathcal{H}_1\right) \sim \mathrm{N}\left(\sqrt{P_s}, \sigma_n^2\right) \end{cases} \tag{4}$$

where P_s is the signal power, and $\sigma_n^2 = kT/T_{\mathrm{coh}}$ is the noise power with k being the Boltzmann constant and T the temperature of the noise, and T_{coh} the coherent accumulation time of the correlator. The Eq. (4) is the different probability density distribution of the detection value. If the authenticable element does not present, the detection value will be a noise distribution whose mean value is zero. If the unpredictable authenticable elements exist, the detection value will be a normal distribution with a non-zero mean value. In this scenario, the mean value of the distribution is related to the power of these unpredictable authenticable elements.

According to the model discussed above, the constant false alarm detection threshold $T(P_{FA})$ of signal authentication detection can be represented as Eq. (5):

$$T(P_{FA}) = \sigma_n Q(P_{\mathrm{FA}}) \tag{5}$$

where $Q(x)$ is the right-tailed function of the standard normal distribution and can be represented as Eq. (6). The noise power can be estimated in the noise branch of the tracking loop.

$$Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{1}{2}t^2\right) \mathrm{d}t \tag{6}$$

Authenticity validation

The fundamental structure of authenticity validation is an extractor $f_e\left(r(n), K_p\right)$ designed to extract the security code carried by elements of the GNSS signal. This

detector is a function with received samples $r(n)$ and prior knowledge K_p as input and the security code estimation $\hat{u}(n)$ as output. The process of authenticity validation is a process of cryptographic validation. It can be encryption or decryption of a symmetric cipher, validation of an asymmetric digital signature, or verification of consistency in hash calculation. Various forms have different characteristics and fit different scenarios.

The *decryption of symmetric ciphers* is often used to communicate while authenticating the signal. By checking the legality of the format of the decryption result information, the receiver can verify the origin of the security code. The decrypted information can transmit certain information, such as prior knowledge or other auxiliary information for the next authentication. Constrained by the block length, symmetric cipher decryption, especially the authenticity validation using block cipher decryption, usually has specific requirements on the length of the security code.

Verifying digital signatures is often used to establish the fundamental trust for signal authentication. Because of the low complexity of public key distribution in asymmetric cryptography, most receivers can access the prior knowledge of verifying digital signatures. This feature enables asymmetric cryptography represented by digital signatures to reduce the complexity of establishing signal authentication trust. Constrained by the algorithm design and the choice of the underlying mathematical complex problem, the length of a digital signature is usually strictly limited. This feature also makes authenticity validation using digital signatures require a security code of strictly limited length.

Checking hash consistency is the most flexible method for authenticity validation and mainly used to confirm whether the source of the security code is authentic. Since the hash result can be arbitrarily truncated without affecting its one-way and random characteristics, choosing the truncated cryptographic hash output as the security code can achieve more flexible and efficient signal authentication.

Performance evaluation and key indicators

There are four main aspects of performance in the navigation signal authentication scheme. *Robustness* assesses the possibility that the receiver can precisely detect the spoofing signal. *Security* assesses the probability and the difficulty for an attacker to compromise the authentication scheme. *Efficiency* assesses how often a receiver can perform signal authentication. *Cost* assesses the implementation costs of receivers, GNSS constellation, and other systems of the signal authentication scheme.

Robustness

The robustness is mainly evaluated through the authentication detection probability P_D under the condition of constant missing alarms (Fernandez-Hernandez, 2015). It is the probability to correctly detect the authentication symbols when the possibility of spoofing detecting is fixed. The higher the probability, the more reliable the authentication scheme can detect whether the signal is spoofed. In practice, robustness is described by the indicator $P_D(C/N_0, P_{\mathrm{FA}})$. It is under C/N_0 of carrier to noise ratio and a fixed possibility P_{FA} to missing detection of signal without any authentication structure, evaluating the possibility of authentic signal passing the authentication scheme.

The indicator $P_D(C/N_0, P_{\mathrm{FA}})$ consists of two parts that can be represented as Eq. (7):

$$P_D(C/N_0, P_{\mathrm{FA}}) = P_{\mathrm{detection}} \times P_{\mathrm{validation}} \tag{7}$$

where $P_{\mathrm{detection}}$ is the detection probability of presence detection, and $P_{\mathrm{validation}}$ is the correct probability of authenticity validation, which is relevant to the Bit Error Rate (BER) of the security code extraction. Since cryptographic algorithms have an avalanche effect in bit changing, a one-bit error could fail the authenticity validation. Thus, the correct probability of authenticity validation can be demonstrated as Eq. (8):

$$P_{\mathrm{validation}} = (1 - d_{\mathrm{BER}})^{L_{\mathrm{sec}}} \tag{8}$$

where d_{BER} is the bit error rate of the security code extraction, and L_{sec} is the bit number of the security code involved in a single authentication.

Security

The security of navigation signal authentication mainly assesses whether it can maintain the authentication capability under cryptographic analysis attacks and SCER attacks. Spoofing attacks against satellite navigation are generally carried out by transmitting fake navigation signals to a target receiver. Since the authenticable signal contains the security code that the attacker cannot predict or generate independently, it is infeasible to generate a fake signal based on the signal interface documentation. Divided by the generation method of spoofing signals, the spoofing attacks against authenticable navigation signals mainly include cryptographic analysis attacks and SCER attacks.

Since the security codes are unpredictable, spoofing attackers cannot directly generate counterfeit signals. However, suppose the spoofing attacker can construct a predictor to predict the security code from past signal observations. In that case, the spoofing attacker will be able to forge a counterfeit replica of the authenticable

signal. This attack method is called a cryptographic analysis attack. Security under a cryptographic analysis attack mainly evaluates the hardness for attackers to perform a cryptographic analysis attack. This performance indicator is described by effective key length L_{ek}, which means the calculation complexity is approximately $\mathcal{O}\left(2^{L_{\mathrm{ek}}}\right)$ for attackers to perform a cryptographic analysis attack. It is a prerequisite that the computational complexity of an attacker can be assessed in this way. This presupposes that the cryptographic algorithm used by the authentication method is ideal. That is, the cryptographic algorithm can map each key bit to the degree of uncertainty of the signal. With the development of quantum computing, traditional asymmetric cryptographic algorithms that rely on difficult mathematic problems such as large integer decomposition will face a great challenge. However, the choice of a cryptographic algorithm can be largely decoupled from the design of specific signaling regimes. Therefore, when evaluating the security performance of signal authentication, the key length and the security of the selected algorithm can be considered separately.

In addition to the security of the key length and cryptographic algorithms, the signal authentication algorithm using the symmetric cryptosystems also needs to consider the security of key distribution and updates. Signal authentication methods using asymmetric cryptosystems need to focus on credibly distributing public keys to users.

The SCER attack is an advanced method specially designed for navigation signals with authentication capability. Suppose the navigation signal authentication scheme is not designed safely. In that case, its authentication feature may be bypassed by the SCER attack so that the authentication scheme can no longer protect the authenticity of the signal. The receiver can no longer determine whether the signal's source is authentic through the authentication process. When constructing an SCER attack, the attacker first receives and tracks the authentic GNSS signal, i.e., the target signal. Then, the attacker regards the authentication symbols as the information carried in the signal. An estimator is set up to estimate these authentication symbols. Finally, the estimation result is utilized to reassemble the spoofed signal (Humphreys, 2013).

Unlike spoofing attacks through signal re-transmission, SCER attacks can forge a negative latency (Zhang and Papadimitratos, 2019). Its construction method is first to estimate the unpredictable symbol within the time width, filling the corresponding position in the spoofing signal with random information before finishing the estimation process. After the SCER estimator completes the symbol estimation, the SCER attacker fills the rest position with the estimated symbol until the end of that symbol and raises the power of the spoofing signal. This method of falsifying the signal phase relies on enough time width of unpredictable symbol width. The larger the symbol width is, the greater the accuracy of the estimation and the temporal freedom of the phase forgery will be.

This type of attack will pose a significant threat to the authentication signal. Suppose no additional detection methods are used to detect the SCER attack. In that case, it is necessary to reduce the width of the unpredictable symbol in the authentication signal as much as possible. The security of preventing SCER attacks is mainly evaluated by three indicators: the Maximum Predictable Time (MPT), the Unpredictable Symbol Rate (USR), and the Unpredictable Symbol Width (USW). MPT is the maximum time of signal segments without security code covering. Spoofing attackers can easily forge spoofing signals during this time since it is predictable. USR is the average symbol rate of security code, indicating the frequency and complexity for attackers to estimate the unpredictable symbols in the authenticable signal. USW is the width of a single unpredictable security symbol, which is the maximum time for attackers to estimate it. The smaller the USW is, the more unlikely the attackers can get a reliable estimation.

The type of attack against SCA is usually a direct retransmission of authentic signals. There is an irrevocable feature of signal retransmission: spoofed signals have an indispensable delay relative to authentic signals. The receiver's trusted acceptance strategy for SCA signals is as follows. First, confirm that the authentic signal may be received in the current signal environment through power detection or other means. Then, search and track all navigation signals that meet the conditions and authenticate them one by one. Finally, process the signal that is most advanced in phase and can pass the signal authentication as an authentic signal. This whole set of strategies is based on the receiver's ability to authenticate navigation signals, and retransmission spoofing attack signals are implemented with a delay relative to the authentic signal.

Efficiency

The efficiency of an authentication scheme is assessed mainly through the Time to the First Authenticated Fix (TTFAF) or the Time Between Authentications (TBA) (Fernandez-Hernandez, 2015). TTFAF means the time it takes for the receiver to calculate from the first time it tracks the signal until it obtains the positioning output under the trusted signal authentication result. This time determines how long the receiver needs to operate without signal authentication. That is, how long the receiver needs to output results without being able to determine

the authenticity of the positioning results. TBA means that the interval between two adjacent signal authentications of the receiver which cannot confirm the trustworthiness of the signal in real-time. If this is too long, the receiver may be affected by a towed spoofing attack that outputs incorrect positioning results between authentications. Sometimes, TTFAF and TBA can also indicate the latency of signal authentication. That is, this completed authentication is responsible for the time the signal authenticity has lasted.

Generally, if the authentication process is distributed evenly and every authentication attempt takes the same time, t_{TTFAF} will be 0.5 times the t_{TBA} plus an average TBA time $t_{\overline{\mathrm{TBA}}}$. This phenomenon occurs because the receiver tracks the signal randomly so that the authentication structure may pass half the time. Hence, the receiver has to wait for the following authentication structure to start a new authentication process. Then the process has a specific possibility to pass successfully, which is the average TBA. Thus, the relationship between t_{TTFAF} and $t_{\overline{\mathrm{TBA}}}$ is defined by Eq. (9).

$$t_{\mathrm{TTFAF}} = \frac{t_{\mathrm{TBA}}}{2} + t_{\overline{\mathrm{TBA}}} \tag{9}$$

However, if a unique receiving process is demanded to authenticate the signal for the first time, t_{TTFAF} may become longer. Suppose the time length of the signal structure of these processes demanded to authenticate the signal for the first time is $T_{A,0}$, considering the receiver will also track at a random point. In that case, the t_{TTFAF} will be 0.5 times of $T_{A,0}$ plus an average $\overline{T_{A,0}}$ time.

Here the relationship between t_{TBA} and $t_{\overline{\mathrm{TBA}}}$ is defined by Eq. (10).

$$t_{\overline{\mathrm{TBA}}} = \frac{t_{\mathrm{TBA}}}{P_D} \tag{10}$$

The rate and the total length of the security code will directly affect the t_{TBA} and determine the t_{TTFAF}.

Cost

Cost mainly evaluates three aspects of performance: performance deterioration of receivers compared with no authentication signal, communication overhead, and calculation and storage complexity of receivers and satellites.

The insertion of the security code may influence the navigation message, spreading code, or other elements of the original GNSS signal, which may cause a deterioration in service performance. This deterioration in service performance can often be described by indicator L_{C/N_0}, which is the equivalent loss in signal C/N_0. The communication overhead is applicable when the authentication scheme requires an additional communication link. This overhead can be described by indicators R_s and R_u. Here R_s is the required communication bit rate for authentication servers, and R_u is the required communication bit rate for authentication users. Calculation and storage complexity described by maximum calculation complexity N_{cal} and maximum storage requirement N_{storage} indicates the hardness of implementing the scheme.

For the overhead of updating keys and managing them, most signal authentication methods use navigation messages, public documents, or data communications. These costs can often be combined into the loss of navigation message transmission rate or the cost of communication link capability.

Table of Key Performance Indicators (KPIs)

The table of KPIs in an authentication scheme is summarized in Table 1.

Cryptographic-based authentication schemes

Reported authentication schemes mainly use navigation messages and spreading code as signal elements for authentication. The schemes that use navigation messages are categorized as NMA, and schemes that use spreading code are categorized as SCA.

Navigation Message Authentication

MA schemes use navigation messages as the vital element to authenticate signals. Receivers authenticate

Table 1 The table below summarizes the description of indicators to evaluate the performance of an authentication approach

Domain	Indicator	Description
Robustness	P_D	Detection probability
	P_{FA}	Missing detection probability (fixed design parameter)
Security	L_{ek}	Effective key length
	MPT	Maximum predictable time
	USR	Unpredictable symbol rate
	USW	Unpredictable symbol width
Efficiency	t_{TTFAF}	Time to the first authenticated fix*
	t_{TBA}	Time between authentications
Cost	L_{C/N_0}	Equivalent loss in signal C/N_0
	R_s	Server communication rate
	R_u	User communication rate
	$N_{\mathrm{cal,s}}$	Satellite calculation complexity
	$N_{\mathrm{cal,r}}$	Receiver calculation complexity
	$N_{\mathrm{storage,s}}$	Satellite storage requirement
	$N_{\mathrm{storage,r}}$	Receiver storage requirement

*t_{TTFAF} is modified to Time to the First Authenticated Channel (TTFAC) to indicate the time required to track the first authentic signal

the received signal by demodulating and decoding the navigation message and verifying its authenticity. This authentication is performed through the information attached to the navigation message or assisting messages transmitted from third-party sources such as satellite or ground-based augment systems, e.g. Satellite-Based Augmentation System (SBAS) or Ground-Based Augmentation Systems (GBAS). This information is typically generated through cryptosystems. Receivers can verify the authenticity of the received signal by validating the cryptographically generated security code.

Most schemes of NMA authenticate the navigation message itself. A typical NMA scheme jointly uses TESLA protocol and asymmetric cipher to build a trust system anchored to a revealed public key. The structure of the NMA reinforced navigation message can be demonstrated in Fig. 2.

Open Service Navigation Message Authentication for Galileo

Among all the NMA schemes, the Open Service Navigation Message Authentication (OSNMA) proposed for Galileo is the most famous and successful. In 2010, an initial analysis was made by De Castro et al. (2010) to introduce the possibility and added value of authentication in the navigation message of Galileo. Later, Hernandez et al. (2014) further explains the design drivers, scheme consideration, and robustness assessment of the OSNMA especially giving a set of performance indicators for NMA schemes. Curran and Paonni (2014) focused on the data burden and concluded that the increased data extraction burden is not significant and does not constitute a significant impediment to the typical users. This research ensures that the OSNMA is a low-cost scheme suitable for fast implementation.

In 2015 and 2016, the OSNMA was formally proposed to Galileo as a potential scheme to build its authentication capability (Fernandez-Hernandez et al., 2016; Walker et al., 2015). In this proposed version, the baseline design

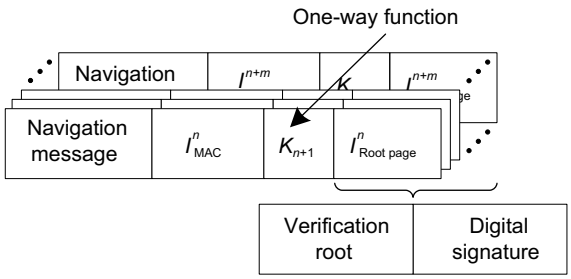

Fig. 2 Message in typical NMA schemes consists of navigation messages, Message Authentication Codes (MACs) I^{n}_{MAC}, keys in a delayed-disclosure one-way chain, and root information. Root page $I^{n}_{Root\ page}$ consists of a verification root to verify keys and a digital signature to verify the verification root

of OSNMA is described in detail. The OSNMA obtains authentication capability by adding authentication information based on symmetric and asymmetric ciphers in the reserved area of the signal navigation message. The symmetric cipher is the MAC calculated from the navigation message and the key in a TESLA chain. The asymmetric part is a replica and the digital signature of the verification root of the TESLA chain. Then, this information is packed into the frame structure of the navigation message in E1OS of Galileo. Receivers can authenticate the navigation message through these ciphers and digital signatures.

After that, OSNMA also has undergone several rounds of revisions and adjustments. The security issues and the proper length of MAC selection were analyzed for the OSNMA in 2016 (Caparra et al., 2016; Fernandez-Hernandez et al., 2021a, 2021b). In 2017, the structure of authenticable navigation message is evaluated, and Authentication Error Rate (AER) is analyzed to propose a Forward Error Correction (FEC) scheme (E. Gkougkas et al., 2017a, 2017b). Later in 2018, I. Fernandez-Hernandez et al., (2018a, 2018b) introduced the developing program and the policy perspective of the OSNMA. Hernandez et al. (2019) focuses on the authentication of the public keys and renewal and revocation of all keys.

In the implementation of OSNMA, Margaria et al. (2016) demonstrated the OSNMA in both a commercial GPS receiver and a modified software receiver. Sarto et al. (2017) reported the implementation and testing progress of OSNMA for Galileo till 2017. Motella et al. (2020) proposed a real-time OSNMA-ready software receiver that includes a detailed set-up and running demonstration. Later the scheme is implemented in the Galileo based Timing Receiver for Increasing Critical Infrastructures Resilience (GIANO) receivers (Catalano et al., 2020). Improved from an initial analysis in 2019 (Simon Cancela et al., 2019a, 2019b; Cancela et al., 2019a, 2019b), M. T. Gamba et al., (2020a, 2020b) built OSNMA in an ARM-based embedded platform and analyzed the computational load of OSNMA under real-time processor load meaning (Gamba et al., 2021). The analysis finds that the functionality that exhibits the worst degradation is the digital signature verification. Cucchi et al. (2021) assessed the OSNMA under various scenarios through a software-defined receiver. In 2021, the OSNMA came into the preparation phase (Gotzelmann et al., 2021), and drivers for future service provision are reported. In 2022, the OSNMA has entered the public observation phase (Nicola et al., 2022) and will be ready to begin service formally.

Further research has been conducted to optimize the efficiency and security of Galileo OSNMA. Manandhar and Shibasaki (2018) studies to utilize the Quasi-Zenith

Satellite System (QZSS) to transmit the authenticated navigation message of Galileo to improve efficiency. Marucco et al. (2020) describes the Galileo-based trusted applications for health and sustainability (GOEASY) project, which jointly utilizes the OSNMA and the extra e-security features built additionally. O'Driscoll and Fernandez-Hernandez (2020) help the receiver to re-encode the navigation message into symbols and compare the symbol error rates to avoid the forward estimation attack (Curran and O'Driscoll, 2016). Gallardo and Yuste (2020) analyzed the model of SCER spoofing attacks on the OSNMA and proposed a machine learning technique for its detection.

NMA proposed for GPS

The NMA schemes are also proposed for GPS. Wesson et al. (2011) proposed the NMA-based cryptographic authentication for GPS. In the study, authentication methods, as well as approaches to detect SCER attacks, are analyzed. Later in 2012, more details are added to the initial design with algorithm selection and performance evaluation (Wesson et al., 2012). Recently, Ghorbani et al. (2020) evaluated the feasibility and proposed an NMA scheme for GPS L1C and L1C/A navigation messages. The scheme is also based on TESLA and digital signature structure similar to the OSNMA.

The NMA scheme designed for GPS in the above research combines symmetric and asymmetric cryptography. The scheme uses the symmetric key driven by the TESLA protocol to calculate the MAC of the navigation message and uses the digital signature to asymmetrically authenticate the verification root of the TESLA chain and the wide-area navigation message.

In recent years, Chu et al. (2022) proposed an NMA scheme for GPS utilizing a chameleon hash keychain, similar to TESLA but with fewer synchronization requirements.

NMA proposed for BDS

Recently, the NMA scheme was proposed for BeiDou Navigation Satellite System (BDS) to authenticate its navigation message. Yuan et al. (2017) proposed an NMA scheme similar to the OSNMA for Beidou civilian signals. In the research, reserved bits in the navigation signal of the BDS civilian signal are counted, and the feasibility of installing an OSNMA-liked authentication scheme is analyzed. Wu et al. (2020) proposed an NMA scheme using SM cryptographic algorithm (SAC, 2016b, 2017) series for BeiDou-2 Navigation Satellite System (BDS-2), which is also a MAC and digital signature combined structure.

NMA proposed for other systems

The NMA scheme is also proposed for other systems, such as SBASs. Chiara et al. (2017) and Ignacio Fernandez-Hernandez et al., (2018a, 2018b) studied the drivers and the consideration aspects of SBAS authentication for European Geostationary Navigation Overlay Service (EGNOS). The performance of the schemes of OSNMA used in the SBAS authentication is also evaluated. Cogdell and Reddan (2018) proposed an NMA scheme designed for the Dual Frequency Multi-Constellation (DFMC) SBAS in Australia and New Zealand. The research demonstrates the viability of a single-message authentication approach using the DFMC SBAS L5-Q channel. Tosato et al. (2021) studied the concepts of message authentication in future SBAS services, concluding that the solutions broadcast in the Q channel are of advantage and suitable for implementation. Walter et al. (2021) and Wullems et al. (2021) also proposed a candidate scheme for DFMC SBAS service and analyzed its future performance for the EGNOS and the Wide Area Augmentation System (WAAS). Furthermore, Hirokawa and Fujita (2019) and Fernandez-Hernandez et al. (2021b) discussed the same NMA structure utilized in Precise Point Positioning (PPP) or PPP-Real-Time Kinematic (RTK).

Besides authenticating the SBAS service, the SBAS service can also provide NMA capability for GNSS civilian signals. Dalla Chiara et al. (2016) and Manandhar and Shibasaki (2017) discussed the concept and proposed an NMA scheme assisted by QZSS L1S augmenting signal. Walter et al. (2021) proposed an SBAS message scheme to support the NMA for GNSS signals, ensuring rigorous user protection by guaranteeing that unauthenticated data is discarded and cannot harm the user.

The advantage of NMA is that the changes to the navigation signal are small, and the implementation cost of receivers and satellites is also tiny. However, limited by the low symbol rate of navigation messages, the security of NMA under SCER attack is poor. Also, due to the limitation of symbol rate and the bit length of cryptographic information, it is not easy to improve the upper limit of authentication efficiency of NMA.

Spreading code authentication

SCA approaches use spreading code to verify the authenticity of GNSS signals. The most famous SCA scheme is the chip-message robust authentication (Chimera) proposed for GPS. The Chimera utilizes both NMA and SCA, while the SCA part is vital.

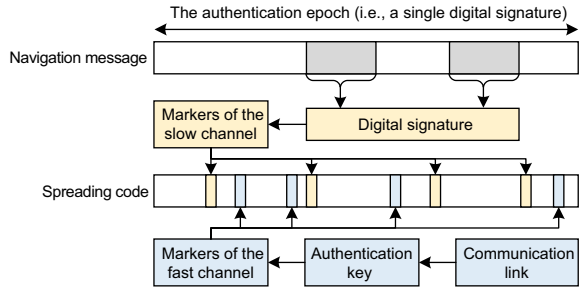

Fig. 3 The NMA of the Chimera scheme is constructed through the digital signature of the navigation message. The SCA is achieved by inserting markers into the civilian spreading code. The yellow blocks in the figure above indicate the authentication of the slow channel, while the blue blocks indicate the fast channel

Chip-message robust authentication for GPS

Firstly introduced as a concept in 2014 (Scott, 2014), the Chimera scheme was proposed in 2017 (Anderson et al., 2017) to jointly utilize NMA and SCA for GPS L1C signal authentication. The Chimera pseudo-randomly inserts a series of encrypted spreading codes to the signal's spreading code. The authentication receiver locally generates the signal's spreading code by obtaining the position and code sequence of these encrypted spreading codes from the navigation message or the additional communication link. The signal structure of the Chimera scheme is demonstrated in Fig. 3.

There are two authentication channels in the Chimera scheme of GPS, the slow channel and the fast channel. The slow channel authentication uses only the navigation signal itself. The slow channel authentication verifies the navigation message with the digital signature attached to the navigation message and uses this digital signature to generate the sequence and insertion position of the slow channel markers in the spreading code. The fast channel authentication uses a communication link to receive the prior knowledge required for authentication. After the key required for authentication is received from the communication link, it uses this key to generate the sequence and insertion position of the fast channel markers in the spreading code. Whether it is a fast channel or a slow channel, the basic authentication process of its SCA is to perform correlation and existence verification on the flag sequence in the spreading code. The Chimera scheme combines the NMA and the SCA to achieve a time binding that enhances the security of the authentication scheme. The security features (i.e., the time-binding scheme) are analyzed in (Poltronieri et al., 2018), concluding that the hardness of performing a collision attack is very close to an attack against the uniform model.

In the system-level implementation, the Chimera scheme has been tested in the experimental satellite Navigation Technology Satellite—3 (NTS-3) since 2021 (Hinks et al., 2021). Nicola et al. (2020) assessed the performance of the Chimera scheme both in theoretical metrics and actual implementation inside the receiver. Micaela Troglia Gamba et al., (2020a, 2020b) developed a software model of Chimera and demonstrated its compatibility with Chimera. Nicola et al. (2021) built a software receiver with the Chimera scheme to demonstrate the scheme and analyzed its performance. Mina et al. (2021) utilized stochastic reachability analysis to achieve a continuous GPS authentication with the Chimera scheme.

Further research utilized Chimera-based structures in other systems. Jia et al. (2021) briefed the GNSS authentication technology and proposed a Chimera-liked scheme for BDS civilian signals. Motella et al. (2021) combined the Chimera and the OSNMA to achieve a more robust authentication. Wang et al. (2022) studied the marker distributions applied to the BDS B1C signal and concluded that the greater the markers' dispersion, the higher the collision probability will be in a segment. Besides, the correlation performance is little affected by the dispersion of markers.

SCA via military spreading code

Since military signals have an in-built authentication capability, military spreading code is a proper material to authenticate civilian GNSS signals (Bertran et al., 2005; Hein and Avila-Rodriguez, 2005; Rugamer et al., 2014a). Encryption, while preventing unauthorized use, also gives signals the feature that they cannot be repudiated. Because an attacker without the key will be unable to decrypt or receive military signals and generate a counterfeit military signal, this non-replicable feature is what signal authentication requires. Multiple schemes use the military spreading code to achieve civilian GNSS signal authentication. In order to solve the problem of distributing the prior knowledge for authentication (i.e., the military spreading code segments or material to derive the military spreading code), communication links are utilized.

The exploring PRS low-end receivers (EXPLORERS) program (Turner et al., 2015) is a spreading code authentication proposed for Galileo open service via spreading code of Galileo PRS. It is a communication-assisted authentication system, including two services, called PRS/Open Service Positioning and Authentication (PROSPA) (Turner et al., 2013) and National Space Technology Program (NSTP) Aspire project (ASPIRE) (Rugamer et al., 2016, 2020; Turner et al., 2015). The PROSPA sends Galileo PRS spreading code segments to

the receiver. The receiver authenticates the signal by performing a correlation between the received signal and those spreading code segments at the corresponding time to detect the existence of the PRS spreading code. Since the PRS spreading code is cryptographically generated and only for authorized use, the service either broadcasts past spreading codes for delayed authentication or is only available to authorized users such as military users. The ASPIRE receives signal samples from the receiver to perform a spoofing detection through local PRS spreading code and then sends the results back to the receiver (Rugamer et al., 2014b). Since this service needs to process the data of each user individually, its service capacity is limited by communication and computing resources.

GPS uses the P(Y) code military signal in the quadrature phase with the C/A code civilian signal to construct the communication-assisted authentication (O'Hanlon et al., 2013; Psiaki et al., 2013). The trusted receiver in the service center first receives and tracks the civilian L1C/A signal and then sends the baseband sample of the quadrature branch (including P(Y) code samples) of the signal to the user. This sample is correlated with the received signal to detect whether there is a P(Y) code signal with the corresponding phase, thereby authenticating the signal. Since the P(Y) signal sample sent by the service center contains noise, authentication detection performance will deteriorate compared to the EXPLORERS designed for Galileo. Furthermore, Heng et al. (2014) discussed the method to maintain the authentication capability when the reference receiver is unreliable, proposing an improved validating algorithm. Bhamidipati et al. (2018) presented a practical application for power systems utilizing the authentication scheme discussed above.

Other SCA schemes

Improved from an initial concept in (Pozzobon et al., 2010), Pozzobon et al. (2014) proposes an SCA scheme using an additional signal synchronized to the civilian signal. The authenticable signal uses a secret spreading code with a Code Shift Keying (CSK) modulation, while another secret information is CSK modulated onto the secret spreading code. The research called this structure the supersonic code. Later Elias Gkougkas et al., (2017a, 2017b) proposed a similar scheme designed for low-power authentication to reduce the power splitting in the supersonic code.

Gkougkas et al. (2019) proposed an authentication scheme utilizing a new stand-alone signal component along with an NMA authenticated GNSS signal. The stand-alone authentication signal is equipped with a secret and random spreading code synchronized to the GNSS signal. Codeless receiving techniques can track the stand-alone signal to authenticate the GNSS signal.

Wang et al. (2021) proposed an SCA scheme by modifying the phase of the original constellation points of the civilian signal. Since the shift in the phase consists of a sequence generated from a cryptosystem, receivers can authenticate this sequence through the correlation between the received samples and a local replica. In the performance analysis, the proposed scheme is similar to traditional SCA.

Yuan et al. (2022a) uses the cross-correlation between different delays of signal samples instead of local recovered authentication spreading codes. This modification avoids the massive storage in typical SCA schemes, which significantly reduces the storage. Another scheme is also proposed to trade-off the security and the cost by authenticating the signal via the fluctuation in correlation results (Yuan et al., 2022b). This scheme randomly flips spreading code in the signal to produce a fluctuation in the correlation result and encodes the security code into this fluctuation for authentication, which also avoids the massive storage.

SCA takes full advantage of the high rate of the spreading code of the navigation signal. The high spread spectrum code rate makes SCER attacks challenging to construct. Furthermore, the authentication receiver can receive and authenticate the signal at a higher temporal resolution. These advantages bring better security to SCA. However, the high rate of spread spectrum code also requires the receiver to cache the baseband sampling of the navigation signal when performing delayed authentication processing. This size of cache places a more significant burden on the amount of storage than on navigation messages. This makes it difficult for existing SCA-related authentication methods to be popularized in low-cost, lightweight receivers.

Comprehensively comparing the characteristics of the NMA method and the SCA method, it can be found that they are suitable for different scenarios. NMA is more suitable for the applications which need basic signal security requirements but cannot pay more for hardware. For example, conventional civilian scenarios such as smartphones and the industrial Internet of Things. While SCA is more suitable for the applications which require higher security and can also pay more hardware costs in receivers, such as life safety-related services, power grids, and other critical infrastructure.

Performance comparison and trends

This section summarizes performance comparisons for the reported authentication schemes in Table 2.

It can be seen from Table 2 that the NMA-liked schemes have the advantages of good reliability and low implementation overhead. However, the message rate

Table 2 This table compares the performance of different navigation signal authentication schemes

Scheme	Robustness	Security			Efficiency		Cost			
	P_D	MPT	USR	USW	TTFAF	TBA	L_{C/N_0}	R_u	N_{cal}	$N_{storage}$
OSNMA for Galileo	High	~6 s	~5 SPS	10 ms	~270 s	30 s	0	0	Low	Very low
SBAS assisted NMA	High	~6 s	~10 SPS	~10 ms	~36 s	6 s	0	Low	Low	Very low
Chimera for GPS (Fast channel)	Moderate	~50 μs	$\sim 256 \times 10^3$ SPS	~2 μs	Variable*	Variable*	~−1 dB	Moderate*	Low	Low
Chimera for GPS (Slow channel)	Moderate	~50 μs	$\sim 256 \times 10^3$ SPS	~2 μs	~270 s	180 s	~−1 dB	0	Low	High
PROSPA	Moderate	~1 μs	$\sim 10 \times 10^6$ SPS	~1 μs	Variable**	Variable**	0	Moderate to high	High	Moderate
ASPIRE	High	~1 μs	$\sim 10 \times 10^6$ SPS	~1 μs	Variable**	Variable**	0	Moderate to high	Low	High
P(Y) samples (Psiaki et al., 2013)	Moderate	~20 μs	$\sim 5.115 \times 10^3$ SPS	~20 μs	Variable**	Variable**	0	Moderate to high	Low	High
Supersonic code (Pozzobon et al., 2014)	Moderate	~10 μs	$\sim 1 \times 10^6$ SPS	~10 μs	~50 ms	~1 ms	Variable***	Low	High	Low
Codeless authentication (Gkougkas et al., 2019)	Moderate	~20 μs	$\sim 500 \times 10^3$ SPS	~20 μs	~1 s	~20 ms	Variable***	Low	High	Low
Binary phase hop (Wang et al., 2021)	Moderate	~10 μs	$\sim 1 \times 10^6$ SPS	~10 μs	~50 ms	~50 ms	Variable***	Low	High	Low

Some indicators are assessed qualitatively and others quantitatively

The performance evaluation of the authentication scheme mainly comes from its recommended set of typical implementation parameters. Also, it refers to other articles and research on the performance evaluation of the authentication scheme. Since P_{FA} is a design parameter, the performance analysis will let $P_{FA} = 10^{-3}$ as a background set. Besides, all the authentication schemes can equip a high length of L_{ek} that will not display again in the table.

*The efficiency of the fast channel is depended on the capability of the communication channel.

**The efficiency of PROSPA, ASPIRE and P(Y) sample authentication depends on the communication bit rate.

***The L_{C/N_0} of the supersonic code, codeless authentication and binary phase hopping depends on how much power is assigned from the civilian signal to the supersonic code signal.

limits its security. The SCA-liked schemes are less reliable, and the implementation overhead is usually significant, but the security against SCER attacks is good.

Almost all the navigation signal authentication schemes reported so far use navigation messages or spreading codes as the signal elements used for authentication. In addition, navigation signal authentication usually only authenticates the signal broadcast by a single satellite and does not explore the possibility of mutual authentication of different satellite signals. Therefore, future navigation signal authentication will have the following development trends.

Various and multiple elements for authentication

In addition to the navigation message and spreading code, the power of the navigation signal, the carrier frequency and phase, and even the clock of the navigation signal itself are potential elements that can carry authentication information. Wang et al. (2021) attempted to carry the navigation signal authentication information on the carrier phase. However, since the shifted phase will align with the spreading code and its synchronization design, it can be regarded as spreading code authentication.

Both navigation messages and spreading codes carrying authentication information have certain defects. The relatively low symbol rate limits the navigation message and makes NMA limited protection against SCER. The SCA to the civil navigation signal needs to change the spreading code sequence, which will bring an inevitable loss of processing C/N_0. Authenticating military signals or other cryptographically generated spreading code signal branches based on communication links require strong data communication support and may not be suitable for lightweight pure navigation receivers.

The design of future navigation signal authentication schemes can consider using signal elements such as signal power and carrier frequency to carry the security code. Further, like the Chimera scheme, the feasibility of multiple signal elements to carry the signal authentication information cooperatively should also be studied.

Joint authentication of multi-satellite signals

The navigation signal authentication schemes reported so far usually authenticate one satellite signal at a time. In future there will be low-orbit navigation constellations composed of massive satellites in service. When the number of satellites is large, the scheme of authenticating one satellite signal at a time will significantly limit the efficiency of signal authentication. A possible development trend is to verify the authenticity of multiple satellite signals in a single authentication process.

Yuan et al. (2022a) attempted to authenticate the signals from two satellites in a single process. The scheme is inserting a similar security code to every satellite signal with a different initial phase. Since cross-correlation can extract and detect the security code in any signal, two signals involved in the correlation can be authenticated simultaneously.

Facing the future massive low-orbit satellite constellation navigation signals, the navigation signal authentication scheme that can perform multi-channel signal authentication simultaneously is a powerful tool to improve service efficiency. We can refer to the mechanism design of multi-signal cooperative authentication from the aspects of security code mutual information, secure multi-party computation, and multi-key cryptosystems.

Inherent unpredictability authentication

Most navigation signal authentication schemes discussed above require the modification of the entirely predictable civilian navigation signal. Some modifications change the navigation messages or spreading codes of civilian navigation signals by adding unpredictable information to them. Other modifications are to add a security signal component along with the civilian navigation signals or to use military navigation signals directly for authentication. So, the authentication can be achieved by exploiting the inherent unpredictability of navigation signals.

The non-uniformity of satellite clocks and the jitter characteristics of onboard power amplifiers are unpredictable physical characteristics of civil navigation signals. These features come not only from cryptographic calculations but also from the physical properties of the satellite itself. Suppose a detector or extractor can be designed to detect or extract these features or feature pattern. These features are not naturally generated but involved in a manual process structure. This category in the integration circuit field is called the Physical Unclonable Functions (PUF). Not the same as existing anti-spoofing techniques that detect via naturally generated physical observations, these features can also be a physical unclonable function in signal generation. In that case, the navigation signal authentication can be realized without changing the structure of the navigation signal but only by updating the satellites themselves.

Conclusion

This paper reviews the signal authentication for civil satellite navigation services. First, the theory of satellite navigation signal authentication is introduced retrogradely. The theoretical framework includes the generation and verification of authentication information (i.e., security code), the sorting and characteristics of signal elements used to carry security codes, and the authentication

detection and verification theory of signal elements containing security codes. Then, we introduce the leading design and latest development results of the navigation signal authentication scheme. Various navigation signal authentication schemes, including NMA and SCA, and their development are introduced. Finally, a comparison of the performance of mainstream navigation signal authentication schemes is performed, and three possible development directions for future navigation signal authentication schemes are discussed.

Acknowledgements
Not applicable.

Author contributions
MY; methodology, XT and GO; validation, MY; writing—original draft preparation, XT and GO; writing—review and editing, GO; supervision. All authors read and approved the final manuscript.

Funding
This research was funded by the National Natural Science Foundation of China (Grant Nos. U20A0193 and 62003354).

Availability of data and materials
The data presented in this study are available on request from the corresponding author.

Code availability
The code presented in this study are available on request from the corresponding author.

Declarations

Competing interests
The authors declare no competing interests.

Received: 3 August 2022 Accepted: 8 January 2023
Published online: 13 February 2023

References

Akos, D. M. (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (agc). *Navigation, Journal of the Institute of Navigation, 59*(4), 281–290. https://doi.org/10.1002/navi.19

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. (2017). Chips-message robust authentication (chimera) for GPS civilian signals. In *30th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2017*, September 25, 2017–September 29, 2017.

Becker, G. T., Lo, S., De Lorenzo, D., Qiu, D., Paar, C., & Enge, P. (2009). Efficient authentication mechanisms for navigation systems—A radio-navigation case study. In *22nd international technical meeting of the satellite division of the institute of navigation 2009, ION GNSS 2009*, ION GNSS 2009, September 22, 2009–September 25, 2009.

Bertran, X., Vidal, A., & Panefieu, B. (2005). Galileo's Public Regulated Service (PRS)—Future perspective and benefits. In *Proceedings of the 18th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2005*, ION GNSS 2005, September 13, 2005–September 16, 2005.

Bhamidipati, S., Mina, T. Y., & Gao, G. X. (2018). GPS time authentication against spoofing via a network of receivers for power systems. In *2018 IEEE/ION position, location and navigation symposium, PLANS 2018—Proceedings*, April 23, 2018—April 26, 2018.

Bhatti, J., & Humphreys, T. E. (2017). Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *Navigation, Journal of the Institute of Navigation, 64*(1), 51–66. https://doi.org/10.1002/navi.183

Blanch, J., Walter, T., & Enge, P. (2010). RAIM with optimal integrity and continuity allocations under multiple failures. *IEEE Transactions on Aerospace and Electronic Systems, 46*(3), 1235–1247. https://doi.org/10.1109/TAES.2010.5545186

Borio, D., & Gioia, C. (2016). A sum-of-squares approach to GNSS spoofing detection. *IEEE Transactions on Aerospace and Electronic Systems, 52*(4), 1756–1768. https://doi.org/10.1109/TAES.2016.150148

Broumandan, A., Siddakatte, R., & Lachapelle, G. (2017). Feature article: An approach to detect GNSS spoofing. *IEEE Aerospace and Electronic Systems Magazine, 32*(8), 64–75. https://doi.org/10.1109/MAES.2017.160190

Cancela, S., Calle, J. D., & Fernandez-Hernandez, I. (2019a). CPU consumption analysis of TESLA-based navigation message authentication. In *European navigation conference, ENC 2019a*, April 9, 2019a–April 12, 2019a.

Cancela, S., Navarro, J., Calle, D., Reithmaier, T., Chiara, A. D., Broi, G. D., Fernández-Hernández, I., Seco-Granados, G., & Simón, J. (2019b). Field testing of GNSS user protection techniques. In *Proceedings of the 32nd international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2019b*, September 16, 2019b–September 20, 2019b.

Caparra, G., Sturaro, S., Laurenti, N., & Wullems, C. (2016). Evaluating the security of one-way key chains in TESLA-based GNSS Navigation Message Authentication schemes. In *Proceedings of 2016 international conference on localization and GNSS, ICL-GNSS 2016*, June 28, 2016–June 30, 2016.

Caparra, G., Ceccato, S., Sturaro, S., & Laurenti, N. (2017). A key management architecture for GNSS open service Navigation Message Authentication. In *2017 European navigation conference, ENC 2017*, May 9, 2017–May 12, 2017.

Catalano, V., Prata, R., Carvalho, F., Nunes, R., Marradi, L., Franzoni, G., Puccitelli, M., Campana, R., & Gioia, C. (2020). Galileo OSNMA preliminary implementation in the GIANO GNSS receiver. In: *Proceedings of the 33rd international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2020*, September 22, 2020–September 25, 2020, Virtual, Online.

Chiara, A. D., Broi, G. D., Pozzobon, O., Sturaro, S., Caparra, G., Laurenti, N., Fidalgo, J., Odriozola, M., Ramon, J. C., Fernandez-Hernandez, I., & Chatre, E. (2016). Authentication concepts for satellite-based augmentation systems. In *29th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2016*, September 12, 2016–September 16, 2016.

Chiara, A.D., Broi, G.D., Pozzobon, O., Sturaro, S., Caparra, G., Laurenti, N., Fidalgo, J., Odriozola, M., López, G. M., & Fernandez-Hernandez, I. (2017). SBAS authentication proposals and performance assessment. In *Proceedings of the 30th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2017)*. https://www.ion.org/publications/abstract.cfm?articleID=15327

Chu, Y. H., Keoh, S. L., Seow, C. K., Cao, Q., Wen, K., & Tan, S. Y. (2022). GPS signal authentication using a Chameleon Hash Keychain. In *IFIP advances in information and communication technology 15th IFIP WG 11.10 international conference on critical infrastructure protection, ICCIP 2021*, March 15, 2021–March 16, 2021, Virtual Online.

Cogdell, K., & Reddan, P. (2018). Australia/New Zealand DFMC SBAS and navigation message authentication. In *Proceedings of the 31st international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2018*, September 24, 2018–September 28, 2018.

Coulon, M., Chabory, A., Garcia-Pena, A., Vezinet, J., Macabiau, C., Estival, P., Ladoux, P. & Roturier, B. (2020). Characterization of meaconing and its impact on GNSS receivers. In *Proceedings of the 33rd international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2020*, September 22, 2020–September 25, 2020, Virtual, Online.

Cucchi, L., Damy, S., Paonni, M., Nicola, M., Troglia Gamba, M., Motella, B., & Fernandez-Hernandez, I. (2021). Assessing galileo OSNMA under different user environments by means of a multi-purpose test bench, including a software-defined GNSS receiver. In *Proceedings of the 34th international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2021*, September 20, 2021–September 24, 2021.

Curran, J. T., & Paonni, M. (2014). Securing GNSS: An end-to-end feasibility study for the galileo open service. In *27th international technical meeting*

of the satellite division of the institute of navigation, ION GNSS 2014, September 8, 2014–September 12, 2014.
Curran, J. T., & O'Driscoll, C. (2016). Message authentication, channel coding & anti-spoofing. In *29th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2016*, September 12, 2016–September 16, 2016.
Daemen, J., & Rijmen, V. (2002). *The design of rijndael: AES—The Advanced Encryption Standard*. The Design of Rijndael: AES - The Advanced Encryption Standard.
Dang, Q. H. (2015). *Secure hash standard*. https://doi.org/10.6028/NIST.FIPS.180-4
De Castro, H. V., Van Der Maarel, G., & Safipour, E. (2010). The possibility and added-value of authentication in future Galileo open signal. In *23rd international technical meeting of the satellite division of the institute of navigation 2010, ION GNSS 2010*.
De Wilde, W., Sleewaegen, J.M., Bougard, B., Cuypers, G., Popugaev, A., Landmann, M., Schirmer, C., Roca, D. E., López-Salcedo, J. A. & Granados, G. S. (2018). Authentication by polarization: A powerful anti-spoofing method. In *Proceedings of the 31st international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2018*, September 24, 2018–September 28, 2018.
Fernandez-Hernandez, I. (2015). *Snapshot and authentication techniques for satellite navigation*. Ph.D. Dissertation, Aalborg University, UK
Fernandez-Hernandez, I., Rijmen, V., Seco-Granados, G., Simon, J., Rodriguez, I., & Calle, J. D. (2016). A navigation message authentication proposal for the Galileo open service. *Navigation, Journal of the Institute of Navigation, 63*(1), 85–102. https://doi.org/10.1002/navi.125
Fernandez-Hernandez, I., Chatre, E., Dalla Chiara, A., Da Broi, G., Pozzobon, O., Fidalgo, J., & Rijmen, V. (2018a). Impact analysis of SBAS authentication. *Navigation, Journal of the Institute of Navigation, 65*(4), 517–532. https://doi.org/10.1002/navi.267
Fernandez-Hernandez, I., Vecchione, G., & Daaz-Pulido, F. (2018b). Galileo authentication: A programme and policy perspective. In *Proceedings of the international astronautical congress, IAC 69th international astronautical congress: #InvolvingEveryone, IAC 2018b*, October 1, 2018b–October 5, 2018b.
Fernandez-Hernandez, I., Ashur, T., & Rijmen, V. (2021a). Analysis and recommendations for MAC and key lengths in delayed disclosure GNSS authentication protocols. *IEEE Transactions on Aerospace and Electronic Systems, 57*(3), 1827–1839. https://doi.org/10.1109/TAES.2021.3053129
Fernandez-Hernandez, I., Hirokawa, R., Rijmen, V., & Aikawa, Y. (2021b). PPP/PPP-RTK message authentication. In *Proceedings of the 34th international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2021b*, September 20, 2021b–September 24, 2021b.
Gallardo, F., & Yuste, A. P. (2020). SCER spoofing attacks on the Galileo open service and machine learning techniques for end-user protection. *IEEE Access, 8*, 85515–85532. https://doi.org/10.1109/ACCESS.2020.2992119
Gamba, M. T., Nicola, M., & Motella, B. (2020a). Galileo OSNMA: An Implementation for ARM-based Embedded Platforms. In *2020a international conference on localization and GNSS (ICL-GNSS)*.
Gamba, M. T., Nicola, M., & Motella, B. (2020b). GPS chimera: A software profiling analysis. In *Proceedings of the 33rd international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2020b*, September 22, 2020b–September 25, 2020b, Virtual, Online.
Gamba, M. T., Nicola, M., & Motella, B. (2021). Computational load analysis of a Galileo OSNMA-ready receiver for Arm-based embedded platforms. *Sensors, 21*(2), 1–21. https://doi.org/10.3390/s21020467
Ghorbani, K., Orouji, N., & Mosavi, M. R. (2020). Navigation message authentication based on one-way hash chain to mitigate spoofing attacks for GPS L1. *Wireless Personal Communications, 113*(4), 1743–1754. https://doi.org/10.1007/s11277-020-07289-z
Gkougkas, E., Dotterbock, D., Pany, T., & Eissfeller, B. (2017a). A low power authentication signal for open service signals. In *30th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2017a*, September 25, 2017a–September 29, 2017a.
Gkougkas, E., Pany, T., & Eissfeller, B. (2017b). Evaluation of new message structures for navigation message authentication. In *30th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2017b*, September 25, 2017b–September 29, 2017b.
Gkougkas, E., Arizabaleta, M., Pany, T., & Eissfeller, B. (2019). A novel authentication signal component for codeless correlation. In *ION 2019 international technical meeting proceedings Institute of Navigation International Technical Meeting 2019, ITM 2019*, January 28, 2019–January 31, 2019.
Gotzelmann, M., Koller, E., Semper, I. V., Oskam, D., Gkougkas, E., Simon, J., & de Latour, A. (2021). Galileo open service navigation message authentication: Preparation phase and drivers for future service provision. In *Proceedings of the 34th international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2021*, September 20, 2021–September 24, 2021.
Gunther, C. (2014). A survey of spoofing and counter-measures. *Navigation, Journal of the Institute of Navigation, 61*(3), 159–177. https://doi.org/10.1002/navi.65
Hein, G. W., & Avila-Rodriguez, J. A. (2005). Performance of a Galileo PRS/GPS M-code combined service. In *Proceedings of the institute of navigation, national technical meeting institute of navigation, 2005 National Technical Meeting, NTM 2005*, January 24, 2005–January 26, 2005.
Heng, L., Chou, D., & Gao, G. X. (2014). Cooperative GPS signal authentication from unreliable peers. In *27th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2014*, September 8, 2014–September 12, 2014.
Hernandez, I. F., Rijmen, V., Granados, G. S., Simon, J., Rodriguez, I., & Calle, J. D. (2014). Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service. In *27th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2014*, September 8, 2014–September 12, 2014.
Hernandez, I. F., Ashur, T., Rijmen, V., Sarto, C., Cancela, S., & Calle, D. (2019). Toward an operational navigation message authentication service: Proposal and justification of additional OSNMA protocol features. In *European navigation conference, ENC 2019*, April 9, 2019–April 12, 2019.
Hinks, J., Gillis, J. T., Loveridge, P., Miller, S., Myer, G., Rushanan, J. J., & Stoyanov, S. (2021). 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*, September 20, 2021–September 24, 2021.
Hirokawa, R., & Fujita, S. (2019). 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*, September 16, 2019–September 20, 2019.
Humphreys, T. E. (2013). Detection strategy for cryptographic gnss anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems, 49*(2), 1073–1090. https://doi.org/10.1109/TAES.2013.6494400
Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner Jr, P. M. (2008). Assessing the spoofing threat: Development of a portable gps civilian spoofer. In: *21st international technical meeting of the satellite division of the institute of navigation, ION GNSS 2008*, September 16, 2008–September 19, 2008.
Jensen, O. D., & Andersen, K. A. (2017). *A5 Encryption In GSM*. http://koclab.cs.ucsb.edu/teaching/cren/project/2017/jensen+andersen.pdf
Jia, X., Su, R., Liang, W., Shen, F., Zheng, C., Wang, Z., Wang, X., & Xu, L. (2021). Research on civil GNSS signal authentication service design. In *Lecture Notes in Electrical Engineering 12th China Satellite Navigation Conference, CSNC 2021*, May 22, 2021–May 25, 2021.
Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security, 1*(1), 36–63. https://doi.org/10.1007/s102070100002
Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics, 31*(4), 617–636. https://doi.org/10.1002/rob.21513
Laurenti, N., & Poltronieri, A. (2020). Optimal Compromise among security, availability and resources in the design of sequences for GNSS spreading code authentication. In *2020 international conference on localization and GNSS, ICL-GNSS 2020—Proceedings*, June 2, 2020–June 4, 2020.
Manandhar, D., & Shibasaki, R. (2017). Signal authentication for anti-spoofing based on QZSS L1S. In *Proceedings of the institute of navigation pacific positioning, navigation and timing meeting, pacific PNT, PACIFIC PNT 2017*, May 1, 2017–May 4, 2017.
Manandhar, D., & Shibasaki, R. (2018). 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*, September 24, 2018–September 28, 2018.

Margaria, D., Marucco, G., & Nicola, M. (2016). A first-of-a-kind spoofing detection demonstrator exploiting future Galileo E1 OS authentication. In *Proceedings of the IEEE/ION position, location and navigation symposium, PLANS 2016*, April 11, 2016–April 14, 2016.

Margaria, D., Motella, B., Anghileri, M., Floch, J.-J., Fernandez-Hernandez, I., & Paonni, M. (2017). Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives. *IEEE Signal Processing Magazine, 34*(5), 27–37. https://doi.org/10.1109/MSP.2017.2715898

Marucco, G., Ligios, M., Chala, S. A., & Rosengren, P. (2020). Galileo open service navigation message authentication: Exploitation in the frame of an E-security infrastructure. In *2020 European Navigation Conference, ENC 2020*, November 23, 2020–November 24, 2020.

Mina, T., Kanhere, A., Kousik, S., & Gao, G. (2021). Continuous GPS authentication with chimera using stochastic reachability analysis. In *Proceedings of the 34th international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2021*, September 20, 2021–September 24, 2021.

Mohan Naik, R., Sathyanarayana, S. V., & Sowmya, T. K. (2020). Key Management Using Elliptic Curve Diffie Hellman Curve 25519. In *MPCIT 2020—Proceedings: IEEE 3rd international conference on "multimedia processing, communication and information technology"*, MPCIT 2020, December 11, 2020–December 12, 2020.

Motella, B., Gamba, M. T., & Nicola, M. (2020). A real-time OSNMA-ready software receiver. In *ION 2020 international technical meeting proceedings* Institute of Navigation International Technical Meeting 2020, ITM 2020, January 21, 2020–January 24, 2020.

Motella, B., Nicola, M., & Damy, S. (2021). Enhanced GNSS authentication based on the joint CHIMERA/OSNMA scheme. *IEEE Access, 9*, 121570–121582. https://doi.org/10.1109/ACCESS.2021.3107871

Mukherjee, C. S., Roy, D., & Maitra, S. (2021). Design specification of ZUC stream cipher. In C. S. Mukherjee, D. Roy, & S. Maitra (Eds.), *Design and cryptanalysis of ZUC: A stream cipher in mobile telephony* (pp. 43–62). Springer. https://doi.org/10.1007/978-981-33-4882-0_3

Nicola, M., Motella, B., & Gamba, M. T. (2020). The chimera solution: Performance assessment. In *2020 European navigation conference, ENC 2020*, November 23, 2020–November 24, 2020.

Nicola, M., Motella, B., & Gamba, M. T. (2021). GPS chimera: A software receiver implementation. In *Proceedings of the 34th international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2021*, September 20, 2021–September 24, 2021.

Nicola, M., Motella, B., Pini, M., & Falletti, E. (2022). Galileo OSNMA public observation phase: Signal testing and validation. *IEEE Access, 10*, 27960–27969. https://doi.org/10.1109/ACCESS.2022.3157337

O'Driscoll, C., & Fernandez-Hernandez, I. (2020). Mapping bit to symbol unpredictability in convolutionally encoded messages with checksums, with application to galileo osnma. In *Proceedings of the 33rd international technical meeting of the satellite division of the institute of navigation, ION GNSS+ 2020*, September 22, 2020–September 25, 2020, Virtual, Online.

O'Hanlon, B. W., Psiaki, M. L., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013). Real-time GPS spoofing detection via correlation of encrypted signals. *Navigation, Journal of the Institute of Navigation, 60*(4), 267–278. https://doi.org/10.1002/navi.44

Pande, A. S., & Thool, R. C. (2016). Survey on logical key hierarchy for secure group communication. In *International conference on automatic control and dynamic optimization techniques, ICACDOT 2016*, September 9, 2016–September 10, 2016.

Perrig, A., Song, D., Canetti, R., Tygar, J. D., & Briscoe, B. (2005). *Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction*. https://www.rfc-editor.org/rfc/rfc4082

Poltronieri, A., Caparra, G., & Laurenti, N. (2018). Analysis of the chimera time-binding scheme for authenticating GPS l1c. In *ESA workshop on satellite navigation technologies and European workshop on GNSS signals and signal processing, NAVITEC*, December 5, 2018–December 7, 2018.

Pozzobon, O., Canzian, L., Danieletto, M., & Chiara, A. D. (2010). Anti-spoofing and open GNSS signal authentication with signal authentication sequences. In *Programme and abstract Book—5th ESA workshop on satellite navigation technologies and European workshop on GNSS signals and signal processing, NAVITEC 2010*.

Pozzobon, O., Gamba, G., Canale, M., & Fantinato, S. (2014). Supersonic GNSS authentication codes. In *27th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2014*, September 8, 2014–September 12, 2014.

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE, 104*(6), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

Psiaki, M., & Humphreys, T. (2021). Civilian GNSS spoofing, detection, and recovery. In *Position, navigation, and timing technologies in the 21st century: Integrated satellite navigation, sensor systems, and civil applications* (pp. 655–680). IEEE. https://doi.org/10.1002/9781119458449.ch25

Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013). GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems, 49*(4), 2250–2267. https://doi.org/10.1109/TAES.2013.6621814

Rugamer, A., Neumaier, P., Sommer, P., Garzia, F., Rohmer, G., Konovaltsev, A., Baumann, S. (2014a). BaSE-II: A robust and experimental Galileo PRS receiver development platform. In *27th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2014a*, September 8, 2014a–September 12, 2014a.

Rugamer, A., Stahl, M., Lukin, I., & Rohmer, G. (2014b). Privacy protected localization and authentication of georeferenced measurements using Galileo PRS. In *Record—IEEE PLANS, Position Location and Navigation Symposium*, May 5, 2014b–May 8, 2014b.

Rugamer, A., Rubino, D., Lukcin, I., Taschke, S., Stahl, M., & Felber, W. (2016). Secure position and time information by server side PRS snapshot processing. In *29th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2016*, September 12, 2016–September 16, 2016.

Rugamer, A., Garzia, F., Meister, D., Van Der Merwe, J. R., Taschke, S., Zubizarreta, X., Wendel, J. (2020). Enhanced robustness and spoofing resistance by Galileo PRS processing. In *2020 European navigation conference, ENC 2020*, November 23, 2020–November 24, 2020.

SAC. (2016a). Information security techniques - SM3 cryptographic hash algorithm. In (Vol. GB/T 32905–2016a): Standardization Administration of China.

SAC. (2016b). Information security technology - SM4 block cipher algorithm. In (Vol. GB/T 32907–2016b): Standardization Administration of China.

SAC. (2017). *Information security technology—SM2 cryptographic algorithm usage specification*. In (Vol. GB/T 35276–2017): Standardization Administration of China.

SAC. (2020). *Interface specification for signal in space of Beidou navigation satellite system—Part 1: Open service signal B1C*. In (Vol. GB/T 39414.1–2020): Standardization Administration of China.

Sarto, C., Pozzobon, O., Fantinato, S., Montagner, S., Fernandez-Hernandez, I., Simon, J., Gohler, E. (2017). Implementation and testing of OSNMA for Galileo. In *30th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2017*, September 25, 2017–September 29, 2017.

Schielin, E., Allien, A., Taillandier, C., Jeannot, M., & Brocard, D. (2012). On the foundation of GNSS authentication mechanisms. In *25th international technical meeting of the satellite division of the institute of navigation 2012, ION GNSS 2012*, September 17, 2012–September 21, 2012.

Scott, L. (2013). *Spoofing*. I. GNSS. https://insidegnss.com/spoofing/

Scott, L. (2014). Introductory remarks: Session C3b: GNSS authentication. In *27th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2014*, September 8, 2014–September 12, 2014.

Swider, R., Dickshinski, D., Robb, R., & Martel, J. (2000). GPS selective availability: A retrospective. In *IAIN World Congress and the 56th Annual Meeting of The Institute of Navigation (2000)*.

Tosato, L., Dalla Chiara, A., Pozzobon, O., Serrano, G. F., Calabrese, A., Wullems, C., Vecchione, G. (2021). Broadcast data authentication concepts for future SBAS services. In *ION 2021 international technical meeting proceedings* 2021, Institute of Navigation International Technical Meeting, ITM 2021, January 25, 2021–January 28, 2021, Virtual, Online.

Turner, M., Chambers, A., Mak, E., Aguado, L. E., Wales, B., & Dumville, M. (2013). PROSPA: Open service authentication. In *26th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2013*, September 16, 2013–September 20, 2013.

Turner, M., Richardson, A., Haddon, J., Batiste, M., Aguado, E., Wales, B., Togneri, P. (2015). Galileo public regulated services (PRS) with limited key distribution. In *28th international technical meeting of the satellite division*

of the institute of navigation, ION GNSS 2015, September 14, 2015–September 18, 2015.
Walker, P., Rijmen, V., Fernandez-Hernandez, I., Bogaardt, L., Seco-Granados, G., Simon, J., Pozzobon, O. (2015). Galileo open service authentication: A complete service design and provision analysis. In *28th international technical meeting of the satellite division of the institute of navigation, ION GNSS 2015*, September 14, 2015–September 18, 2015.
Walter, T., Anderson, J., & Lo, S. (2021). 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*, September 20, 2021–September 24, 2021.
Wang, F., Li, H., Yang, Y., & Lu, M. (2016). GNSS spoofing detection based on collaborative RAIM. In *Institute of navigation international technical meeting 2016, ITM 2016*, January 25, 2016–January 28, 2016.
Wang, S., Liu, H., Tang, Z., & Ye, B. (2021). Binary phase hopping based spreading code authentication technique. *Satellite Navigation*. https://doi.org/10.1186/s43020-021-00037-z
Wang, H., Tang, X., Yuan, M., & Ou, G. (2022). Dispersion analysis of ranging-code markers applied to beidou B1C signal based on Chimera. In *Lecture Notes in Electrical Engineering 13th China satellite navigation conference, CSNC 2022*, May 25, 2022–May 27, 2022.
Wesson, K. D., Rothlisberger, M. P., & Humphreys, T. E. (2011). A proposed navigation message authentication implementation for civil GPS anti-spoofing. In *24th international technical meeting of the satellite division of the institute of navigation 2011, ION GNSS 2011*, September 19, 2011–September 23, 2011.
Wesson, K., Rothlisberger, M., & Humphreys, T. (2012). Practical cryptographic civil GPS signal authentication. *Navigation, Journal of the Institute of Navigation, 59*(3), 177–193. https://doi.org/10.1002/navi.14
Wu, Z., Zhang, Y., & Liu, R. (2020). BD-II NMASSI: An scheme of anti-spoofing and open BeiDou II D2 navigation message authentication. *IEEE Access, 8*, 23759–23775. https://doi.org/10.1109/ACCESS.2020.2970203
Wullems, C., Tosato, L., Dalla Chiara, A., Pozzobon, O., Serrano, G. F., & Mabilleau, M. (2021). Management of active data and authentication in future SBAS receivers. In *ION 2021 International Technical Meeting Proceedings 2021 Institute of Navigation International Technical Meeting, ITM 2021*, January 25, 2021–January 28, 2021, Virtual, Online.
Yuan, M., Lv, Z., Chen, H., Li, J., & Ou, G. (2017). An implementation of navigation message authentication with reserved bits for civil BDS anti-spoofing. In *Lecture Notes in Electrical Engineering 8th China Satellite Navigation Conference, CSNC 2017*, May 23, 2017–May 25, 2017.
Yuan, M., Tang, X., Lou, S., Ma, C., & Ou, G. (2022a). Cross-Correlation Based Spreading Code Authentication Scheme for Civil GNSS Signals. In *Lecture Notes in Electrical Engineering 13th China Satellite Navigation Conference, CSNC 2022a*, May 25, 2022a–May 27, 2022a.
Yuan, M., Tang, X., Sun, P., Huang, Y., & Ou, G. (2022b). *Randomly Flipped Chip based signal power authentication for GNSS civilian signals*. https://doi.org/10.1049/rsn2.12341 (IET Radar, Sonar and Navigation)
Zhang, K., & Papadimitratos, P. (2019). On the effects of distance-decreasing attacks on cryptographically protected GNSS signals. In *ION 2019 international technical meeting proceedings institute of navigation international technical meeting 2019, ITM 2019*, January 28, 2019–January 31, 2019.

Publisher's Note