Development of Algorithms for Increasing the Information Secrecy of the Satellite Communication System Based on the Use of Authentication Technology

Nikita Chistousov [1], Igor Kalmykov [1], Aleksandr Olenev [2] *and* Natalya Kalmykova [1]

[1] *North-Caucasus Federal University, Pushkina, 1, Stavropol, 355009, Russia.*
[2] *Stavropol State Pedagogical Institute, Lenina St., 417 "A" , Stavropol, 355028, Russia*

Abstract

One of the most promising applications of low-earth orbit satellite systems is remote monitoring and control systems for unattended objects located in the Far North. Therewith, there is a tendency to increase the groupings of such satellites. Therefore, ensuring the information secrecy of the low-earth orbit satellite becomes an important task. To prevent the intruder satellite from imposing a previously captured and delayed control command, it is proposed to use the "friend-foe" system for satellites, which uses a zero-knowledge authentication algorithm. It is necessary to increase the speed of the satellite authentication process to reduce the probability of a response signal being picked up. To do this, it is proposed to use modular codes (MC), which can simultaneously perform the operations of addition, subtraction, and multiplication. As a result, the probability of picking up the signal of the responder located onboard the satellite is reduced. In addition, the MC can correct multi-bit errors within a single remainder in the presence of two redundant bases. Therefore, the development of an algorithm for correcting errors arising in the process of satellite authentication caused by failures, and interference in the communication channel is an urgent task. The work aims to increase the information secrecy of the low-earth orbit satellite by using the developed authentication algorithm, which has a minimum time for determining the satellite status, as well as an algorithm for correcting errors that occur during the operation of the satellite identification system and data transmission, implemented using a single algebraic system – parallel modular codes.

Keywords

satellite authentication algorithm, modular code, error detection, and correction algorithm

1. Introduction

In recent years, there has been a tendency to an increase in the number of low-orbit satellite constellations, which are used in remote monitoring, control, and management systems for unattended objects of environmentally hazardous technologies used in the production and transportation of hydrocarbons in the Far North. Herewith, an increase in the number of countries involved in the development of the Arctic's natural resources contributes to the intensification of destructive impacts on the low-earth orbit satellite (LEOS) to disrupt their work. One of the promising areas to counteract these actions is to ensure the information secrecy of the LEOS [1-3].

To increase the information secrecy of the LEOS, it is proposed to use a satellite authentication system that will not allow the intruder satellite to impose on the receiver an intercepted and delayed signal that can disable the control object and cause an environmental disaster. To reduce the probability

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia
EMAIL: chistousov.nik@yandex.ru (Nikita Chistousov); kia762@yandex.ru (Igor Kalmykov); olenevalexandr@gmail.com (Aleksandr Olenev); kmi545@yandex.ru (Natalya Kalmykova)
ORCID: 0000-0002-0286-7391 (Nikita Chistousov); 0000-0002-9854-5310 (Igor Kalmykov); 0000-0003-2719-6624 (Aleksandr Olenev); 0000-0003-2498-8765 (Natalya Kalmykova)

of picking up a response signal by an intruder satellite, it is proposed to use modular codes (MC), which will increase the speed of satellite identification. Therewith, the MC can also correct errors that occur in the calculation process due to failures [4, 5]. The article presents the developed algorithm for detecting and correcting MC errors that occur during the satellite authentication process and are caused by both failures, and interference in the communication channel, the use of which will ensure the information secrecy of the LEOS even during destructive impacts of natural and artificial nature on the identification system.

2. Materials and methods

2.1. Modular codes

Modular codes are arithmetic non-positional codes [4, 5]. In these codes, the integer X is uniquely given by a tuple of the remainder

$$X = (x_1, x_2, ..., x_k), \quad (1)$$

where $x_i \equiv X \bmod m_i$, m_i –bases of the modular code; $(m_i, m_j) = 1; i = 1,...,k$.

Since the bases of MC are pairwise prime numbers m_i, where $i = 1,...,k$, their product sets the size of the working range

$$M_k = \prod_{i=1}^{k} m_i > X. \quad (2)$$

Since modular codes perform summation, diminution, and multiplication operations in parallel

$$X + C = ((x_1 + c_1) \bmod m_1, (x_2 + c_2) \bmod m_2, ..., (x_k + c_k) \bmod m_k), \quad (3)$$

$$X - C = ((x_1 - c_1) \bmod m_1, (x_2 - c_2) \bmod m_2, ..., (x_k - c_k) \bmod m_k), \quad (4)$$

$$X \cdot C = ((x_1 \cdot c_1) \bmod m_1, (x_2 \cdot c_2) \bmod m_2, ..., (x_k \cdot c_k) \bmod m_k), \quad (5)$$

then it is advisable to use them to increase the speed of calculations. Since authentication algorithms use such operations, they can be implemented in the MC. Therefore, modular codes have found wide application in real-time systems.

In works [6-9] it is offered to use modular code for construction of special processors of digital signal processing. Modular codes allow to increase the efficiency of digital filters [10-13]. Work [14] presents the protocol "Electronic Cash" with inspection correction rules of the electronic e-cash number for e-Commerce systems, which uses SOC. This allows to increase the authentication speed of the applicant. In [15] it is shown that the codes of a polynomial residue number system, aimed at reducing the effects of failures in the AES cipher. Error correction of digital signal processing devices using non-positional modular codes is shown in [16-19]. The use of redundant modular codes for improving the fault tolerance of special processors for digital signal processing is shown in [20]. A method of increasing the reliability of telemetric well information transmitted by the wireless communication channel is shown in [21]. Consider the use of modular codes in authentication protocols. Let's use the protocol given in the [22].

2.2. Development of an authentication algorithm in MC

In this algorithm, the following parameters are used:

- $m_1, ..., m_k$ –bases of the modular code;
- the satellite secret key $X = (X_1, ..., X_k) < M_k$;
- the session key $Y(j) = (Y_1(j), ..., Y_k(j)) < M_k$;

- and the parameter $L(j)=(L_1(j),...,L_k(j))<M_k$ used to verify the repeated use of the session key, where $X \equiv X_i \bmod m_i$; $Y(j) \equiv Y_i(j) \bmod m_i$; $L(j) \equiv L_i(j) \bmod m_i$; $i = 1,2,...,k$; j is the number of the communication session.

The preliminary stage of the satellite authentication algorithm:

1. The responder calculates the true status of the satellite

$$\begin{aligned} W_1 &= \left| b^{X_1} b^{Y_1(j)} b^{L_1(j)} \right|_{m_1}^{+}; \\ W_2 &= \left| b^{X_2} b^{Y_2(j)} b^{L_2(j)} \right|_{m_2}^{+}; \\ &\vdots \\ W_k &= \left| b^{X_k} b^{Y_k(j)} b^{L_k(j)} \right|_{m_k}^{+}; \end{aligned} \tag{6}$$

where b is the generating multiplicative group to modulo m_i.

2. The responder chooses random numbers

$$\{\Delta X, \Delta Y(j), \Delta L(j)\} < M_k = \prod_{i=1}^{k} m_i \ , \tag{7}$$

and makes a noise of the secret parameters of the algorithm

$$\begin{aligned} X_i^* &= \left| X_i + \Delta X_i \right|_{p_i}^{+}, \\ Y_i^*(j) &= \left| Y_i(j) + \Delta Y_i(j) \right|_{p_i}^{+}, \\ L_i^*(j) &= \left| L_i(j) + \Delta L_i(j) \right|_{p_i}^{+}, \end{aligned} \tag{8}$$

where $p_i = \varphi(m_i)$ is the Euler function of the number m_i; $\Delta X, \Delta Y(j), \Delta L(j)$ – random numbers; $\Delta X_i \equiv \left| \Delta X \right|_{m_i}^{+}$ $\Delta Y(j) \equiv \Delta Y_i(j) \bmod m_i$; $\Delta L(j) \equiv \Delta L_i(j) \bmod m_i$.

3. The responder calculates the noisy status of the satellite

$$\begin{aligned} W_1^* &= \left| b^{X_1^*} b^{Y_1^*(j)} b^{L_1^*(j)} \right|_{m_1}^{+}; \\ W_2^* &= \left| b^{X_2^*} b^{Y_2^*(j)} b^{L_2^*(j)} \right|_{m_2}^{+}; \\ &\vdots \\ W_k^* &= \left| b^{X_k^*} b^{Y_k^*(j)} b^{L_k^*(j)} \right|_{m_k}^{+}; \end{aligned} \tag{9}$$

The authentication algorithm consists of the following steps.

1. The requester passes the responder a random number $g = (g_1, g_2, ..., g_k)$.

2. The responder, having received number g, calculates the answers

$$\begin{aligned} v_i(1) &= \left| X_i^* - g_i X_i \right|_{p_i}^{+}, \\ v_i(2) &= \left| Y_i^*(j) - g_i Y_i(j) \right|_{p_i}^{+}, \\ v_i(3) &= \left| L_i^*(j) - g_i L_i(j) \right|_{p_i}^{+}. \end{aligned} \tag{10}$$

The responder transmits the following data to the requester

$$\left\{(W_1, ..., W_k), (W_1^*, ..., W_k^*), (v_1(1), ..., v_k(1)), (v_1(2), ..., v_k(2)), (v_1(3), ..., v_k(3))\right\}.$$

3. The requester checks the received responses

$$Z_1 = \left| W_1^{g_1} b^{v_1(1)} b^{v_1(2)} b^{v_1(3)} \right|_{m_1}^{+},$$
$$Z_2 = \left| W_2^{g_2} b^{v_2(1)} b^{v_2(2)} b^{v_2(3)} \right|_{m_2}^{+}, \quad (11)$$
$$Z_k = \left| W_k^{g_k} b^{v_k(1)} b^{v_k(2)} b^{v_k(3)} \right|_{m_k}^{+}.$$

Applicant A has the "own" status if the equality is met $\left\{ Z_1 = W_1^*, ..., Z_k = W_k^* \right\}$.

The originality of this solution is based on a new idea – the use of MC, which effectively provides parallelization of calculations at the level of arithmetic operations when authenticating the satellite. The novelty of the obtained result is that an authentication algorithm has been developed for the first time, implemented in MCs, the use of which makes it possible to increase the information secrecy of the LEOS by reducing the probability of selecting a response signal "Own", caused by a reduction in the time spent on satellite identification due to parallelization of the calculation at the level of arithmetic operations.

When implementing the hardware design of the system, the Vivado HLS 2019.2 development tool was used. The clock frequency of the FPGA was 250 MHz. Comparative analysis showed that it takes 3.1 ms to complete one round of the authentication stage using Shnor protocol and 1.2 ms for the developed protocol when using a 32-bit base.

2.3. Error correction algorithm in modular codes

To correct a batch of errors within a single remainder $x_i^* = \left| x_i + \Delta x_i \right|_{m_i}^{+}$, where $\Delta x_i = \{1, ..., m_i - 1\}$ is the error depth, two control bases are introduced [4, 5]

$$p_{k+1} p_{k+2} > p_k p_{k-1}. \quad (12)$$

The result is the full range of the code

$$M_{k+2} = \prod_{i=1}^{k+2} m_i. \quad (13)$$

Redundant MC does not contain an error during execution

$$X = (x_1, ..., x_k, x_{k+1}, x_{k+2}) < M_k = \prod_{i=1}^{k} m_i. \quad (14)$$

Therefore, the MC use the positional characteristic (PC) interval number, which shows the location of the code relative to M_k

$$S = \left[\frac{X}{M_k} \right], \quad (15)$$

where $[\ ]$ is the integer part when dividing.

If the positional characteristic:

- S = 0 – there is no error;
- S > 0 – there is an error.

Let us use the Chinese remainder theorem to translate from modular code to positional code,

$$X = x_1 B_1 + x_2 B_2 + ... + x_{k+2} B_{k+2} \, mod \, M_{k+2} = \\ = \sum_{i=1}^{k+2} x_i B_i \, mod \, M_{k+2}, \quad (16)$$

where B_i – orthogonal basis of the redundant MC.

The orthogonal bases are calculated according to [4]

$$B_i = \left| M_{k+2}^{-1} \right|_{m_i}^{+} \frac{M_{k+2}}{m_i}. \quad (17)$$

Let us substitute expression (15) into expression (14). The result is the algorithm for calculating this positional characteristic in the MC without translating it into a positional code

$$\begin{cases} S_{k+1} = \left(\sum_{i=1}^{k+2} x_i K_i + \left[\sum_{j=1}^{k} \alpha_j B_j^* \left(M_k \right)^{-1} \right] \right) mod\, m_{k+1}, \\ S_{k+2} = \left(\sum_{i=1}^{k+2} x_i K_i + \left[\sum_{j=1}^{k} \alpha_j B_j^* \left(M_k \right)^{-1} \right] \right) mod\, m_{k+2}, \end{cases} \quad (18)$$

where $B_i = K_i M_k + B_i^*$; B_i^* is the orthogonal basis of the redundant MC.

The originality of the developed algorithm is based on a new idea – to use redundant MC to correct errors caused not only by failures of the satellite identification system but also by interference in the channel. In addition, the MC can correct multi-bit errors within a single remainder in the presence of two redundant bases. This allowed assuming that the redundant MC are close to the Reed-Solomon codes in their correcting abilities. This means that the use of redundant MC will allow abandoning the cascade codes, in which the external code is designed to detect and correct errors caused by failures, and the internal code – to search for and correct errors caused by interference in the communication channel. The novelty of the obtained result lies in the fact that for the first time an algorithm was developed for correcting errors by redundant MC arising in the process of satellite authentication caused by both failures, and interference in the communication channel, which will ensure information secrecy of the LEOS even during the destructive effects on the system. To evaluate the effectiveness of the algorithm for constructing a modular turbo code, a software package was created that allows simulating a communication channel with impulse noise. The analysis of the research results shows that the application of the developed algorithm for constructing a modular turbo code makes it possible to increase the noise immunity of the identification system. So, with the signal-to-noise ratio E_b/N_0 = 13 dB, the probability of a system error using the developed algorithm is $P = 3 \cdot 10^{-5}$, while for the classical MC - $P = 8{,}6 \cdot 10^{-5}$.

3. Acknowledgements

This work was supported by the Russian Foundation for Basic Research, project No. 20-37-90009

4. References

[1] Jonathan C. McDowel, The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation. The Astrophysical Journal Letters. Volume 892. Number 2. (2020): 1- 10.

[2] George Sebestyen, Steve Fujikawa Low Earth Orbit Satellite Design. Springer, New York, NY, 2018

[3] Bo Zhao, Guangliang Ren, Huining Zhang Multisatellite Cooperative Random Access Scheme in Low Earth Orbit Satellite Networks. IEEE systems journal. volume 13, no. 3, September (2019): 2617 - 2629

[4] Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation. Imperial College Press. UK 2007.

[5] Ananda Mohan Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland. 2016.

[6] Katkov K. A., Kalmykov I.A. Application of parallel technologies in navigation management under the conditions of artificial ionospheric disturbances. World Applied Sciences Journal. 26(1). (2013): 108-113

[7] Katkov K.A., Naymenko D.O., Makarova A.V. Parallel modular technologies in digital signal processing. Life Science Journal. 11(11s). (2014): 435-438

[8] Veligosha A. V., Kaplun D. I., Klionskiy D. M., Gulvanskiy V. V. Parallel-pipeline implementation of digital signal processing techniques based on modular codes. Proceedings of the 19th International Conference on Soft Computing and Measurements. SCM 2016. 7519731. (2016): 213-214
[9] Katkov K. A., Timoshenko L. I., Dunin A. V. Application of Modular Technologies in the Large-Scale Analysis of Signals. Journal of Theoretical and Applied Information Technology. 80(3). (2016): 391-400.
[10] Kaplun D., Voznesensky A., Veligosha A., Kalmykov I., Kandarpa Kumar Sarma Technique to adjust adaptive digital filter coefficients in Residue Number System based filters. IEEE Access. 9.9446075. (2021): 82402-82416.
[11] Chervyakov N. I., Veligosha A. V., Ivanov P. E. Digital filters in a system of residual classes // Izvestiya Vysshikh Uchebnykh Zavedenij. Radioelektronika. 38(8). (1995): 11-20.
[12] Veligosha A.V., Kaplun D.I., Bogaevskiy D.V. Adjustment of adaptive digital filter coefficients in modular codes // Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering. ElConRus 2018. January (2018): 1167-1170.
[13] Yurdanov D. A., Gostev D. B. The implementation of information and communication technologies with the use of modular codes // CEUR Workshop Proceedings 1837. (2017): 206-212.
[14] Lapina M., Kononova N. Development of the protocol «Electronic Cash» with inspection correction rules of the electronic e-cash number for e-Commerce systems // CEUR Workshop Proceedings 2254. (2018): 147-153.
[15] Stepanova, E.P., Toporkova, E.V Application of the codes of a polynomial residue number system, aimed at reducing the effects of failures in the AES cipher. Journal of Digital Information Management. 14(2). (2016): 114-123.
[16] Kaplun D. I., Klionskiy D. M., Bogaevskiy D. V. Error correcting of digital signal processing devices using non-positional modular codes. Automatic Control and Computer Sciences. 51(3). (2017):167-173.
[17] Selivanova M. V., Tyncherov K. T., Ikhsanova F. A. A method of paired zeroing of numbers in a residue system. Journal of Physics. Conference Series 1333. 022015. (2019).
[18] Tyncherov K. T., Ikhsanova F. A., Olenev A.A. Proof of the method of paired zeroing of numbers in a residue system. Journal of Physics. Conference Series. 1333. 022016. (2019).
[19] Selivanova M. V., Tyncherov K. T. A device for paired zeroing of numbers in a residue system. Journal of Physics. Conference Series. 1333. (2019). 022017.
[20] Stepanova E. P., Makarova A. V. The use of redundant modular codes for improving the fault tolerance of special processors for digital signal processing. CEUR Workshop Proceedings. 1837. (2017): 115-122.
[21] Tyncherov K.T., Chervyakov N.I., Selivanova M.V. Method of increasing the reliability of telemetric well information transmitted by the wireless communication channel. Bulletin of the Tomsk Polytechnic University. Geo Assets Engineering. 329(3). (2018): 36-43.
[22] Pashintsev, V.P., Zhuk, A.P., Rezenkov, D.N Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. International Journal of Mechanical Engineering and Technology. 9(5). (2018): 958-965.