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

ORIGINAL ARTICLE Open Access

# Binary phase hopping based spreading code authentication technique

Shenran Wang, Hao Liu, Zuping Tang* and Bin Ye

**Abstract**

Civil receivers of Global Navigation Satellite System (GNSS) are vulnerable to spoofing and jamming attacks due to their signal structures. The Spreading Code Authentication (SCA) technique is one of the GNSS message encryption identity authentication techniques. Its robustness and complexity are in between Navigation Message Authentication (NMA) and Navigation Message Encryption (NME)/Spreading Code Encryption (SCE). A commonly used spreading code authentication technique inserts unpredictable chips into the public spreading code. This method changes the signal structure, degrades the correlation of the spreading code, and causes performance loss. This paper proposes a binary phase hopping based spreading code authentication technique, which can achieve identity authentication without changing the existing signal structure. Analysis shows that this method can reduce the performance loss of the original signal and has good compatibility with the existing receiver architecture.

**Keywords:** Global navigation satellite system, Message encryption, Spreading code authentication, Binary phase hopping

## Introduction

Global Navigation Satellite System (GNSS) is an important national infrastructure, which plays a key role in vehicle navigation, civil aviation, financial transactions and many others (Liang et al. 2013). GNSS civil receivers are vulnerable to spoofing and jamming attacks because the format and modulation of GNSS civil signals are public ("GPS Interface Control Documents IS-GPS-200G" 2012; Humphreys 2013), and there exist obvious security vulnerabilities (Guenther 2014). Deception jamming is divided into repeater deception jamming and generated spoofing jamming (Hu et al. 2016). It is of great significance to study the anti-deception technology and improve the robustness of receivers. GNSS anti-spoofing technology is categorized into non-encryption-based technology and encryption-based technology (Psiaki and Humphreys 2016). The non-encryption-based technology mainly includes signal quality monitoring, doppler consistency monitoring and other anti-spoofing technologies. The encryption-based technology includes Navigation Message Authentication (NMA), Spreading Code Authentication (SCA), Navigation Message Encryption (NME) and Spreading Code Encryption (SCE) (Dovis 2015; Shen and Guo 2018a). Anti-spoofing technology can greatly enhance the security of information (Wesson et al. 2012).

The SCA technique is considered to be one of the key innovations for the next generation of GNSS civil signals (Margaria et al. 2017). Its robustness and complexity are in between NMA and NME/SCE. For the SCA technique unpredictable chips are inserted into the unencrypted public spreading code and verified in receivers to ensure the credibility of pseudo range measurement (Shen and Guo 2018a; b). At present, the main implementation methods of the SCA technique include Spread Spectrum Security Code (SSSC) (Scott 2003), Hidden Marker (HM) (Kuhn 2005) and Signal Authentication Sequence (SAS) (Pozzobon et al. 2011; Pozzobon 2011). The ideas adopted at the signal level are inserting unpredictable authentication chips into the public spreading code. The advantage of the SCA technique is that the received power is −160 dB·W. Unless the encrypted information

*Correspondence: tang_zuping@hust.edu.cn
School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, China

is available, it is difficult for attackers to predict the SCA chips correctly. The disadvantage is that the output of the correlator will be greatly attenuated as the proportion of the SCA chips in the code sequence increases, resulting in the failure of acquisition and tracking, for receivers do not participate in identity authentication (Pozzobon 2011). When the proportion of the inserted chips is small, the signal is vulnerable to multiple access interference. The adjustment of time, position and scale of chip insertion is not flexible.

In view of the above problems, this paper proposes a binary phase hopping based SCA technique. The proposed technique avoids non-cooperative parties to obtain information, and improves the signal confidentiality performance. Phase hopping modulation can be in multi-ary, and the proposed technique uses binary phase hopping. By adding pseudo-random phase hop into the civil signal, and correlating demodulation results with pseudo-random code in the receiver, we can achieve identity authentication. This technique can reduce the performance loss of the original signal and the impact on the receivers, which do not participate in authentication. Besides, it has good compatibility with the existing receiver architecture. This technique also has stronger anti-multiple access interference ability and higher authentication success rate. Moreover, it is more flexible because the transmitter can adjust the ratio of authentication component flexibly, and the receiver can also choose a flexible receiving mode. This SCA method provides a good technical solution for the design of modern GNSS signals.

## Phase hopping modulation

Phase hopping modulation is a new anti-interception method for improving the security and reliability of a system. Its aim is to improve the security performance of a wireless communication system without increasing the system bandwidth.

Phase hopping modulation is suitable for a variety of signals, such as baseband signal, Radio Frequency (RF) signal, and carrier. This modulation can also be regarded as a secondary modulation after the basic modulation, including Phase Shift Keying (PSK) modulation, Quadrature Amplitude Modulation (QAM), etc. The phase hopping sequence generator generates a phase hopping sequence to control the phase shifter, so the initial phase of the input signal changes with the hopping of the phase hopping sequence. Then the output signal can be processed according to different requirements and transmitted by the antenna. For the demodulation unit in the receiver, the same phase sequence generator generates the phase hopping sequence and controls the phase compensator to compensate the signal phase so as to achieve demodulation. The phase compensator is implemented by a phase shifter, which makes the phase of the input signal change with the hopping sequence. These two hopping procedures are complementary, which is essential for the signal synchronization.

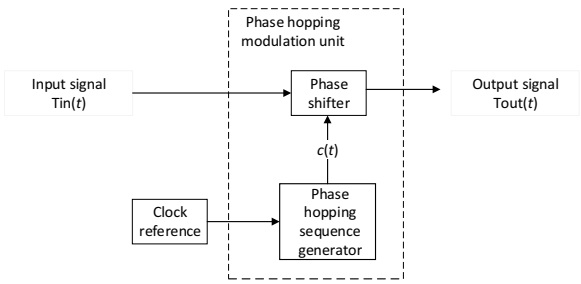


**Fig. 1** Phase hopping modulation unit

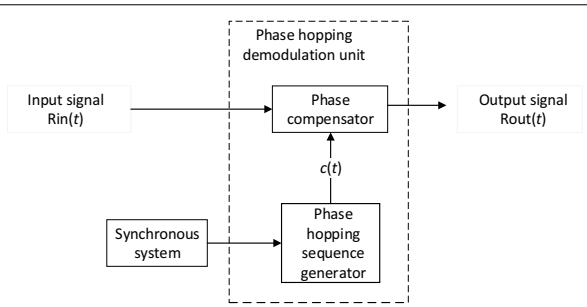


**Fig. 2** Phase hopping demodulation unit

### Phase hopping modulation unit

The phase hopping modulation unit is shown in Fig. 1.

The phase hopping sequence generator generates $N$-ary pseudo-random sequence $c(k)$, which is used as the phase hopping sequence, and the corresponding phase offset is

$$\varphi(k) = 2\pi \frac{c(k)}{N} \tag{1}$$

The output signal $T_{\text{out}}(t)$ is

$$T_{\text{out}}(t) = T_{\text{in}}(t) e^{j\varphi(t)} \tag{2}$$

where $e^{j\varphi(t)}$ is phase shift factor. The relationship between $t$ and $k$ is

$$k = \lfloor t/T_c \rfloor \tag{3}$$

where $T_c$ is the chip width of the phase hopping sequence.

### Phase hopping demodulation unit

The phase hopping demodulation unit is shown in Fig. 2.

Under the control of a synchronous system, the phase hopping sequence generator generates the same

pseudo-random sequence $c(k)$. The output signal $R_{\text{out}}(t)$ is

$$R_{\text{out}}(t) = R_{\text{in}}(t)e^{-j\varphi(t)} \tag{4}$$

where $e^{-j\varphi(t)}$ is phase compensation factor.

## Binary phase hopping based SCA technique

The commonly used SCA technique inserts unpredictable authentication chips into the public spreading code. This paper proposes an SCA technique that modulates authentication information on the signal phase.

### Signal structure

The phase hopping sequence $c(k)$ is binary and its value is given by

$$c(k) \in \{-1, 1\} \tag{5}$$

The corresponding phase offset is

$$\varphi(k) \in \{-\varphi_{\text{PH}}, \varphi_{\text{PH}}\} \tag{6}$$

where $\varphi_{\text{PH}}$ is the phase hopping amplitude.

Assuming that there are two GNSS signal components, and they are compounded together, such as Global Positioning System (GPS) L5, Galileo Navigation Satellite System (Galileo) E5a, BeiDou Navigation Satellite System (BDS) B2a, using the Quadrature Phase Shift Keying (QPSK) modulation. The baseband equivalent expression of the phase hopping modulation unit is

$$T_{\text{in}}(t) = d(t)c_d(t) + jc_p(t) \tag{7}$$

where $d(t)$ is the data bits, $c_d(t)$ is the spreading code of the data channel (I channel), $c_p(t)$ is the spreading code of the pilot channel (Q channel). The output signal of the phase hopping modulation unit is

$$\begin{aligned} T_{\text{out}}(t) &= T_{\text{in}}(t)e^{j\varphi(t)} \\ &= \left[d(t)c_d(t)\cos\varphi(t) - c_p(t)\sin\varphi(t)\right] \\ &\quad + j\left[d(t)c_d(t)\sin\varphi(t) + c_p(t)\cos\varphi(t)\right] \end{aligned} \tag{8}$$

if

$$\begin{aligned} I_{\text{out}} &= d(t)c_d(t)\cos\varphi(t) - c_p(t)\sin\varphi(t) \\ Q_{\text{out}} &= d(t)c_d(t)\sin\varphi(t) + c_p(t)\cos\varphi(t) \end{aligned} \tag{9}$$

and the RF signal is

$$\begin{aligned} s_{\text{PH}}(t) &= \sqrt{2P_1}\left[d(t)c_d(t)\cos\varphi(t) - c_p(t)\sin\varphi(t)\right]\cos(\omega_c t + \varphi_0) \\ &\quad - \sqrt{2P_2}\left[d(t)c_d(t)\sin\varphi(t) + c_p(t)\cos\varphi(t)\right]\sin(\omega_c t + \varphi_0) \\ &= \sqrt{2P_1}I_{\text{out}}\cos(\omega_c t + \varphi_0) - \sqrt{2P_2}Q_{\text{out}}\sin(\omega_c t + \varphi_0) \end{aligned} \tag{10}$$

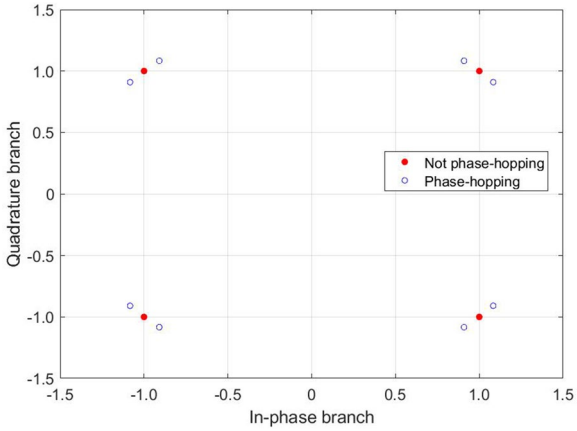


**Fig. 3** Binary phase hopping modulation constellation

where $P_1$ is the power of the data channel, $\omega_c$ is carrier frequency, $\varphi_0$ is carrier initial phase, $P_2$ is the power of the pilot channel. Figure 3 shows the constellation of the output signal, where $P_1 = P_2$, and $\varphi_{PH} = 5°$.

### SCA at receiver end

In the user segment, it is easy for a receiver to achieve authentication, and there is no need to make massive changes to the existing receiver. The process is as follows.

After the down conversion, the Intermediate Frequency (IF) signal obtained from the receiver is

$$\begin{aligned} s_{\text{IF}}(t) =& \sqrt{2P_{r1}}I_{\text{out}}\cos(\omega_i t + \varphi_i) \\ &- \sqrt{2P_{r2}}Q_{\text{out}}\sin(\omega_i t + \varphi_i) + n \end{aligned} \tag{11}$$

where $P_{r1}$ is the data channel power, $P_{r2}$ is the pilot channel power, $\omega_i$ is the IF carrier frequency, $\varphi_i$ is the IF carrier phase, and $n$ is noise.

The identity authentication relies on the $\sin\varphi(t)$, which can be implemented in the following three ways.

1. Only pilot channel used for authentication

The schematic diagram is shown in Fig. 4. The dashed box in the figure is the identity authentication module, and the rest is the traditional tracking loop. After mixing the IF signal with the locally generated carriers,

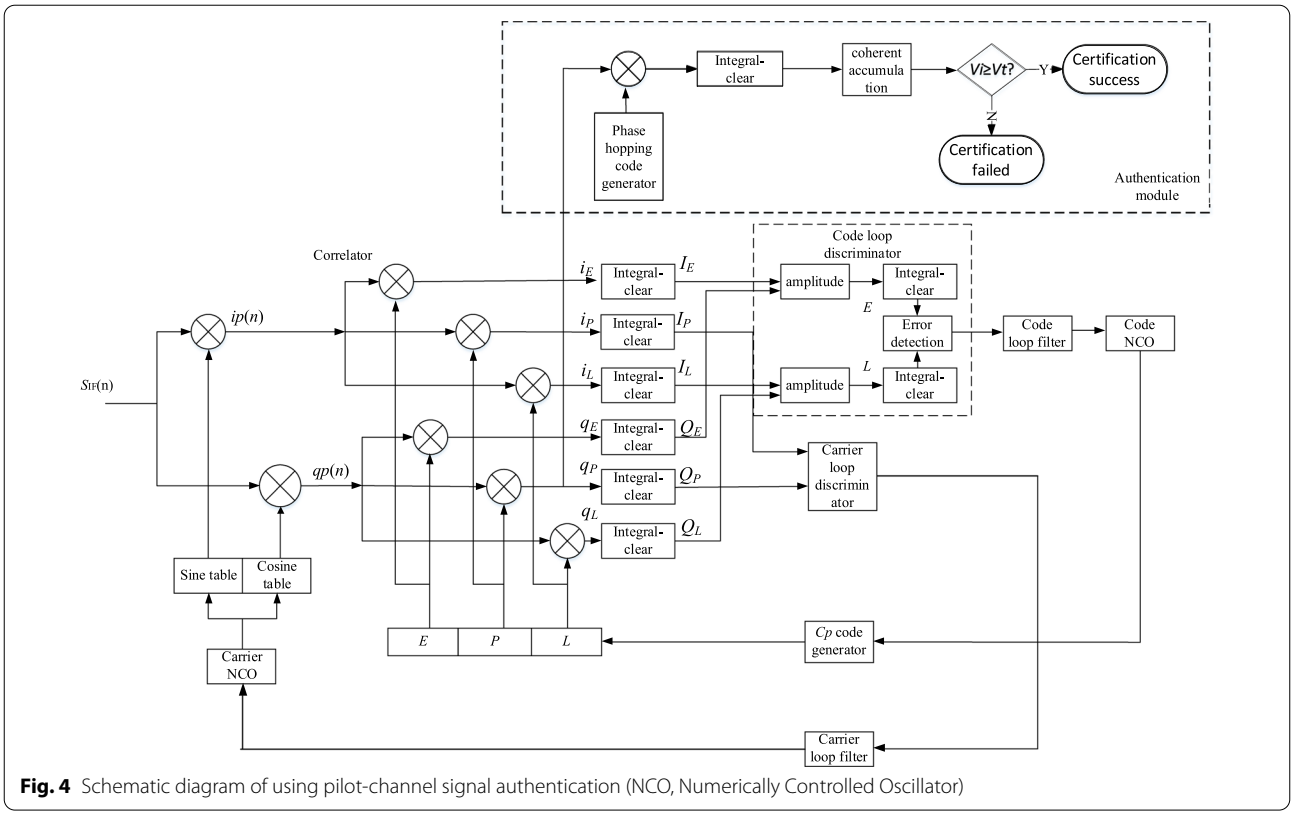


**Fig. 4** Schematic diagram of using pilot-channel signal authentication (NCO, Numerically Controlled Oscillator)

the high-order components are filtered out. When the tracking loop is stable, the I and Q channel signals are (assuming there are no frequency difference and initial phase difference between the received IF signal and the replicated signal)

$$\begin{aligned} i_p(t) &= s_{\mathrm{IF}}(t)\sqrt{2}\cos(\omega_o t + \varphi_{o,p}) \\ &= \sqrt{P_{r2}}Q_{\mathrm{out}} + n_{i,p} + \cdots \\ q_p(t) &= s_{\mathrm{IF}}(t)\sqrt{2}\sin(\omega_o t + \varphi_{o,p}) \\ &= \sqrt{P_{r1}}I_{\mathrm{out}} + n_{q,p} + \cdots \end{aligned} \tag{12}$$

where $\omega_o$ is the frequency of the local carrier, $\varphi_{o,p}$ is the initial phase of the local carrier, and $n_{i,p}$, $n_{q,p}$ are the noises of the I and Q channels, respectively.

Equation (9) tells that the authentication is not affected by the data bits. First, the Q channel signal in Eq. (12) is correlated and integrated with the pilot channel spreading code $c_p$ and the phase hopping sequence $c(k)$. The higher-order components will be cleared after the filter in the authentication module. Then, to further improve $\mathrm{C}/\mathrm{N}_0$, a coherent accumulation for the length of $T_{\mathrm{coh}}$ is carried out, and the normalized detection value $V_i$ is

$$V_i = -\sqrt{P_{r1}}(\varphi_{\mathrm{PH}} \cdot \pi/180) \tag{13}$$

when $\theta$ is small, $\sin\theta \approx \theta$. The threshold value $V_t$ is

$$V_t = \sigma_n\sqrt{-2\ln P_{\mathrm{fa}}} \tag{14}$$

where $\sigma_n$ is the standard deviation of the noise, and $P_{\mathrm{fa}}$ is false alarm probability. If $V_i$ is higher than $V_t$, the authentication successes, otherwise fails.

2. Only data channel used for authentication

The schematic diagram is shown in Fig. 5. The dashed box in the figure is the identity authentication module, and the rest is the traditional tracking loop. After mixing the IF signal with the locally generated carriers, the high-order components are filtered out. When the tracking loop is stable, the I and Q channel signals are (assuming there are no frequency difference and initial phase difference between the received IF signal and the replicated signal)

$$\begin{aligned} i_d(t) &= s_{\mathrm{IF}}(t)\sqrt{2}\cos(\omega_o t + \varphi_{o,d}) \\ &= \sqrt{P_{r1}}I_{\mathrm{out}} + n_{i,d} + \cdots \\ q_d(t) &= s_{\mathrm{IF}}(t)\sqrt{2}\sin(\omega_o t + \varphi_{o,d}) \\ &= -\sqrt{P_{r2}}Q_{\mathrm{out}} + n_{q,d} + \cdots \end{aligned} \tag{15}$$

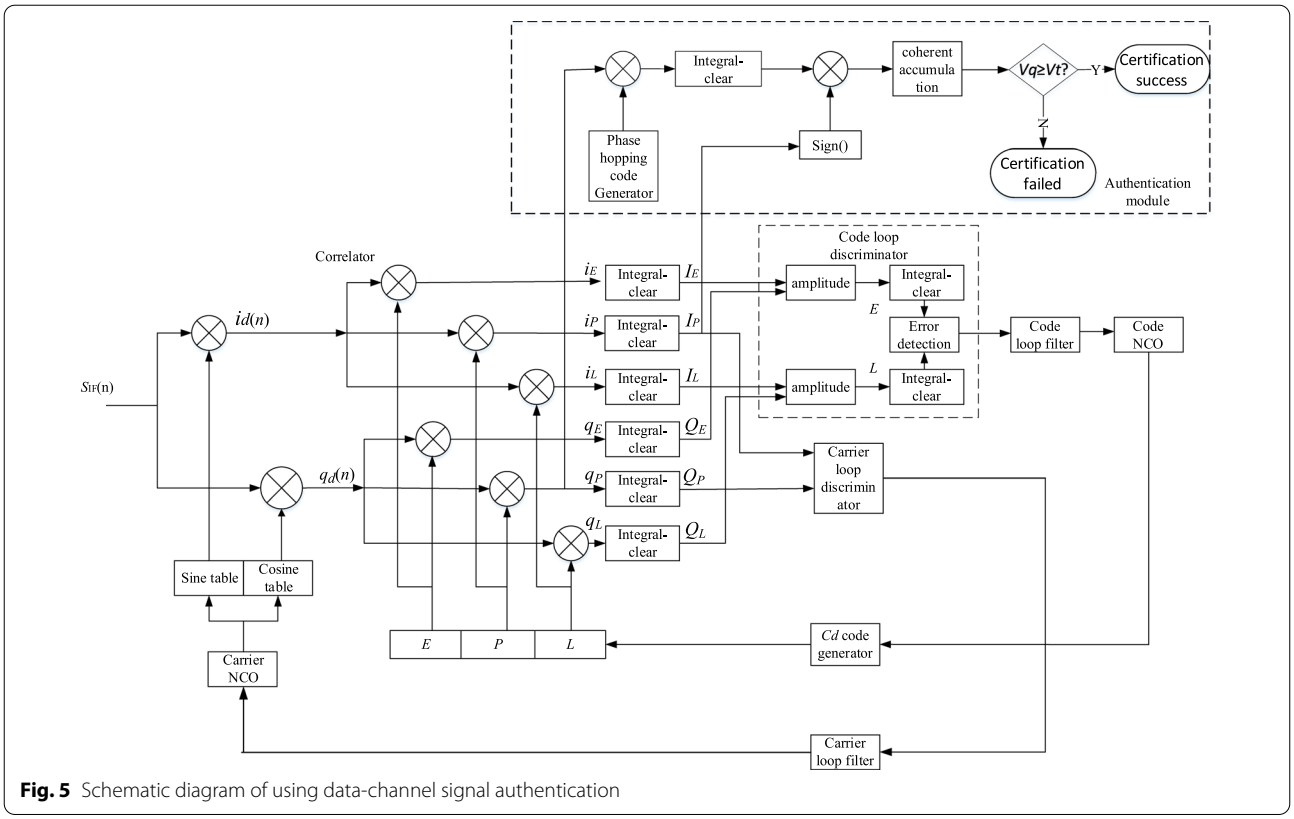


**Fig. 5** Schematic diagram of using data-channel signal authentication

where $\omega_o$ is the frequency of the local carrier, $\varphi_{o,d}$ is the initial phase of the local carrier, and $n_{i,d}$, $n_{q,d}$ are the noises of the I and Q channels, respectively.

Equation (9) tells that to use the data channel for authentication, it is necessary to eliminate the influence of data bits. First, the Q channel signal in Eq. (15) is correlated and integrated with the data channel spreading code $c_d$ and the phase hopping sequence $c(k)$ respectively. The higher-order components will be cleared after the filter in the authentication module. Then the influence of data bit inversion is eliminated according to the data bit estimation of the I channel. Next, to further improve $\mathrm{C}/\mathrm{N}_0$, a coherent accumulation for the length of $T_{\mathrm{coh}}$ is carried out, and the normalized detection value $V_q$ is

$$V_q = -\sqrt{P_{r2}}(\varphi_{\mathrm{PH}} \cdot \pi/180) \tag{16}$$

when $\theta$ is small, $\sin\theta \approx \theta$. The threshold value $V_t$ is

$$V_t = \sigma_n \sqrt{-2\ln P_{\mathrm{fa}}} \tag{17}$$

where $\sigma_n$ is the standard deviation of the noise, and $P_{\mathrm{fa}}$ is false alarm probability. If $V_q$ is higher than $V_t$, the authentication successes, otherwise fails.

3. Both data and pilot channels used for authentication

When the receiver tracks pilot signal and data signal independently, the above two methods are directly combined to get the normalized detection value $V$ as

$$V = V_i + V_q \tag{18}$$

While if the receiver tracks pilot signal and data signal jointly, it is necessary to determine the phase relation between $V_i$ and $V_q$ according to the practical tracking loop and make a right combination.

To use the above three methods, we only need to add an identity authentication module in the classic tracking loop. Table 1 shows the increase in hardware complexity, which is mainly reflected in the number of code sequence generators and correlators.

## Performance analysis

In order to verify the performance of the binary phase hopping based SCA technique, this paper simulates the performance loss and detection probability, then compares it with the inserting chip based SCA technique. It is assumed that the energy proportion of the authentication part is the same, i.e., $(\sin\varphi_{\mathrm{PH}})^2$.

**Table 1 Implementation complexity**

| Method number | Code sequence generator | | Percentage increased (%) | Correlator | | Percentage increased (%) |
|---|---|---|---|---|---|---|
| | Non-authentication | Authentication | | Non-authentication | Authentication | |
| 1 | 1 | 2 | 100 | 6 | 7 | 16.7 |
| 2 | 1 | 2 | 100 | 6 | 7 | 16.7 |
| 3 | 2 | 3 | 50 | 12 | 14 | 16.7 |

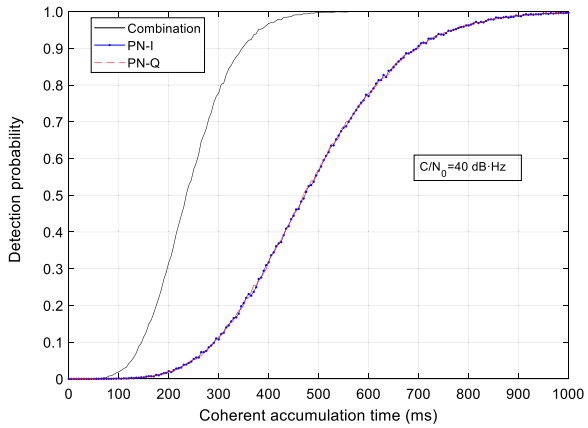


**Fig. 6** Performance simulation of authentication module

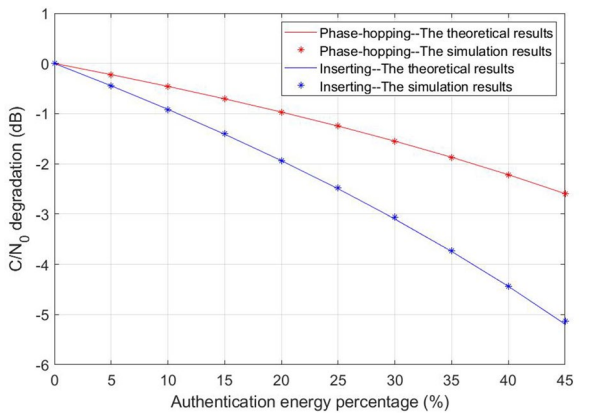


**Fig. 7** $C/N_0$ degradation

### Performance simulation of three authentication methods at receiver end

The simulation parameters are as follows: code rate $R_c = 1.023$ Mcps, phase hopping amplitude $\varphi_{\mathrm{PH}} = 5°$, $C/N_0 = 40$ dB·Hz, coherent integration time 1000 ms, and false alarm probability $10^{-4}$.

The simulation result is shown in Fig. 6. In the figure, "PN_I" represents the method of using the data channel for authentication, "PN_Q" represents the method of using the pilot channel for authentication. The detection probability curves of the two methods coincide. "Combination" represents the method of using both pilot channel and data channel for authentication. When both channels are used, the signal power is fully utilized, so its performance is optimal. The coherent accumulation time required to achieve the same detection probability is reduced by a half.

### Performance loss of receivers not participating in authentication

For the existing civil receivers which do not include identity authentication module. The authentication component in the signal is regarded as noise, which will degrade $C/N_0$.

For the inserting chip based SCA technique, assuming the spreading code length is $N$, the length of the authentication codes is $K$, signal amplitude is $A$, and the power of noise is $\sigma^2$, then the $C/N_0$ of the non-authentication signal is $\frac{A^2}{2\sigma^2} \cdot N$. For the receivers which do not participate in authentication, the $C/N_0$ is $\frac{A^2}{2\sigma^2} \cdot \frac{(N-K)^2}{N}$. So, the $C/N_0$ degradation is

$$\Delta C/N_0 = 10\log_{10}(1-p_u)^2 \tag{19}$$

where $p_u$ is the ratio of the authentication part in a signal, that is, the ratio of the unpredictable sequence inserted in the spreading code sequence.

For the binary phase hopping based SCA technique, the $C/N_0$ degradation is

$$\Delta C/N_0 = 10\log_{10}(1-p_u) \tag{20}$$

where $p_u$ is the ratio of the authentication part in a signal, and the relationship with the phase hopping amplitude is

$$p_u = (\sin\varphi_{\mathrm{PH}})^2 \tag{21}$$

it is known that theoretically the $C/N_0$ degradation of the binary phase hopping based SCA technique is lower, which is a half of that for the inserting chip based SCA technique.

Figure 7 shows the simulation results of $C/N_0$ degradation of the two SCA techniques. The theoretical results coincide with the simulation results. The binary phase

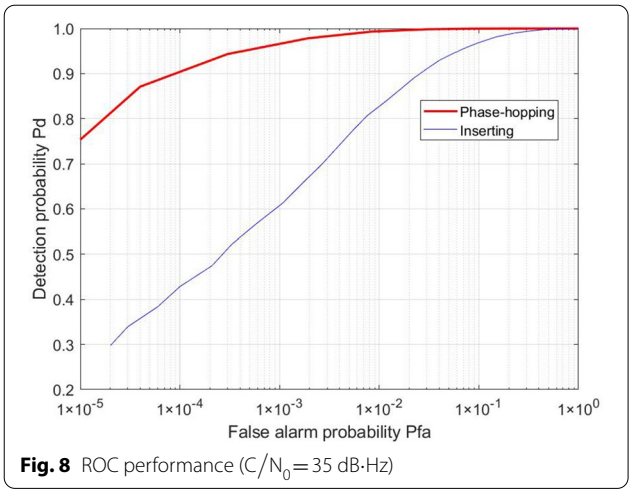


**Fig. 8** ROC performance ($C/N_0 = 35$ dB·Hz)

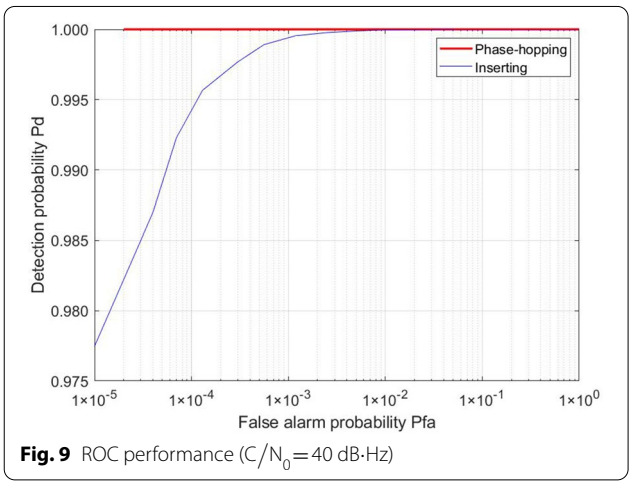


**Fig. 9** ROC performance ($C/N_0 = 40$ dB·Hz)

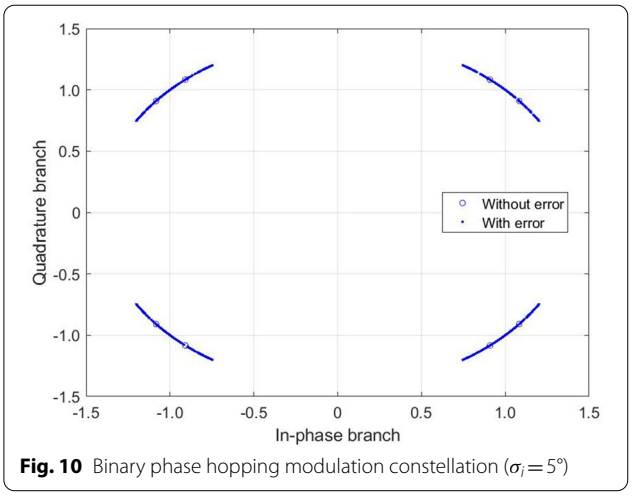


**Fig. 10** Binary phase hopping modulation constellation ($\sigma_i = 5°$)

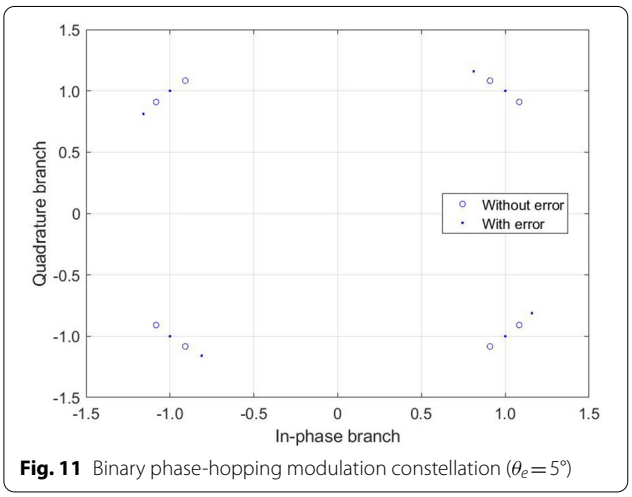


**Fig. 11** Binary phase-hopping modulation constellation ($\theta_e = 5°$)

hopping based SCA technique has lower $C/N_0$ degradation and better compatibility with the existing receiver architecture.

### Simulation of detection probability

This section simulates the Receiver Operating Characteristic (ROC) performance for the two SCA techniques, and the binary phase hopping based SCA technique uses the third authentication method. In the following figures the abscissa represents the false alarm probability $P_{\text{fa}}$ and the ordinate is for the detection probability $P_{\text{d}}$. The simulated ROC performances are plotted in Figs. 8 and 9 with the coherent integration time $T_{\text{coh}} = 600$ ms, code rate $R_c = 1.023$ Mcps, phase jump amplitude $\varphi_{\text{PH}} = 5°$, and $C/N_0$ being 35 dB·Hz and 40 dB·Hz, respectively.

When $C/N_0$ is 40 dB·Hz, the coherent integration time of 600 ms is long enough. There is no significant difference between the authentication success rates of the two SCA techniques. Under the same false alarm probability, the authentication success rates of the two SCA techniques are almost 100%. When $C/N_0$ is reduced to 35 dB·Hz, the coherent integration time of 600 ms is not enough. Under the same false alarm probability, the authentication success rate of the phase hopping based SCA technique improves obviously. One reason is that in the same coherent integration time, the authentication code length of the phase hopping based SCA technique is $R_c \cdot T_{\text{coh}}$, and the authentication code length of the inserting chip based SCA technique is $R_c \cdot p_u \cdot T_{\text{coh}}$. For a GNSS signal, the longer the spreading code sequence is, the higher the spreading gain will be, meaning stronger anti-multiple access interference ability.

Considering the errors in PLL, such as phase jitter and dynamic stress error, Fig. 10 shows the constellation diagram of demodulation with the root-mean-square error (RMSE) of phase jitter $\sigma_i$ being 5°. The phases of actual

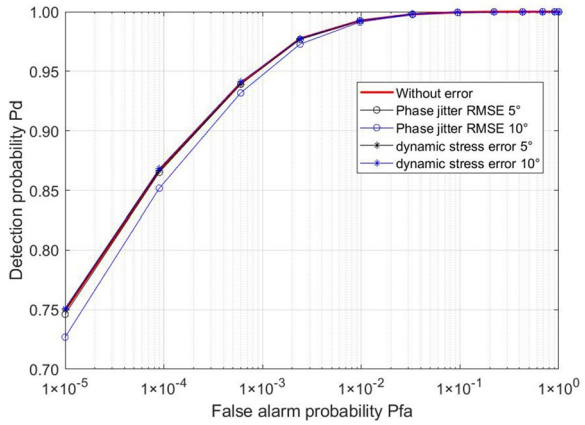


**Fig. 12** ROC performance ($C/N_0 = 35$ dB·Hz)

signal jitter are near the ideal eight phase points. Figure 11 shows the constellation diagram of demodulation with the steady-state value of dynamic stress error $\theta_e$ being 5°. There is a fixed deviation between the phase points of the actual signal and the eight ideal phase points.

Figure 12 shows the ROC performance of authentication module for the cases that the root-mean-square error of phase jitter is 5° and 10°, the steady value of dynamic stress error is 5° and 10°, and $C/N_0$ is 35 dB·Hz. Compared with the ideal (i.e., without error), the dynamic stress error hardly affects the ROC performance of authentication module, while the phase jitter does, but not much deteriorate the ROC performance.

### Flexibility analysis

The premise of successful authentication is the correct detection of the authentication code, which requires low false alarm probability and high detection probability. The success rate of authentication is related to the power and time of authentication signal. When the total power of the signal is constant, the higher the power proportion of the authentication signal, the shorter the necessary time for successful authentication will be, otherwise the longer the authentication time should be adopted. Therefore, there is a need for a tradeoff between the authentication component power proportion and the real-time authentication, which can be adjusted if necessary.

For the inserting chip based SCA technique, if we want to change the percentage of unpredictable sequence inserted in the spreading code sequence, the strategies of generating spreading sequence on the satellite and the receiver processing spreading code sequence need to be adjusted. The insert position and time need to update, and the transmission and synchronization of these updated information also need additional resources, which is less flexible.

For the binary phase hopping based SCA technique, to change the energy proportion of the authentication part in the signal, only the phase hopping amplitude needs to be changed. The receiver does not need to change the receiving mode and processing strategy, which has high implementation flexibility.

### Applicability analysis

The modulation mode adopted in the simulation is Direct Sequence Spread Spectrum (DSSS)/QPSK, and code rate is 1.023 Mcps. In the design of a modern GNSS signal structure, subcarrier modulation and higher code rate are also used for some signals. Compared with the proposed modulation method, the difference of the subcarrier modulation process is that it adds a subcarrier modulation module before the carrier modulation. The corresponding demodulation in the receiver does not affect the constellation diagram of the signal, which means it does not affect the receiver authentication module. At the same time, higher code rate will bring higher spreading gain, which can also improve the performance of the receiver authentication module. Therefore, the proposed scheme is suitable for modern GNSS signals.

## Conclusion

In this paper, a new SCA technique of the binary phase hopping based SCA technique is proposed. The performance of this technique is compared with the inserting chip based SCA technique through a simulation. In terms of compatibility, the proposed technique is more compatible with the existing receiver architecture, and also reduces the impact on the receivers that do not participate in identity authentication. In terms of authentication success rate, the binary phase hopping based SCA technique has stronger anti-multiple access interference ability and higher authentication success rate in the same condition. In terms of flexibility, the binary phase hopping based SCA technique is more flexible and easier to adjust. The binary phase hopping based SCA technique provides an efficient implementation scheme for future GNSS security design.

#### Acknowledgements

Not applicable.

#### Authors' contributions

SW and HL accomplish thesis writing, simulation and modification; ZT proposed the idea of this paper; BY assisted in carrying out the simulation. All authors read and approved the final manuscript.

**Funding**
This study is supported by Key-Area Research and Development Program of Guangdong Province (Grant No. 2019B010158001).

**Availability of data and materials**
Data sharing is applicable to this article.

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

Received: 20 May 2020 Accepted: 14 January 2021
Published online: 26 February 2021

**References**

Dovis, F. (2015). GNSS interference, threats, and countermeasures. *Radar receivers*.
GPS Interface Control Documents IS-GPS-200G. (2012). Retrieved from http://www.gps.gov/technical/icwg/
Guenther, C. (2014). A survey of spoofing and counter-measures. *Navigation, 61*(3), 159–177.
Hu, Y., Bian, S., Ji, B., & Li, H. (2016). Discussions of satellite navigation countermeasures on spoofing and anti-spoofing techniques. In *2016 China Satellite Navigation Conference (CSNC)*.
Humphreys, T. E. (2013). Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace Electronic Systems, 49*(2), 1073–1090.
Kuhn, M. G. (2005). *An asymmetric security mechanism for navigation signals* (pp. 239–252). Heidelberg: Springer.
Liang, H., Daniel, B. W., & Gao, X. (2013). Cooperative GNSS authentication reliability from unreliable peers. *Inside GNSS*, pp. 70–75.
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.
Pozzobon, O. (2011). Keeping the spoofs out: Signal authentication services for future GNSS. *Inside GNSS, 6*(3), 48–55.
Pozzobon, O., Canzian, L., Danieletto, M., & Chiara, A. D. (2011). Anti-spoofing and open GNSS signal authentication with signal authentication sequences. In *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*. IEEE.
Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE, 104*(6), 1258–1270.
Scott, L. (2003). *Anti-spoofing & authenticated signal architectures for civil navigation systems*. Paper presented at the Ion Gps.
Shen, C., & Guo, C. (2018b). Research on structure-based authentication approaches for civil GNSS signal. In *Proceedings of the 9th China Satellite Navigation Conference—S03 Satellite Navigation Signal and Anti-interference Technology*.
Shen, C., & Guo, C. (2018). Study and evaluation of GNSS signal cryptographic authentication defense. *GNSS World of China, 43*(3), 7–12.
Wesson, K., Rothlisberger, M., & Humphreys, T. (2012). Practical cryptographic civil GPS signal authentication. *Navigation, 59*(3), 177–193.