International Journal of Mechanical Engineering and Technology (IJMET)
Volume 9, Issue 5, May 2018, pp. 958–965, Article ID: IJMET_09_05_106
Available online at http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=9&IType=5
ISSN Print: 0976-6340 and ISSN Online: 0976-6359

APPLICATION OF SPOOF RESISTANT AUTHENTICATION PROTOCOL OF SPACECRAFT IN LOW EARTH ORBIT SYSTEMS OF SATELLITE COMMUNICATION

Vladimir Petrovich Pashintsev, Igor Anatolyevich Kalmykov, Aleksandr Pavlovich Zhuk, Maksim Igorevich Kalmykov
North-Caucasus Federal University, Stavropol, 355009, Russia

Denis Nikolaevich Rezenkov
Stavropol State Agrarian University, Stavropol, 355017, Russia

ABSTRACT

Efficient application of low Earth orbit (LEO) satellite communication systems (SCS) is clearly demonstrated in remote monitoring and control complexes of non-maintainable facilities intended for production and transportation of hydrocarbons in the Far North. In order to arrange continuous communication with such facilities SCS is comprised of from 48 to 60 spacecrafts. Increase in the number of such orbital constellations can lead to situation when an alien satellite would attempt to impose previously intercepted command to receiver located on non-maintainable facility. As a consequence, the intercepted and imposed control command would shut down the oil production facilities, thus impairing Arctic wild landscape. In order to prevent such situation, it is proposed to apply Identification-Friend-or-Foe system (IFF system) of spacecraft (SC). It is obvious that spoof resistance of such system depends mainly on authentication protocol. Aiming at reduction of time consumptions for authentication, this article proposes to use modular codes. In such codes computations are carried out in parallel according to code modules and independent on each other. The aim of the work is increase in execution of question/answer authentication protocol by means of modular codes.

Keywords: inquiry/response system of satellite identification, question/answer authentication protocols, zero knowledge proofs, modular code.

Cite this Article: Vladimir Petrovich Pashintsev, Igor Anatolyevich Kalmykov, Aleksandr Pavlovich Zhuk, Maksim Igorevich Kalmykov and Denis Nikolaevich Rezenkov, 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, pp. 958–965
http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=9&IType=5

1. INTRODUCTION

Application of remote monitoring and control systems of oil production facilities located within the Polar Circle makes it possible to decrease prime cost of production and transportation of hydrocarbons. The use of LEO SCS makes it possible to provide continuous communication between non-maintainable facilities and control center. Flyover time of LEO spacecraft (SC) above subscriber can be as low as 10-20 minutes. Herewith, there is higher probability that a violator would attempt to disturb normal operation of LEO SCS by interception, delay and imposing of control command. In its turn, this leads to destabilization of monitoring and control system of environmentally dangerous facilities with possible equipment failures. The involved consequences can partially disturb activity of Far North ecosystem.

One of the approaches to solve this problem is application of IFF system which can identify SC status in real time in the visibility range of subscriber terminal of remote controlled facility [1]. It is obvious that spoof resistance of such system depends mostly on authentication protocol. As a rule, such inquiry/response protocols based on zero-knowledge proof are implemented according to large module which influences negatively on authentication rate. The time consumption for verification of satellite status can be decreased by application of modular codes (MC) [2-4]. Hence, implementation of authentication protocols with zero knowledge proof on the basis of modular codes is an urgent task.

2. METHODS

2.1. Modular codes

Modular codes include position-independent codes where X is presented as remainders $X = (x_1, x_2, ..., x_k)$, where $x_i \equiv X \bmod m_i$, m_i are the co-prime MC bases, i = 1, 2, …, k [2, 5, 6]. Then, for MC the following expressions are valid:

$$X + Y = ((x_1 + y_1) \bmod m_1, ..., (x_k + y_k) \bmod m_k), \quad (1)$$

$$X - Y = ((x_1 - y_1) \bmod m_1, ..., (x_k - y_k) \bmod m_k), \quad (2)$$

$$X \cdot Y = ((x_1 \cdot y_1) \bmod m_1, ..., (x_k \cdot y_k) \bmod m_k), \quad (3)$$

where $Y \equiv y_i \bmod m_i$; i = 1, 2, …, k.

In order to obtain correct answer in MC, it is required that the results are in the scope of operating range:

$$P = \prod_{i=1}^{k} m_i. \quad (4)$$

In order to perform conversion from MC to position code (PC), the Chinese remainder theorem is applied according to which the following is valid:

$$X = \sum_{i=1}^{k} x_i T_i M_i \ (\bmod P), \quad (5)$$

where $M_i = P/m_i$; $T_i M_i = 1 \bmod m_i$.

Analysis of Eqs. (1)- (3) demonstrates that MC are characterized by high response, since paralleling in them takes place at the level of arithmetic operations [3, 7- 9]. Due to such properties, MC is applied in digital signal processing systems [10-12]. The work [5] describes principles of neurocomputer architecture operating in MC. Application of neural finite ring network and adjusting MC made it possible to develop architecture of fault-free neurocomputer. The work [10] describes application of MC in digital filtration. The use of parallel computing channels determined by MC bases made it possible to develop digital filter of residue class operating in real time. The works [12, 7, 9] describe principles of application of excessive MC. Independent residue processing by computing tracts determined by MC bases, the absence of mutual exchange operations among MC modules make it possible not only to increase signal processing rate but also to improve the system failure safety. Introduction of two control MC bases enables correction of 100% of single errors, occurring during computations due to faults upon operation. The work [13] describes possibility to apply polynomial MC in order to improve reliability of AES encryption. The developed new architecture principles of correcting polynomial MC improve reliability of SPN cryptosystems upon the use of one excessive base. The work [14] presents cash withdrawal protocol based on MC.

2.2. Zero knowledge proof

The performed studies demonstrated that the operation algorithm of IFF system was based on inquiry/response protocols. Such protocols are efficiently used in interactive information systems where prior to the dialogue between two subjects each of them should verify the appropriate status of the other [15].

In order to develop spoof resistant system of friend-or-foe identification, it would be reasonably to use authentication protocols based on zero knowledge proof and characterized by high encryption strength. The work [16] presents the Fiat-Shamir authentication protocol, for its implementation **t** verification rounds are required. Each round includes three-step algorithm of interactive data exchange in order to verify a candidate. Encryption strength of one round is 0.5. In order to increase the protocol encryption strength **t** rounds of verification are required. Herewith, the protocol encryption strength increases with the number of rounds. The authors [17] present the Guillou-Quisquater protocol which involves lower number of rounds of data exchange than the Fiat-Shamir protocol. However, in order to achieve the preset probability of correction proof of the presented identifier, multiround authentication procedure is required. This can be eliminated by the Schnorr authentication protocol [16].

Aiming at improvement of encryption strength, such protocols use high numbers. However, increase in the length of processed data leads to decrease in the rate of multiplicative operations. Application of MC increases the computation rate. This is stipulated by the fact that operands in these codes are modulo remainders of MC. And addition, subtraction and multiplication are performed in parallel without data exchange between different modules.

Now let us consider implementation of this protocol in modular code. We select prime numbers $m_1, m_2, \ldots, m_k$ as bases, then we determine prime number q_i, $q_i \mid m_i$ for them. Then we determine the number g_i, satisfying the condition:

$$g_i^{q_i} \equiv 1 \bmod m_i . \qquad 6$$

The secret key is the number $L = (l_1, l_2, \ldots, l_k)$, satisfying the condition:

$$L < H = \prod_{i=1}^{k} q_i \quad . \qquad 7$$

The open key is the number $Z = (z_1, z_2, \ldots, z_k)$, for which the following is valid:

$$z_i = g_i^{-l_i} \bmod m_i \quad . \qquad 8$$

Authentication protocol is executed as follows:

1. Candidate A selects random number $T = (t_1, t_2, \ldots, t_k)$, satisfying the condition $T < H$. Then the number $U = (u_1, u_2, \ldots, u_k)$ is calculated as follows:

$$u_i = g_i^{t_i} \bmod m_i \quad . \qquad 9$$

The calculated value is transferred to verifying subscriber B.

2. The subscriber B selects random number $S = (s_1, s_2, ..., s_k) \in \{1, 2, ..., 2^v - 1\}$, where v is a certain selected parameter. This number is sent to the subscriber A.

3. The subscriber A, receiving the number E, determines the number $D = (d_1, d_2, \ldots, d_k)$ as follows:

$$d_i = (t_i + s_i l_i) \bmod q_i \quad . \qquad 10$$

The calculated $D = (d_1, d_2, \ldots, d_k)$ is sent to the subscriber B.

4. The subscriber B, receiving the response $D = (d_1, d_2, \ldots, d_k)$, verifies the response correctness:

$$f_i = g_i^{d_i} z_i^{s_i} \bmod m_i \quad . \qquad 11$$

If the calculated $F = (f_1, f_2, \ldots, f_k)$ coincides with $U = (u_1, u_2, \ldots, u_k)$, then the candidate A is "a friend", otherwise, the candidate A is "a foe".

With the aim of comparative analysis, let us apply the developed authentication protocol implemented in MC. This protocol is based on single module protocol enabling identification of candidate status [1]. In this protocol an MC session key $S(j) = (S_1(j), S_2(j), ..., S_k(j))$ and parameter $T(j) = (T_1(j), T_2(j), ..., T_k(j))$ are used for the equation of repeated use of session key, where $S(j) \equiv S_i(j) \bmod m_i$; $T(j) \equiv T_i(j) \bmod m_i$; i = 1, 2, …, k.

At preliminary stage of authentication, the following computations are performed:

1. Candidate A computes real satellite status presented in MC:

$$C_i = \left| g^{S_i(j)} g^{T_i(j)} \right|_{m_i}^{+} , \qquad 12$$

where **g** is the generator of multiplicative group of modulo m_i; i = 1, 2, …, k.

2. The candidate A shadows secret parameters of the protocol:

$$S_i^*(j) = \left| S_i(j) + \Delta S_i(j) \right|_{m_i}^{+} ; \quad T_i^*(j) = \left| T_i(j) + \Delta T_i(j) \right|_{m_i}^{+} . \qquad 13$$

where $\Delta S(j), \Delta T(j)$ are random values; $\Delta S(j) \equiv \Delta S_i(j) \bmod m_i$; $\Delta T(j) \equiv \Delta T_i(j) \bmod m_i$.

3. The candidate A calculates the noisy satellite status using MC:

$$C_i^* = \left| g^{S_i^*(j)} g^{T_i^*(j)} \right|_{m_i}^+ . \quad 14$$

Authentication algorithm is comprised of the following stages:

1. Interrogator B transfers random number d = (d1, d2, …, dk) to the candidate A.

2. The candidate A, receiving d = (d1, d2, …, dk), calculates responses as follows:

$$r_i(1) = \left| S_i^*(j) - d_i S_i(j) \right|_{\varphi(m_i)}^+ ; \; r_i(2) = \left| T_i^*(j) - d_i T_i(j) \right|_{\varphi(m_i)}^+ . \quad 15$$

The candidate A sends the following data to the interrogator B:

$$\left\{ (C_1, ..., C_k), (C_1^*, ..., C_k^*), (r_1(1), ..., r_k(1)), (r_1(2), ..., r_k(2)) \right\}$$

3. The interrogator B verifies the received responses d = (d_1, d_2, …, d_k):

$$Y_i = \left| C_i^{d_i} g^{r_i(1)} g^{r_i(2)} \right|_{m_i}^+ . \quad 16$$

The candidate A is "a friend", if the following is valid:

$$\left\{ Y_1 = C_1^*, Y_2 = C_2^*, ..., Y_k = C_k^* \right\} . \quad 17$$

3. RESULTS

Let us consider execution of the Schnorr authentication protocol in MC. We select the MC bases of modular code: m_1 =11, m_2 = 23, m_3 = 29. Operation range of the system is P = 7337. Let us determine factors of MC bases:q_1 = 5, q_2 = 11, m_3 = 7 with Q = 385. Let us use Eq. (6) and select g_1 = 3, g_1 = 2, g_3 = 7. Let the secret key of the subscriber A be L = (3, 5, 5). Then the first portion of the open key presented in modular code is as follows:

$$z_1 = g_1^{-l_1} \bmod m_1 = 3^{-3} \bmod 11 = 9 ;$$

$$z_2 = g_2^{-l_2} \bmod m_2 = 2^{-5} \bmod 23 = 18 ;$$

$$z_3 = g_3^{-l_3} \bmod m_3 = 7^{-5} \bmod 29 = 20 .$$

The open key is $(z_i, m_i, g_i) = ((9, 18, 20)(11, 23, 29)(3, 2, 7))$.

1. The candidate A selects numbers $T = (2, 7, 2)$ and calculates:

$$u_1 = g_1^{t_1} \bmod m_1 = 9 ; \; u_2 = g^{t_2} \bmod m_2 = 13 ; \; u_3 = g_3^{t_3} \bmod m_3 = 24 .$$

The calculated U = (9, 13, 24) is transferred to the interrogator B.

2. The interrogator B selects S = (4, 8, 4) which is transferred to the candidate A.

3. The candidate A calculates the response by Eq. (10):

$$d_1 = (t_1 + s_1 l_1) \bmod q_1 = 4 ; \; d_2 = (t_2 + s_2 l_2) \bmod q_2 = 3 ; \; d_3 = (t_3 + s_3 l_3) \bmod q_3 = 2 .$$

The calculated D= (4, 3, 2) is transferred to the subscriber B.

4. The subscriber B verifies correctness of the response $f_1 = g_1^{t_1} z_1^{s_1} \bmod m_1 = (3^4 \cdot 9^4) \bmod 11 = 9$.

$f_2 = g_2^{t_2} y_2^{s_2} \bmod m_2 = (2^3 \cdot 18^8) \bmod 23 = 13$; $f_3 = g_3^{t_3} y_3^{s_3} \bmod m_3 = (7^2 \cdot 20^4) \bmod 29 = 24$.

Since F = (9, 13, 24) = U is valid, then the status of the candidate A is "a friend".

Let us consider execution of the developed authentication protocol in MC. The bases m_1 =13, m_2 = 19, m_3 = 29 are given, we have for them: g = 2. The working range is P = 7136. The session key is S(j) = 16 = (3, 16, 16) and T(j) = 25 = (12, 6, 25). Using Eq. (12), we obtain real spacecraft status:

$$C_1 = g^{S_1} g^{T_1} \bmod m_1 = \left|2^3 \cdot 2^{12}\right|_{13}^{+} = 8; \quad C_2 = g^{S_2} g^{T_2} \bmod m_2 = \left|2^{16} \cdot 2^6\right|_{19}^{+} = 16;$$

$$C_3 = g^{S_3} g^{T_3} \bmod m_3 = 14.$$

Real status in code C = (8, 16, 14) is stored in the satellite memory.

Let us select the noise value equaling to $\Delta S = 7, \Delta T = 8$. Then the noisy values are $S^*(j)$ = (10, 4, 26) and $T^*(j)$ = (7, 15, 4). Using (Eq. 12), we obtain the value of satellite noisy status :

$$C_1^* = \left|g^{S_1^*} g^{T_1^*}\right|_{13}^{+} = \left|2^{10} \cdot 2^7\right|_{13}^{+} = 6; C_2^* = \left|g^{S_2^*} g^{T_2^*}\right|_{19}^{+} = \left|2^4 \cdot 2^{15}\right|_{19}^{+} = 2; C_3^* = \left|g^{S_3^*} g^{T_3^*}\right|_{29}^{+} = \left|2^{26} \cdot 2^4\right|_{29}^{+} = 4.$$

The calculated noisy status C^* = (6, 2, 4) is stored in memory.

Upon satellite authentication the interrogator transfers random number d = (8, 5, 4). Let us determine the responses to inquiry d_1 = 8. We obtain as follows:

$$r_1(1) = \left|S_1^*(j) - d_1 S_1(j)\right|_{12}^{+} = \left|10 - 8 \cdot 3\right|_{12}^{+} = 10; r_1(2) = \left|T_1^*(j) - d_1 T_1(j)\right|_{12}^{*} = \left|7 - 8 \cdot 12\right|_{12}^{+} = 7.$$ Let us determine the responses to inquiry d_2 = 5. We obtain as follows:

$$r_2(1) = \left|S_2^*(j) - d_2 S_2(j)\right|_{18}^{+} = \left|4 - 5 \cdot 16\right|_{18}^{+} = 14; r_2(2) = \left|T_2^*(j) - d_2 T_2(j)\right|_{18}^{+} = \left|15 - 5 \cdot 6\right|_{18}^{+} = 3.$$

Let us determine the responses to inquiry d_3 = 4. We obtain as follows:

$$r_3(1) = \left|S_3^*(j) - d_3 S_3(j)\right|_{28}^{+} = \left|26 - 4 \cdot 16\right|_{28}^{+} = 18; r_3(2) = \left|T_3^*(j) - d_3 T_3(j)\right|_{28}^{+} = \left|4 - 4 \cdot 25\right|_{28}^{+} = 16.$$

Real and noisy statuses as well as responses to the random number **d** are transferred to the interrogator. The interrogator verifies the spacecraft status:

$$A_1 = \left|C_1^{d_1} g^{r_1(1)} g^{r_1(2)}\right|_{m_1}^{+} = \left|2^5\right|_{13}^{+} = 6;$$

$$A_2 = \left|C_2^{d_2} g^{r_2(1)} g^{r_2(2)}\right|_{m_2}^{+} = \left|2^{37}\right|_{19}^{+} = 2;$$

$$A_3 = \left|C_3^{d_3} g^{r_3(1)} g^{r_3(2)}\right|_{m_3}^{+} = \left|2^{86}\right|_{29}^{+} = 4.$$

Since $A_1 = C_1^* \bmod m_1 = 6, A_2 = C_2^* \bmod m_2 = 2, A_3 = C_3^* \bmod m_3 = 4$, then the interrogator determines that the spacecraft is "a friend', the satellite and the controlled facility start data exchange.

4. DISCUSSION

The performed studies demonstrated efficiency of modular code in the considered authentication protocols based on zero knowledge proof. It is known that the rate of multiplicative modulo operations is proportional to the operand length. In the considered

examples the use of isomorphism generated by the Chinese remainder theorem made it possible to transfer from computations with 17-digit numbers to computations with 5-digit operands. Therefore, the use of modular code increased the rate of computations more than by 3 times in comparison with single module protocol implementation. In addition, the obtained results clearly evidence that the developed protocol of satellite status identification implemented in modular code requires time consumption for authentication lower by the factor of 1.33 in comparison with the Schnorr protocol. This is attributed to the fact that the developed authentication protocol contains less stage required for satellite status identification. Moreover, the Schnorr authentication protocol involves open and private keys applied for subscriber identification. Herewith, the interrogator should have the secret key located on non-maintainable controlled facility. Since such facilities are numerous and they are in low population areas, this increases the chance of unauthorized access to secret key. And this can impair encryption strength of IFF system for LEO SCS. In the developed protocol, authentication does not require a secret key. Therefore, the developed authentication protocol implemented in modular code is the most promising for application in IFF systems.

5. CONCLUSION

This article presented the developed authentication protocol based on zero knowledge proof implemented by modular codes. The developed authentication protocol was compared with the Schnorr protocol with applied multiple module implementation. The obtained results demonstrated that the developed protocol of satellite status identification based on modular code required time consumptions lower by the factor of 1.33 than the Schnorr protocol. The obtained results evidence reasonability of the developed authentication protocol based on modular code in inquiry/response system of satellite identification.

ACKNOWLEDGMENTS

This work was supported by the Russian Foundation for Basic Research, project No. 18–07-01020.

REFERENCES

[1] Pashintsev, V. P. and Lyakhov A. V. Primenenie pomekhoustoichivogo protokola autentifikatsii kosmicheskogo apparata dlya nizkoorbital`noi sistemy sputnikovoi svyazi [Application of spoof resistant authentication protocol of spacecraft for low Earth orbit system of satellite communication]. Infokommunikatsionnye tekhnologii, 2, 2015, pp. 183-190.

[2] Ananda Mohan, P. V. Residue Number Systems: Theory and Applications. Springer, Basel: Birkhäuser, 2016.

[3] Chervyakov, N. I., Kolyada, A. A. and Lyakhov, P. A. Modulyarnaya arifmetika i ee prilozheniya v infokommunikatsionnykh tekhnologiyakh [Modular arithmetic and its provisions in communication technologies]. Moscow: FIZMATLIT, 2017.

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

[5] Chervyakov, N. I., Lyakhov, P. A., Babenko, M. G. An efficient method of error correction in fault-tolerant modular neurocomputers. Neurocomputing, 205, 2016, pp. 32-44.

[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, pp. 108-113.

[7] Katkov K. A., Naumenko D. O., Sarkisov A. B., & Makarova A. V. Parallel Modular Technologies in Digital Signal Processing. Life Science Journal, 11(11 s), 2014, pp. 435-438.

[8] Veligosha, A. V., Kaplun, D. I., Klionskiy, D. M., Kalmykov, I. A. and 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, pp.213-214.

[9] Stepanova, E. P. and 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.

[10] Chervyakov, N. I., Veligosha, A. V. and Ivanov, P. E. Digital filters in a system of residual classes Izvestiya Vysshikh Uchebnykh Zavedenij. Radioelektronika, 38(8), 1995, pp. 11-20.

[11] Katkov K. A., Timoshenko L. I., Dunin A. V., & Gish T. A. Application of Modular Technologies in the Large-Scale Analysis of Signals. Journal of Theoretical and Applied Information Technology, 80(3), 2015, pp. 391-400.

[12] Kaplun, D. I., Klionskiy, D. M. and Bogaevskiy, D. V. Error correcting of digital signal processing devices using non-positional modular codes. Automatic Control and Computer Sciences, 51(3), 2017, pp. 167-173.

[13] Stepanova, E. P., Toporkova, E. V., Kalmykov, M. I., Katkov, R. A. and Rezenkov, D. N. 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, pp. 114-123.

[14] Yurdanov, D. A., Gostev D. B. and Kalmykov M. I. The implementation of information and communication technologies with the use of modular codes. CEUR Workshop Proceedings 1837, 2017.

[15] Goldwasser, S. and Kalai, Y. T. On the (In) security of the Fiat-Shamir Paradigm. 44th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, October, 2003, pp. 102-115.

[16] Hannu, A. P. and Aronsson J. Zero Knowledge Protocols and Small Systems, 1995. http://www.tml.tkk.fi/Opinnot/Tik-110.501/1995/zeroknowledge.html.

[17] Menezes, A., Van Oorschot, P. and Vanstone, S. Handbook of Applied Cryptography. CRC Press, 1996, pp. 816.

[18] Deepali Y Kirange and Kalyani N Neve, Wireless Communication: The Comparative Study Between Broadcasting, Satellite Communication and Cellular Service, International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 5, September – October (2013), pp. 31-41