Cross-Correlation Based Spreading Code Authentication Scheme for Civil GNSS Signals

Muzi Yuan, Xiaomei Tang, Shengqiang Lou, Chunjiang Ma, and Gang Ou(✉)

National University of Defense Technology, Changsha 410073, China
ougangcs@139.com

Abstract. Navigation signal authentication schemes are effective methods to protect civilian receivers against spoofing attacks by providing unforgeable information to verify the authenticity of signals. In this paper Cross-Correlation based Spreading Code Authentication, or CC-SCA, is proposed to authenticate GNSS civilian signals at high time resolution with small storage requirement. CC-SCA employs a cryptographically generated authentication spreading code punctured into public spreading code in civilian signals. Since initial code phases of authentication spreading code are different and derived from security code, a correlation peak can be detected and authenticated in the cross-correlation between baseband signals of different satellites. According to this principle, signal structure and authenticable receiver architecture are proposed while performance metrics and the selection of parameters are analysed. Finally, this scheme is demonstrated with a specific implementation and parameter selection for Beidou B1C civilian signals.

Keywords: Navigation signal authentication · Spreading code authentication · Cross-correlation · Authentication implementation

1 Introduction

Signals of Global Navigation Satellite System (GNSS) are broadcasted with structure details published in Interface Control Documents (ICDs), which makes GNSS an open service with unlimited capacity. However, this characteristic also makes GNSS signals exposed to threats of spoofing attacks performed by generating counterfeit signals. If receivers fail to detect whether the processing signal is forged, spoofing attacks may mislead the positioning, navigation, and timing results and damage the robustness of applications rely on GNSS service. In order to protect the security and authenticity of satellite navigation services, receiver observation based spoofing detections and navigation signal authentications are employed to detect and mitigate spoofing attacks [1]. The observation-based methods detect spoofing attacks through signal and information processing algorithms in receivers. These methods have good adaptation to various navigation signals, while the complexity of anti-spoofing receivers will increase. The authentication-based methods require modifications to navigation signal, while the robustness and security of spoofing detection will be significantly improved. In recent

C. Yang and J. Xie (Eds.): *China Satellite Navigation Conference (CSNC 2022) Proceedings*, LNEE 909, pp. 503–514, 2022.
https://doi.org/10.1007/978-981-19-2580-1_43

years, authentication capability becomes an important aspect of developing trend in most GNSS designs.

Being researched for nearly two decades, there are two main structures proposed for navigation signal authentication: navigation message authentication (NMA) and spreading code authentication (SCA) [2–4]. In practice, NMA is adopted by Galileo as Open Service Navigation Message Authentication [5] (OSNMA) and SCA is adopted by GPS as Chip-Message Robust Authentication [6] (Chimera). At present, OSNMA has been tested in the broadcast signal of Galileo satellites [7] and Chimera will be evaluated and tested on the experimental satellites NTS-3 [8].

Security of NMA is limited by the low symbol rate of navigation messages that may face the threat of security code estimation and replay (SCER) attacks. In this form of spoofing attack, attackers first evaluate the unpredictable symbols in navigation message from authentic navigation signals and then reconstruct counterfeit signals with these estimated symbols. Spoofing signals in SCER form can be constructed with the same authentic message and arbitrarily controlled code phase, which may bypass the NMA scheme [9]. To protect receivers from SCER attack, observation-based detections are used to assist the authentication process, which may increase the complexity of receivers. SCA schemes benefit from the high chip rate of spreading code and immune to SCER attacks in most cases. However, mainstream SCA schemes that authenticate the signal through correlation of local code with received navigation signals may require long-term buffering of navigation signal samples [6] or authorization key distribution to the receiver [2], which will put great pressure on the storage or communication capacity.

To avoid the limitations discussed above, in this paper Cross-Correlation based Spreading Code Authentication (CC-SCA) is proposed to jointly authenticate the navigation message and the spreading code with a small extra storage requirement. The design principle of CC-SCA is to replace part of the public spreading code with authentication spreading code generated by cryptographic algorithms. The initial code phase of this authentication spreading code varies in different PRN numbers and is derived from an extractable security code. In this structure, energy can be accumulated by cross-correlating the baseband of navigation signals with different PRN numbers and a correlation peak of authentication code will appear in the result. The existence and the code phase of correlation peak are defined as the statistic of authentication. This navigation signal authentication scheme takes advantage of the SCA characteristics that immune to SCER attacks and at the same time avoids a long-term storage of navigation signal samples. This paper makes three principal contributions. First, structure of CC-SCA authentication signal and authenticable receiver is proposed. Second, performance metrics and parameter choices are discussed. Third, an implementation example for Beidou B1C civilian signal is demonstrated.

The rest of this paper is divided into five sections. Section 2 proposes the structure and mathematical model of the CC-SCA signal. Section 3 discusses the structure and processing algorithms for CC-SCA receivers. Section 4 analyses the performance metrics and the choice of parameters of the scheme; Sect. 5 demonstrates CC-SCA through an implementation for Beidou B1C civilian signal. Section 6 summarizes the work and draws the conclusion.

2 Model of CC-SCA Signal

2.1 Signal Architecture

The architecture of CC-SCA signal remains the same as legacy navigation signal, which consists of a three-layer structure of navigation message, spreading code and carrier. The mathematical model of CC-SCA signal at PRN number i is shown in Eq. (1).

$$s_i(t) = \mathrm{Re}\left\{A_s C_i^{(auth)}(t) D_i^{(auth)}(t)\exp(2\pi f_c t + \varphi_0)\right\} \tag{1}$$

Here A_s is the amplitude of the signal, f_c and φ_0 are frequency and initial phase of carrier, $C_i^{(auth)}(t)$ and $D_i^{(auth)}(t)$ are spreading code and navigation message at PRN number i with authentication information. The initial code phase of authentication code is derived from security code, which also authenticates the navigation message. Security code can be included in the navigation message to ensure an NMA-only capability. The authentication architecture of CC-SCA signal is illustrated in Fig. 1.

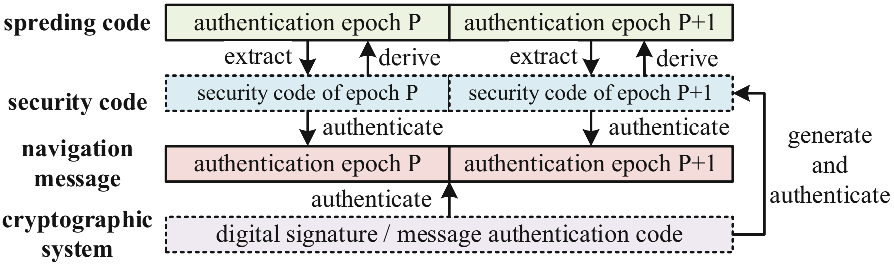

Fig. 1. The authentication architecture of CC-SCA signal.

The authentication epoch defines the lifetime of a single security code, in which all authentication code is derived from the same security code. Security code and authentication code in different epochs remain independent and can be separately authenticated. The length of an epoch is set as multiple periods of civilian spreading code and in practice often equals to the length of a frame in navigation message.

This architecture provides a joint authentication of spreading code and navigation message, ensuring that the navigation message and the spreading code in CC-SCA signal cannot be generated separately.

2.2 Structure of Authenticable Spreading Code

Authenticable spreading code is the core component of CC-SCA signal, which consists of public civilian spreading code and secret authentication spreading code. Civilian spreading code varies with PRN numbers while authentication spreading code remains the same sequence but varies in initial code phase at every PRN number. Authentication spreading code also changes its sequence in every period of civilian spreading code. The model of CC-SCA spreading code at PRN number i is shown in Eq. (2).

$$C_i^{(auth)}(n) = \begin{cases} C_{auth}^{(N)}\left(k - K_i^{(N)}\right) & n \in \{N_{auth}\} \\ C_i(n) & n \notin \{N_{auth}\} \end{cases} \tag{2}$$

Here $C_i^{(auth)}(n)$ is the authenticable spreading code, $C_i(n)$ is the civilian spreading code at PRN number i, $C_{auth}^{(N)}(n)$ is the authentication spreading code of period N in civilian spreading code, which changes in every period. The initial code phase is cyclic controlled with $C_{auth}^{(N)}(-n) = C_{auth}^{(N)}(L_{auth} - n)$ where L_{auth} is the total chip count of authentication spreading code. And $K_i^{(N)}$ is the initial code phase of authentication spreading code at PRN number i in period N and is derived from security code. The position of replacement is indicated by a set $\{N_{auth}\}$ with scale L_{auth} and index k_n represents that n is the k_n th element in set $\{N_{auth}\}$. The structure of the spreading code in CC-SCA signal is shown in Fig. 2.

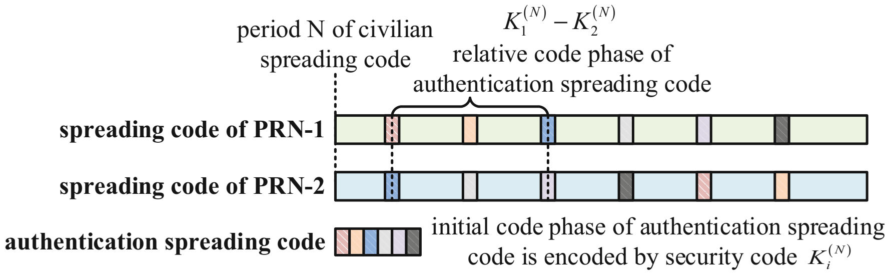
period N of civilian spreading code
$K_1^{(N)} - K_2^{(N)}$
relative code phase of authentication spreading code
spreading code of PRN-1
spreading code of PRN-2
authentication spreading code
initial code phase of authentication spreading code is encoded by security code $K_i^{(N)}$

Fig. 2. Structure of civilian spreading code periods modified by CC-SCA authentication codes.

When calculating the cross-correlation of two streams of spreading code with different PRN number, a correlation peak of authentication spreading code will be accumulated at a certain code phase. This code phase equals to the difference of their initial code phase $K_2^{(N)} - K_1^{(N)}$, from which the security code can be extracted and authenticated.

In order to further improve the detection probability of the authentication spreading code, the initial code phase of authentication spreading code sequences in multiple periods can be set to the same value (e.g., derived from the same security code). One security code may control multiple periods of civilian spreading code and the receiver can obtain a better robustness by accumulating multi-period cross-correlation results.

2.3 Design of Security Code

The design of security code is to ensure that receiver can extract it from any two streams of authenticable spreading code. In the design of CC-SCA, security code itself is a digital signature generated by signing the navigation message in the authentication epoch through asymmetrical cryptographic systems. The generation and authentication of the security code is shown in Fig. 3.

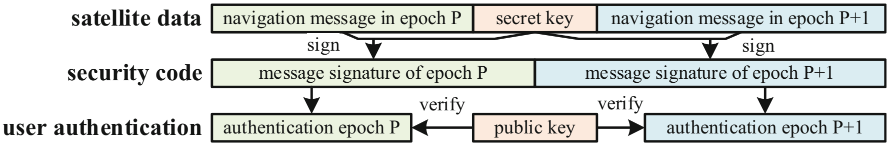

Fig. 3. Generation and authentication structure of security code.

The signature is generated and verified through digital signature algorithms such as SM2 or ECDSA that satellites sign the message with the private keys and users verify the signature with the public keys corresponding to those private keys. Digital signature is easy to be generated and verified, but is not feasible to recover the private key from any signatures. In this section, it is assumed that each security code obtained by calculation can be expressed as a binary sequence with a length of L bits.

Security code derives the initial code phase of authentication spreading code through encoding the phase as below. First, a proper prime number L_{auth} is selected as the length of authentication code in one period of civilian spreading code, mark $M = \lfloor \log_2(L_{auth}) \rfloor$ as the encoding bit in one segment. Second, security code $S^{(P)}$ in authentication epoch P is divided evenly into L/M segments with a M bits length each, marked as $\left\{ s_1^{(P)}, s_2^{(P)}, \ldots, s_{L/M}^{(P)} \right\}$. Finally, the initial code phase of authentication spreading code at PRN number i can be defined as Eq. (3).

$$K_i^{((P-1)\times L/M+j)} = i \times s_j^{(P)} \mod L_{auth} \tag{3}$$

Here $j = 1, 2, \ldots, L/M$. Equation (3) ensures a fixed relationship in code phase between different PRN numbers. For example, the difference of initial code phase between PRN number a and b (assuming $a > b$) is $(a - b) \times s_j^{(P)} \mod L_{auth}$. Since L_{auth} is prime, in Galois Field $GF(L_{auth})$ every element has a unique multiplicative inverse. The segment of security code can be extracted by multiplying the multiplicative inverse to the difference of initial code phase. When multiple segments are extracted, a full security code can be merged and authenticated by verifying whether the security code is a valid signature of navigation message.

Besides the signature scheme discussed above, symmetric cryptographic systems or crypto hash systems such as Timed Efficient Stream Loss-tolerant Authentication (TESLA) [10] can also be adopted as security code generation algorithms. The core derivation precept remains the same in these alternative algorithms.

2.4 Navigation Message

The navigation message of the CC-SCA signals can remain the same as legacy navigation signals, or the security code described in previous section can be included in the message. Detailed design principles of authenticable navigation message and its variations have been discussed in our previous works [11, 12].

3 Structure of Authenticable Receiver

The authenticable receiver of CC-SCA authenticates the security code by performing cross-correlation calculations on the baseband signals between different tracking channels. The structure of a typical authenticable receiver is shown in Fig. 4. Shaded parts are conventional processing steps in legacy receivers; dashed lines are optional processing steps; blue parts are blocks to improve processing SNR in authentication; green parts are signal authentication blocks.

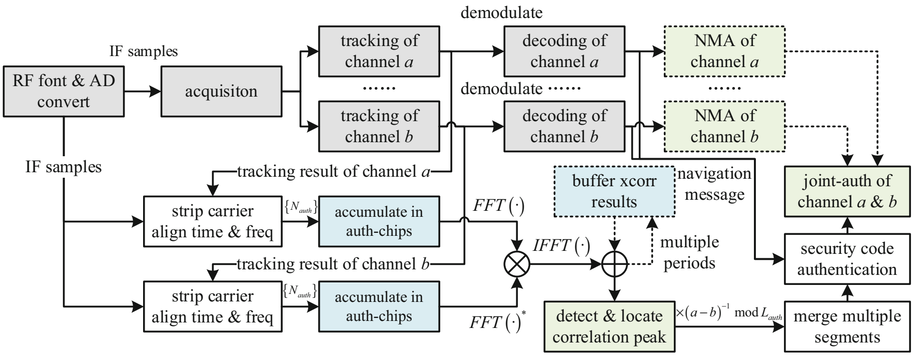

Fig. 4. Structure of signal processing and authentication in a typical receiver with CC-SCA scheme.

Estimations from tracking loops are used to strip the carrier and align the frequency of the intermediate frequency (IF) samples to obtain a time-aligned baseband signal of each PRN number. Then, samples in each chip of authentication spreading code are accumulated according to $\{N_{auth}\}$ that the receiver will get a sample for each authentication spreading code. Finally, the cross-correlation is performed and the results of multiple periods can be accumulated for a higher processing SNR. The computational complexity of cross-correlation operation between channels can be reduced through Fast Fourier Transform (FFT) and its inverse transformation.

The existence of the correlation peak can be tested through a hypothesis testing mentioned in [9]. If the hypothesis that no peak exists is accepted, it indicates that at least one channel may be spoofed by counterfeit signal without authentication spreading code. A further authentication can be made by checking correlation results with other channels. If a correlation peak is detected, segment of security code $s^{(P)}$ can be extracted through Eq. (4) from the code phase $E_j^{(P)}$ of the correlation peak.

$$s_j^{(P)} = E_j^{(P)} \times (a-b)^{-1} \mod L_{auth} \tag{4}$$

Here $a > b$ is the PRN number of the two channel being cross-correlated, $(a-b)^{-1}$ is the multiplicative inverse of $(a-b)$ in Galois Field $GF(L_{auth})$. A digital signature can be obtained by merging the security code segments of multiple periods of civilian spreading code. Through the public key disclosed by the authentication system to all users, the authenticable receiver can verify the consistency of the digital signature and the navigation message, thereby verifying the authenticity of the navigation signal. If security code is included in the navigation message, an NMA process can also be performed to assist the joint authentication of these channels.

4 Parameters and Performance Metrics

Performance metrics of navigation authentication schemes can be categorized as robustness, security, efficiency and cost. Since performance is deeply influenced by parameter selections, parameters need to be chosen cautiously in every specific case. Variable parameters in CC-SCA are defined in Table 1.

Table 1. Variable parameters of authenticable signals in CC-SCA scheme.

Label	Comment
L_{auth}	Length of authentication spreading code in a single period of civilian spreading code, also defines the parameter of Galois Field
RC_{auth}	Periodically repeat times of authentication spreading code with a same initial code phase
L_{SC}	Bit length of a security code, such as the length of a digital signature

Other parameters of CC-SCA can be derived from Table 1 as: duty factor DF_{auth} represents the ratio of authentication spreading code in a period of civilian spreading code; length of security code segment M is the bit length of security code deriving initial code phase in a single period of civilian spreading code and number of segments to construct a security code $N_{SC} = L_{SC}/M$; time length of a security code segment $T_{auth} = RC_{auth} \times T_{CP}$, here T_{CP} is the period of civilian spreading code and commonly set to 1 ms or 10 ms.

4.1 Robustness

The robustness is assessed through the detection probability metric under a constant probability of false alarm. The cross-correlation of authentication spreading codes of satellite signals is affected by the noise of both two baseband signals and will suffer a loss in C/N0. The result can be expressed by Eq. (5).

$$\begin{aligned} R^{(auth)}(\tau) &= \int \left[A_i C^{(auth)}(t) + n_0(t)\right]\left[A_j C^{(auth)}(t-\tau) + n_0(t-\tau)\right] dt \\ &= A_i A_j R_{ij}(\tau) + A_i N_r + A_j N_r \end{aligned} \tag{5}$$

Here A_i and A_j are amplitudes of two signals, N_r is the noise in correlation. The minimum loss in C/N$_0$ is 6 dB when the powers of two signals are equal. Take Beidou B1C signal as an example, when 1031 chips out of 10230 chips of civilian spreading code are replaced, there will be a CC-SCA signal with L_{auth} set to 1031, DF_{auth} is 10.08% and M is 10 bits. Figure 5 shows the relationship between detection probability and C/N$_0$ of the signal under different T_{auth} settings.

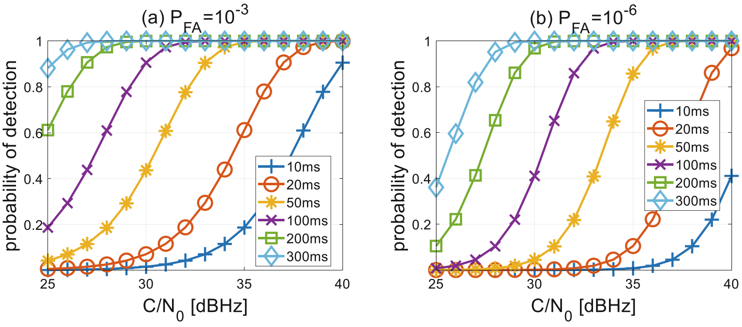

Fig. 5. Probability of detection vs. collection time of authentication spreading codes vs. C/N$_0$ of signal when $P_{FA} = 10^{-3}$ in (a) and $P_{FA} = 10^{-6}$ in (b) when duty factor is 10.08%.

The length of security code segment should be determined comprehensively with reference to the false alarm probability target, the typical C/N$_0$ condition and the authentication efficiency in practice.

4.2 Security

The security metric mainly describes the probability for attackers to forge authentication signals. This forgery of an authentication signal includes two perspectives: cryptographical forgery and signal forgery. The cryptographical security is mainly protected by the cryptographic algorithm which can be expressed by the effective length of the key. In CC-SCA this metric is the length of the private key. The signal security is mainly evaluated by its vulnerability to SCER attacks [9].

The security code of CC-SCA signal is modulated by the code phase of secret authentication spreading codes. Since the authentication spreading code changes in each civilian spreading code period, it is not feasible to recover them in advance of the real signal. Besides, the time resolution of the security code modulation is in multiple-chip level which is slightly worse than chip level in Chimera scheme. It is difficult to perform an SCER attack under properly selected parameters of CC-SCA. Based on the above analysis, CC-SCA has a slightly damaged security metric as Chimera.

4.3 Efficiency

The efficiency metric is mainly evaluated through time to first authenticated fix (TTFAF) and time between authentications (TBA). The former is the time from acquisition to the completion of the first authentication, which affects the use efficiency of the receiver; the latter is the time interval between two authentications, which affects the response speed of spoof detection.

When public key is loaded, the TTFAF and TBA of CC-SCA are both the time for completely receiving a security code, which can be expressed in Eq. (6).

$$TTFAF = TBA = T_{auth} \times \left\lceil \frac{L_{SC}}{M} \right\rceil \tag{6}$$

The efficiency can be effectively improved by reducing the length of the authentication epoch or increasing the duty factor of the authentication spreading code, while these modifications will reduce the robustness or increase the C/N$_0$ loss in processing civilian signal. In practice, there is a tradeoff between efficiency and robustness.

4.4 Cost

Cost metric mainly includes three categories: performance deterioration of receivers without authentication, communication overhead, and calculation and storage complexity of receivers and satellites. Due to the replacement of the authentication spreading code in civilian spreading code, the receiver will suffer a loss in C/N0 when only processing the civilian spreading code. The relationship between loss of C/N0 and duty factor DF_{auth} can be expressed as Eq. (7) and illustrated in Fig. 6 (a).

$$CNR_{loss}(dB) = 10 \times \log_{10}(1 - DF_{auth})^2 \tag{7}$$

Loss in C/N$_0$ will be less than 1 dB when the duty factor is at about 10%, which is acceptable for both signal processing and authentication. While the trust foundation of CC-SCA is built on asymmetric cryptographic system with published public keys, there is no requirement for any communication overheads. Besides, CC-SCA is able to authenticate both channels involved in correlation, which halves the complexity to authenticate all channels.

Compared to Chimera scheme in GPS, CC-SCA significantly reduces the requirement of storage. Since authentication detection is based on the cross-correlation of baseband signals, receiver only needs to buffer the baseband signal in a single authentication period. When quantization is set to 2 bit and sampling frequency is 10 MHz [6], the storage requirement of CC-SCA and Chimera is shown in Fig. 6 (b).

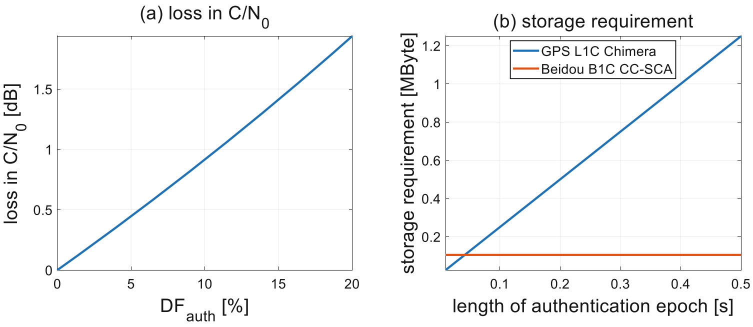

Fig. 6. (a) loss in C/N$_0$ as function of duty factor of authentication spreading code; (b) minimum storage requirement vs. collection time of a single authentication fix.

The minimum storage required for Chimera is significantly greater than the requirement for CC-SCA when the length of a single authentication epoch is larger than 100 ms. According to the detection probability analysis of Chimera [6], data storage requirement in Chimera is 3.6 times to the requirement in CC-SCA for a typical single authentication signal length of 150 ms.

5 Implementation for Beidou B1C

Considering results in Sect. 2 and Sect. 4, this section gives a set of specific implementation parameters for the Beidou B1C civilian signal. Performance comparison is listed with Galileo E1 OSNMA and GPS L1C Chimera. The parameter selection of CC-SCA signal for Beidou B1C civilian signal is shown in Table 2.

Table 2. Variable selections of CC-SCA authenticable signal for Beidou B1C civilian signal.

Parameter	Selection	Comment
L_{auth}	1031	Duty factor is 10.08%, loss in C/N$_0$ is under 1 dB
RC_{auth}	34	Length of a single security code segment is 340 ms, 52 segments are included in a frame of navigation message
L_{SC}	512	Length of digital signature of SM2 algorithm

A list of performance metrics of Beidou B1C CC-SCA, Galileo E1 OSNMA and GPS L1C Chimera are shown in Table 3.

Table 3. Variable choice of CC-SCA authenticable signal for Beidou B1C civilian signal.

Performance metric	CC-SCA	OSNMA	Chimera
Detection probability $P_{FA} = 10^{-6}$@30 dBHz	99.87% @340 ms	~100%	~97% @150 ms accumulation
SCER vulnerability	Invulnerable	Vulnerable	Invulnerable
TTFAF (s)	18	52	180 at slow channel
TBA (s)	18	30	180 at slow channel
Loss in C/N_0 (dB)	0.9158	0	1.121
storage requirement	0.1041	~0	0.375

CC-SCA scheme maintains the same detection probability as OSNMA and Chimera while saves large portions of storage space compared to Chimera. Since the security code can be extracted directly from the authentication spreading code, the authentication efficiency of CC-SCA is better than OSNMA and the slow channel authentication of Chimera because CC-SCA authenticates the signal with the receiving of spreading code and does not need to establish any fast-channel-like scheme.

6 Conclusion

This paper proposes a navigation signal authentication scheme CC-SCA for civilian GNSS signals. By puncturing cryptographically generated spreading code into public spreading code in civilian signals, a correlation peak can be detected in the cross-correlation between baseband signals of different satellites. Since initial code phases of the punctured spreading code are different and derived from security code, security code can be extracted for authentication in receivers. CC-SCA takes advantage of the high chip rate of spreading code that is invulnerable to SCER, and avoids long-term storage of navigation signal samples.

Performance analysis and comparison shows that the CC-SCA scheme has a detection probability equivalent to mainstream navigation authentication schemes, and has advantages in authentication efficiency and receiver storage overhead.

References

1. Psiaki, M., Humphreys, T.: Civilian GNSS spoofing, detection, and recovery. In: Position, Navigation, and Timing Technologies in the 21st Century, pp. 655–680 (2021)
2. Scott, L.: Anti-spoofing & authenticated signal architectures for civil navigation systems. In: ION GPS/GNSS 2003, pp. 1543–1552 (2003)
3. Fernandez Hernandez, I., Rijmen, V., et al.: Design drivers, solutions and robustness assessment of navigation message authentication for the Galileo open service. In: ION GNSS + 2014, pp. 2810–2827 (2014)
4. Margaria, D., Motella, B., et al.: Signal structure-based authentication for civil GNSSs: recent solutions and perspectives. IEEE Signal Process. Mag. **34**(5), 27–37 (2017)

5. Walker, P., Rijmen, V., et al.: Galileo open service authentication: a complete service design and provision analysis. In: ION GNSS+ 2015, pp. 3383–3396 (2015)
6. Anderson, J., Carroll, K., et al.: Chips-message robust authentication (Chimera) for GPS civilian signals. In: ION GNSS+ 2017, pp. 2388–2416 (2017)
7. Gotzelmann, M., Koller, E., et al.: Galileo open service navigation message authentication: preparation phase and drivers for future service provision. In: ION GNSS+ 2021, pp. 385–401 (2021)
8. Hinks, J., Gillis, J., et al.: Signal and data authentication experiments on NTS-3. In: ION GNSS+ 2021, pp. 3621–3641 (2021)
9. Humphreys, T.: Detection strategy for cryptographic GNSS anti-spoofing. IEEE Trans. Aerosp. Electron. Syst. **49**(2), 1073–1090 (2013)
10. Perrig, A., Canetti, R., et al.: The TESLA broadcast authentication protocol. CryptoBytes **5** (2), 2–13 (2002)
11. Yuan, M., Lv, Z., Chen, H., Li, J., Ou, G.: An implementation of navigation message authentication with reserved bits for civil BDS anti-spoofing. In: Sun, J., Liu, J., Yang, Y., Fan, S., Yu, W. (eds.) CSNC 2017. LNEE, vol. 438, pp. 69–80. Springer, Singapore (2017). https://doi.org/10.1007/978-981-10-4591-2_6
12. Yuan, M., Liu, Z., Tang, X., Lou, S., Ou, G.: Design of navigation message authentication assisted by ground based augmentation systems. In: Sun, J., Yang, C., Guo, S. (eds.) CSNC 2018. LNEE, vol. 497, pp. 779–787. Springer, Singapore (2018). https://doi.org/10.1007/978-981-13-0005-9_64
13. Shnidman, D.: The calculation of the probability of detection and the generalized marcum Q-function. IEEE Trans. Inf. Theory **35**(2), 389–400 (1989)
14. Sarto, C., Pozzobon O., et al.: Implementation and testing of OSNMA for Galileo. In: ION GNSS+ 2017, pp. 1508–1519 (2017)
15. Nicola, M., Motella, B.: The Chimera solution: performance assessment. In: The European Navigation Conference ENC (2020)