Development of Imitation-resistant Authentication Protocol for Low-orbital Space Satellite Communication System

Igor Kalmykov
NorthCaucasus Federal University
Stavropol, 355017
kia762@yandex.ru

Maria Lapina
NorthCaucasus Federal University
Stavropol, 355017
mlapina@ncfu.ru

Maxim Kalmykov
NorthCaucasus Federal University
Stavropol, 355017
kim762@yandex.ru

Igor Provornov
NorthCaucasus Federal University
Stavropol, 355017
kia545@yandex.ru

Evgeniy Voloshin
NorthCaucasus Federal University
Stavropol, 355017
norra170@gmail.com

Abstract

In recent years, there has been a tendency to expand the use of low-orbit satellite communication systems (LOSCS). A special role belongs to the systems of remote monitoring, control and management of unattended objects of environmentally hazardous technologies. To ensure uninterrupted operation of the satellite communications system, a certain number of spacecrafts are combined into an orbital group. For a low-orbit CAS, the group consists of 48-60 satellites. However, due to the increase in the number of LOSCS, a situation may arise when a "foe" satellite gets in sight of a satellite communications receiver, which is located at the subscriber terminal of an unattended facility, attempts to impose a previously intercepted control command. This can lead to failure of the control object and provoke an environmental disaster. In order to prevent such a situation, it is necessary to increase the imitation resistance of the LOSCS. It is possible to solve this problem by using the identification of the Identification-Friend-or-Foe system (IFF system) of a spacecraft. Obviously, the effectiveness of such a system is primarily determined by the authentication protocol. Therefore, the goal of the research is to improve the imitability of the LOSCS by a satellite identification system using the developed authentication protocol, built on evidence with zero disclosure zeroknowledge proof knowledge (ZKPK).

Keywords: satellite identification system, authentication protocols with zero knowledge disclosure, algorithm of checking for session key reuse.

In: S. Hölldobler, A. Malikov (eds.): Proceedings of the YSIP-3 Workshop, Stavropol and Arkhyz, Russian Federation, 17-09-2019–20-09-2019, published at http://ceur-ws.org

Introduction

Providing the communication services for global projects like the development of the Northern Sea Route, the creation of information and telemetric systems for air and land transport in high latitudes is impossible without the use of low-orbit satellite communication systems (LOSCS). Satellite communication systems such as Iridium and Iridium NEXT are now widely used to solve these tasks [Iri18], [Iri18], [Wha18].

One of the most promising areas of application of the LOSCS is the exploitation of mineral resources in the regions of the Far North. In this case, LOSCS are an important part of automated management, remote monitoring and control systems, which are used to manage the maintenance-free hydrocarbon production and transportation facilities located beyond the Polar Circle. To organize uninterrupted communications, the NSSS group should contain 48 to 60 spacecraft. However, the increase in the number of countries participating in the development of the natural resources of the Arctic, as well as the large spatial extent of communication lines leads to an increase in the number of satellite constellations. Because of this, a situation may arise when a satellite of the intruder may be in the visibility zone of the receiver, which may disrupt the operation of the LOSCS. This can lead to the failure of maintenance-free control facility and provoke an environmental disaster.

It is possible to solve this problem by increasing the imitation resistance of the LOSCS. To counteract the imposition of an intercepted command, it is advisable to use a satellite identification system (SIS). For efficient work of the inquiry-response identification system friend-foe, it is necessary, foremost, to use an imitation-resistant authentication protocol, and, secondly, encrypting algorithms should not be used when checking satellite status. This problem can be solved only with the help of request-response type protocols, built on evidence with zero disclosure of zero-knowledge proof knowledge (ZKPK) [Feg03], [Pas18], [Sta99], [Smi02]. Therefore, the development of an imitation-resistant authentication protocol with zero disclosure and the minimum time spent on checking the status of a satellite is a topical task.

1 Material and methods of research

1.1 Destructive effects on the low-orbit satellite communication system

An analysis of the following works was carried out to develop the most effective method of countering the destructive effects of the intruder satellite [Mcd17], [Poi12], [Spe02], which allowed to discern three groups of such effects. The basis of the first class of effects on the communication system consists of various methods of electronic signal suppression. The main goal of the electronic signal suppression methods is blocking the transmitted signal from the spacecraft to the control object and back. Usually, active or passive interference is used for this, among which there are:

- harmonic continuous interference, which is determined by equation:

  $$U_{GNP}(t) = U_{mm}cos(\omega_{p2}t + \phi_{p2}(t)), \tag{1}$$

  where $\omega_{p2} \in [\omega_0 - \pi\Delta f_2; \omega_0 + \pi\Delta f_2]$ - angular interference frequency; U_{mm} - amplitude of harmonic continuous interference; ϕ_{p2} - initial phase of harmonic continuous interference.

- quasi-white noise-like interference determined by

  $$U_{SHP}(t) = U_{mm}cos(\omega_{p1}t + \phi_{p1}(t)), \tag{2}$$

  where $U_{mm}(t)$ - alteration in enveloping noise-like interference; $\phi_{p1}(t)$ - phase change in noise-like interference; ω_{p1} - average interference frequency; $\omega_1 \approx \omega_0; \omega_0 = 2\pi L; L$ - carrier wave frequency; - active amplitude modulated noise interference

  $$U(t) = U_P[1 + K_\alpha \Delta U_{MOD}(t)], \tag{3}$$

  where K_α - slope of modulation transmitter characteristic; $\Delta U_{MOD}(t)$ - modeling direction coming from the noise generator.

The basis of the second group is simulated interference. Such interference is called intelligent interference, as it is able to adapt to the transmitted signal, thereby disrupting the effective operation of the radio communication system. The most widespread are:

– targeted simulating disturbance, which is determined by the equation:

$$U_{PIP}(t) = KU_m Q_\iota(t - t_d - \Delta\tau) sin[2\pi(L \pm \Delta f)(t - t_d - \Delta\tau) + \phi], \tag{4}$$

where K - coefficient accounting the targeted simulating disturbance;

– tracking imitation interference,

$$U_{SIM}(t) = KU_m Q(t - t_d - \tau(t)) sin[2\pi(L \pm \Delta f)(t - t_d - \tau(t)) + \phi], \tag{5}$$

where $\tau(t) = r(t)/c$ - distance from satellite to the station.

A special place among the destructive effects on the satellite communication system is occupied by the relay interference. In this case, the intruder satellite intercepts the control command, delays it, and then sends it. Then the receiver located on the control object perceives the received signal as its own and transmits a command to the control system of a maintenance-free object, which can lead to disruption and breakdown.

Studies have shown that in the conditions of the Far North, the method of setting relay interference is the most effective method, while the use of active, passive and imitating interference is a difficult task. Therefore, this paper will propose methods for countering relay interference.

In order to forbid the intruder satellite imposing an intercepted and delayed command on the subscriber station, it is necessary to prevent data exchange between such a spacecraft and the receiver located at the control object. To do this, it is advisable to determine the satellite status before starting a communication session. Because of the use of the friend or foe identification, a satellite that fails authentication will not be able to communicate with the receiver of the subscriber terminal of the remote control object. Currently, there are many "friend or foe" identification systems, which are widely used in many countries. The analysis of the basic principles of building data of the friend or foe identification showed that they are unable to authenticate the satellite and cannot be used in the LOSCS.

1.2 Authentication protocols

This problem can be solved by developing a new method for constructing the friend-foe identification system, which would allow to authenticate the LOSCS satellite using a strong cryptographic protocol. Currently, cryptographic authentication protocols can be divided into three groups. The first group is based on password authentication protocols [Sta99], [Shr96], [Feg10], [Smi02].

Authentication protocols that make up the second group have higher cryptographic security. Such protocols use a request-response method. As these works show, [Sta99], [Feg10], [Smi02] it is proposed to use both symmetric and asymmetric cryptographic systems to increase the strength of such protocols. It should be noted that the following this condition for a group of spacecrafts LOSCS is rather difficult. This is because not only satellites, but the unattended control objects must have the secret keys.

Authentication protocols with zero knowledge proof lack this flaw. They make up the third group. These works [Sha03], [Feg10] examine the Fiat-Shamir protocol.

In order to ensure the required level of probability of noticing an intruder, the authentication procedure is performed repeatedly, where W = 20-40 rounds.

The Schnorr protocol, which is presented in these works, allows to reduce the time spent on authentication, [Sch96], [Fer03]. Although this protocol allows one round authentication, it nevertheless has drawbacks:

– three data exchanges are required between applicant P and verifier V for authentication;

– periodically changing session keys Sj, j = 1, 2, ... are not used.

The developed authentication protocol built on evidence with zero knowledge disclosure and minimum number of identification steps allows to eliminate these drawbacks [Gos15]. This protocol consists of the following steps:

At the preliminary stage of the protocol, the irreducible polynomial $p(x)$ and the value of the secret key and the random number S are chosen. The value of the secret key and S are used to calculate the session keys S_j, where $j = 1, 2, ...$, which satisfy the condition

$$K^{sek} \leq 2^{degp(x)} - 1. \tag{6}$$

$$S \leq 2^{degp(x)} - 1. \tag{7}$$

where $degp(x)$ - is the degree of $p(x)$ polynomial.

The operation of the authentication protocol involves the transponder, which resides on board the satellite and the interrogator that resides at the control site. First, the transponder, upon receiving the value S_j K^{sek} of the session key, calculates the true status of the satellite

$$M_j(x) = X^{S_j} X^{K^{sek}} modp(x) \tag{8}$$

where $S_j(x) = x^{(S_j - 1 + K^{sek})^{-1}} modp(x)$- value of the j-th session key.

If during the calculation of the session key Sj the following condition is true,

$$S_{j-1} + K^{sek} = 0mod2^{degp(x)-1}, \tag{9}$$

then this value is replaced by $2^{degp(x)-1} - 1$.

The next step is to conduct the noise interference of the secret key values and Sj. To do this, the values that change during each session are used. As a result, we get the following expressions

$$\tilde{K}_j^{sek} = (K^{sek} + \Delta K^{sek}) mod2^{degp(x)} - 1, \tag{10}$$

$$\tilde{S}_j = (S_j + \Delta S_j) mod2^{degp(x)} - 1, \tag{11}$$

where $\tilde{K}_j^{sek}, \tilde{S}_j$ are noise-modified values.

Then the noise-modified satellite image will be determined based on the expression

$$\tilde{M}_j(x) = x^{\tilde{S}_j} x^{\tilde{K}^{sek}} modp(x) \tag{12}$$

True and noise-modified satellite images will be used to verify its authenticity. To perform such authentication, the interrogator sends a question, which is a random number.

Upon receiving the d_j query, the transponder must answer the question

$$r_j(1) = (\tilde{K}_j^{sek} - d_j K^{sek}) mod2^{degp(x)} - 1, \tag{13}$$

$$r_j(2) = (\tilde{S}_j - d_j S_j) mod2^{degp(x)} - 1, \tag{14}$$

The transponder sends $(M_j(sek), \tilde{M}_j(sek), r_j(1), r_j(2))$ to the interrogator.

To verify the correctness of the received answers, the verifier V uses an expression in which the true $M_j(sek)$, noise-modified $\tilde{M}_j(sek)$ images of the satellite, two answers $r_j(1)$ and $r_j(2)$, and the question dj must be included. The following expression is used to check the received answers:

$$B_j(x) = M_j(x)^{d_j} X^{r_j(1)} X^{r_j(2)} modp(x). \tag{15}$$

If the $B_j(x) = M_j(x)$ condidtion is true, then the satellite is assigned the status of "friend". Otherwise, satellite status is foe.

Analysis of the developed authentication protocol indicated that it can conduct satellite identification at a higher speed, since the authentication process consists of two stages. To assess the effectiveness of the developed authentication protocol, a comparative analysis was conducted with the Fiat-Shamir and Schnorr protocols. The analysis showed that the developed protocol allows the authentication procedure to be performed in two stages, which is 30 times faster than the Fiat-Shamir protocol and 1.5 times faster than the Schnorr protocol.

It is obvious that the imitability of this authentication protocol will be determined by the session keys S_j, where $j = 1, 2, ...$ If during the operation of the transponder the value of the session key does not change, it will result in the signals transmitted to the interrogator during the $j - thand(j + 1) - th$ session to overlap, since $C_j(x) = C_{j+1}(x)$. In this case, the length of the L-bit response transmitted to the interrogator was reduced by the degree of the selected polynomial $p(x)$. This will lead to an increase in the probability of the answer being guessed by the foe satellite, since

$$P = \frac{1}{2^L} < P^* = \frac{1}{2^{L-degp(x)}} \tag{16}$$

where p^* - probability of guessing the answer when the session key is reused.

This means that double use of the session key reduces the protocol's imitation resistance. In [Lap18] an algorithm that allows to check the correctness of the generation of S_j and the additional parameter T_j is presented. To do this, the verifying party sends the satellite a random query number r. After receiving the question r, the spacecraft calculates the answers.

$$a^*_j(S) = (a_j(S) - r)modq, a^*_j(T) = (a_j(T) - r)modq, \tag{17}$$

where $a_j(T) = \Pi^m_{\iota=1}\frac{1}{T_j+K_j}modq; a_j(S) = \Pi^m_{\iota=1}\frac{1}{S_\iota+K_\iota}modq.$

The blurred values are then calculated.

$$S^*_j = g^{a^*_j(S)}modq, T^*_j g^{a^*_j(T)}modq. \tag{18}$$

The spacecraft finds the product of the true values of Sj and Tj, as well as the blurred parameters. The results are sent to the verifying party V, which checks the obtained values.

$$A = \frac{S_j T_j}{S^*_j T^*_j} = g^{2r}modq. \tag{19}$$

If the calculated value, according to (19), satisfies

$$A^{`} = (g^r)^2 modq = A, \tag{20}$$

this suggests that the values of S_j and the corresponding parameter T_j are generated correctly. However, this algorithm does not allow to determine the reuse of S_j. The developed algorithm for the dual session key reuse check allows to eliminate this drawback.

The satellite and the operation support center (OSC), which controls the operation of the automated facility monitoring system, are involved in the verification. In the developed protocol, an additional parameter T_j is introduced, with which it would be possible to verify if the session key was reused

$$S_j(x) = x^{(S_{j-1}+K^{sek})^{-1}}modp(x). \tag{21}$$

$$T_j(x) = x^{(S_{j-1}+K^{sek}+T)^{-1}}modp(x). \tag{22}$$

where $S_0 = S; j = 1, 2, ...$ If during the calculation of the session key S_j the condition is true, (23)

$$(S_{j-1} + K^{sek} + T_{j-1}) = 0mod2^{degp(x)-1}, \tag{23}$$

then this value is replaced by $2^{degp(x)-1}$.

In the developed algorithm, T_j is used to calculate the test parameter E_j, with which the satellites public key will be obtained when the condition $S_j = S_j + 1$ is true. In the course of the research, an equation was chosen to determine

$$E_j = K^{pub}T^{Y_j}_j modp(x). \tag{24}$$

where Y_j - query number, that is set by OSC on j-th session; $Y_j < 2^{degp(x)-1}$.

The developed algorithm for checking the reuse of the session key in the satellite identification system consists of the following steps.

1 The transponder calculates the values of the session key Sj and Tj.

2 At the j-th session, the center makes a request for which a random number is used.

3 The trasponder, upon receiving this request, calculates the answer (24)

4 E_j, Y_j are transmitted to the center.

5 In the next session, the responder calculates the values of the session key S_{j+1} and T_{j+1}.

6 At the $j+1$-st session, the center makes a request for which a random number is used.

7 The trasponder, upon receiving this request, calculates the answer

$$E_{j+1} = K^{pub} T_{j+1}^{Y_{j+1}} modp(x). \tag{25}$$

8 E_{j+1}, Y_{j+1} are transmitted to the center.

9 The center performs a session key reuse check in the spacecraft identification system

$$W = \left| \left(\frac{(E_j)^{Y_{(j+1)}}}{(E_{j+1})^{Y_{(j)}}} \right)^{(Y_{(j+1)} - Y_{(j)})^{-1}} \right|^{+}_{2^{degp(x)}-1} \tag{26}$$

If the public key of the K^{pub} spacecraft is obtained, this indicates that the satellite reused the session key S_j.

Consider the situation when the operation of the pseudo-random function generator that calculates session keys S_j was disrupted. In this case, the values of the neighboring session keys S_j and S_{j+1} will match

$$S_j(x) = x^{(S_{j-1}+K^{sek})^{-1}} modp(x) = x^{(S_j+K^{sek})^{-1}} modp(x) = S_{j+1}(x). \tag{27}$$

Suppose we have the following equation $S_j = S_{j+1} = S$. Parameters $T_j and T_{j+1}$ are used in the algorithm for checking the reuse of the session key

$$T_j(x) = x^{(S_{j-1}+K^{sek}+T)^{-1}} modp(x) = x^{(S_j+K^{sek}+T)^{-1}} modp(x) = T_{j+1}(x). \tag{28}$$

Then on receiving $Y_{j+1} < 2^{degp(x)} - 1$ query, the transponder sends to the center

$$E_j = K^{pub} T_j^{Y_j} mod 2^{degp(x)} - 1. \tag{29}$$

And on receiving $Y_{j+1} < s^{degp(x)} - 1$ query, center gets the response:

$$E_{j+1} = K^{pub} T_j^{Y_{j+1}} mod 2^{degp(x)} - 1. \tag{30}$$

Then the center gets the equation, where $q = 2^{degp(x)} - 1$.

$$W = \left| \left(\frac{(E_{j+1})^{Y_j}}{(E_j)^{Y_{j+1}}} \right)^{(Y_j - Y_{j+1})^{-1}} \right|^{+}_{q} = \left| \left(\frac{(K^{pub} T_j^{Y_{j+1}})^{Y_j}}{(K^{pub} T_j^{Y_j})^{Y_{j+1}}} \right)^{(Y_j - Y_{j+1})^{-1}} \right|^{+}_{q} = K^{pub} \tag{31}$$

The calculated value of the Kpub satellite public key allows to determine the corresponding satellite and restart the session key generator.

It is obvious that the use of the developed algorithm to verify the reuse of the session key will improve the imitation resistance of the satellite communication system. Therefore, a modification of the developed protocol was carried out. As a result, it consists of the following steps.

2 Preliminary stage of the protocol

For the operation of the satellite identification system built on the basis of the authentication protocol with zero disclosure, an irreducible polynomial $p(x)$ with a large degree $degp(x)$ is chosen. The secret key

$$K^{sek} < degp(x) - 1. \tag{32}$$

To obtain the j-th session key S_j, where $j = 1, 2, ...$, a random number S that satisfies

$$S < degp(x) - 1. \tag{33}$$

In order to verify the dual use of the session key, a random number T is chosen from the equation

$$T < degp(x) - 1. \tag{34}$$

The selected parameters are stored in the satellite memory..
The working stage of the authentication protocol.
Stage 1. The transponder on the satellite board calculates the session key $S_j(x)$ and the parameter $T_j(x)$.
Stage 2. The transponder calculates the true status of the satellite

$$M_j(x) = x^{S_j} x^{K^{sek}} x^{T_j} modp(x). \tag{35}$$

Stage 3. The transponder produces noise-modified parameters using random variables $\Delta\tilde{K}_j^{sek}, \Delta\tilde{S}_j, \Delta\tilde{T}_j$.

$$\tilde{K}_j^{sek} = (K^{sek} + \Delta K^{sek}) mod 2^{degp(x)} - 1, \tag{36}$$

$$\tilde{S}_j = (S_j + \Delta S_j)) mod 2^{degp(x)} - 1, \tag{37}$$

$$\tilde{T}_j = (T_j + \Delta T_j) mod 2^{degp(x)} - 1, \tag{38}$$

Stage 4. The transponder calculates the noise-modified satellite status

$$\tilde{M}_j(x) = x^{\tilde{S}_j} x^{\tilde{K}^{sek}} x^{\tilde{T}_j} modp(x). \tag{39}$$

Authentication process.
Stage 1. The transponder chooses a question number $d_j < 2^{degp(x)-1}$, which it sends to the transponder.
Stage 2. The transponder calculates the answers to the query after receiving the number d_j:

$$r_j(1) = (\tilde{K}_j^{sek} + d_j K^{sek}) mod 2^{degp(x)} - 1, \tag{40}$$

$$r_j(2) = (\tilde{S}_j + d_j S_j) mod 2^{degp(x)} - 1, \tag{41}$$

$$r_j(3) = (\tilde{T}_j + d_j T_j) mod 2^{degp(x)} - 1, \tag{42}$$

Transponder sends $(M_j(x), \tilde{M}_j(x), r_j(1), r_j(2), r_j(3))$. to transponder.
The transponder verifies the correctness of the response:

$$B_j(x) = M_j(x)^{d_j} x^{r_j(1)} x^{r_j(2)} x^{r_j(3)} modp(x). \tag{43}$$

If the equation $B_j(x) = \tilde{M}_j(x)$ is true, then the satellite gets the friend status.

3 Results and Discussion

Consider the work of the developed authentication protocol. Let an irreducible polynomial be given:$p(x) = x^5 + x^2 + 1$. Then the parameters are chosen: $K^{sek} = 14, S = 14, T = 18$. Let us assume $j = 1$.

Step 1. The transponder calculates the session key $S_1(x)$ and $T_1(x)$, where $S_0 = S; j = 1$.

$$S_1(x) = \left| x^{(S_{1-1}+K^{sek})^{-1}} \right|^{+}_{P(x)} = \left| x^{\frac{1}{S_0+K^{sek}}} \right|^{+}_{x^5+x^2+1} = \left| x^{\frac{1}{14+14}} \right|^{+}_{x^5+x^2+1} = \left| x^{10} \right|^{+}_{x^5+x^2+1} = x^4 + 1 = 10001.$$

$$T_1(x) = \left| x^{(S_0+K^{sek}+T)^{-1}} \right|^{+}_{P(x)} = \left| x^{(14+14+18)^{-1}} \right|^{+}_{x^5+x^2+1} = \left| x^{(15)^{-1}} \right|^{+}_{x^5+x^2+1} = \left| x^{29} \right|^{+}_{x^5+x^2+1} = x^3 + 1 = 01001.$$

Step 2. The transponder calculates the true satellite status according to (8).

$$\tilde{M}_j(x) = x^{\tilde{S}_j} x^{\tilde{K}^{sek}} modp(x) = x^{17} x^{14} x^9 modx^5 + x^2 + 1 = x^4 + x^3 + x = 11010$$

Step 3. The transponder calculates the encrypted secret parameters. $\tilde{K}_1^{sek}, \tilde{S}_1, \tilde{T}_1$. If $\{\Delta\tilde{K}_1^{sek} = 4, \Delta\tilde{S}_1 = 10, \Delta\tilde{T}_1 = 2\} < 2^5 - 1$. Then,

$$\tilde{K}_1^{sek} = (K^{sek} + \Delta K_1^{sek}) mod 2^5 - 1 = 18, \qquad \tilde{S}_1 = (S_1 + \Delta S_1)) mod 2^5 - 1 = 27,$$

$$\tilde{T}_1 = (T_1 + \Delta T_1) mod 2^5 - 1 = 11.$$

Step 4. The transponder calculates the encrypted status of the satellite

$$\tilde{M}_j(x) = \left| x^{\tilde{S}_j} x^{\tilde{K}_j^{sek}} x^{\tilde{T}_j} \right|_{p(x)}^{+} = x^{27} + x^{18} + x^{11} mod x^5 + x^2 + 1 = x^{25} = x^4 + x^3 + 1 = 11001$$

4 Authentication process

Step 1. The interrogator chose a $d_1 = 11$ number and sent it to the transponder.

Step 2. The respondent, upon receiving $d_1 = 11$, calculates the answers to the question (13) - (15)

$$r_1(1) = \left| \tilde{K}_1^{sek} + d_1 K^{sek} \right|_{31}^{+} = 19, \qquad r_1(2) = \left| \tilde{S}_1 + d_1 S_1 \right|_{31}^{=} 26,$$

$$r_1(3) = \left| \tilde{T}_1 + d_1 T_1 \right|_{31}^{+} = |11 - 11 \cdot 9|_{31}^{+} = 5$$

Transponder responds to interrogator:

$$(M_1(x), \tilde{M}_1(x), r_1(1), r_1(2), r_1(3)) = (11010, 11001, 10011, 11010, 00101).$$

Satellite status is checked. Transponder calculates the following:

$$B_1(x) = \left| M_1(x)^{d_1} x^{r_1(1)} x^{r_1(2)} x^{r_1(3)} \right|_{p(x)}^{+} = \left| (x^4 + x^3 + x)^{11} x^{19} x^{26} x^5 \right|_{x^5 + x^2 + 1} = x^4 + x^3 + 1.$$

Since the $B_1(x) = \tilde{M}_1(x)$ condition is met, then the satellite is assigned the status of "friend". To evaluate the imitation resistance of the developed authentication protocol, the Matlab R2017b application software package was used. As a criterion for assessing the level of imitation resistance, the probability of a satellites omission by the identification system was chosen. The probability of missing is determined according to the equation:

$$P_{PC} = \frac{N(\iota)}{N_{max}} P_{PO}(\iota), \tag{44}$$

where $P_{PO}(\iota) = 1/2^{L_\iota}$ - probability of selecting the answer; $N(\iota)$, - the number of identification steps in the $\iota - th$ protocol; $N(max) = 60$ - the maximum number of steps in the protocol; L_ι - the number of bits in the answer to the question.

Figure 1 shows the dependence of the probability of a satellites omission by the identification system on the bit depth of the answer to the question posed.

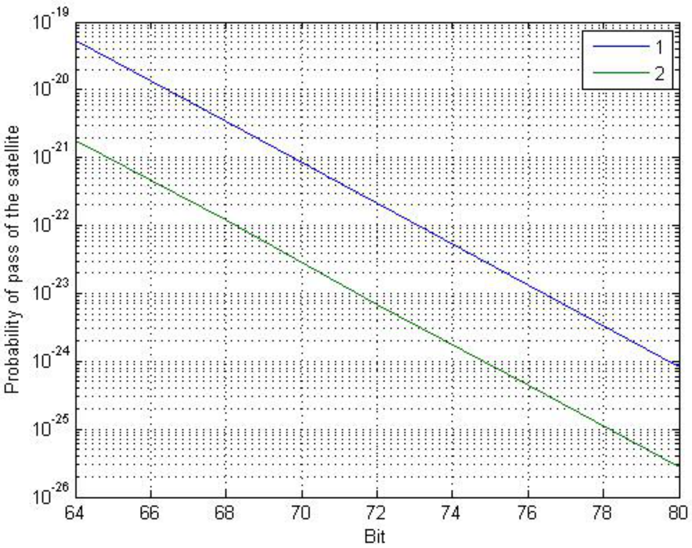

Figure 1 - Dependence of the probability of satellite omission from bit depth of the answer to the question:

1- Fiat-Shamir protocol is used;

2- the developed protocol is used.

Analysis of the graph shows that with a bit depth of L = 72 bits, the probability of a satellite passing by an identification system based on the Fiat-Shamir protocol will be $P_{PS}(1) = 2.1 \cdot 10^{-22}$. Whereas, when using the developed protocol, defined by expressions (6) - (15), the probability of a satellite passing by the identification system will be $P_{PS}(2) = 6.7 \cdot 10^{-24}$. Thus, the use of the developed protocol makes it possible to increase the imitation resistance of a satellite communication system by $3.19 \cdot 10^2$ in comparison with the Fiat-Shamir protocol.

Consider an example of applying a session key reuse check algorithm. We use the data given in the previous example. Then the public key will be equal to $K^{pub} = \left| x^{K^{sek}} \right|^{+}_{p(x)} = \left| x^{14} \right|^{+}_{x^5+x^2+1} = x^4 + x^3 + x^2 + 1 = 11101$. During the first communication session, the following parameters were obtained. $S_1(x) = x^4+1 = 10001, T_1(x) = x^3 + 1 = 01001$.

Let the satellite receive a $Y_1 = 5$ question from the OSC. Then, using expressions (18), the test parameter is $E_1 = k^{pub} T_1^{Y_1} modp(x) = \left| (x^4 + x^3 + x^2 + 1)(x^3 + 1)^5 \right|_{x^5+x^2+1} = x^4 = 10000.$.

The calculated value of E1 is transmitted to the OSC. During the second communication session,

$$T_2(x) = \left| x^{(S_1+K^{sek}+T)^{-1}} \right|^{+}_{P(x)} = \left| x^{(17+14+18)^{-1}} \right|^{+}_{x^5+x^2+1} = \left| x^{(18)^{-1}} \right|^{+}_{x^5+x^2+1} = \left| x^{19} \right|^{+}_{x^5+x^2+1} = x^2 + x = 00110.$$

In the second session the satellite received an $Y_2 = 17$ question from OSC. Then

$$E_2 = k^{pub} T_2^{Y_2} modp(x) = \left| (x^4 + x^3 + x^2 + 1)(x^2 + x)^{17} \right|_{x^3+x+1} = x^4 = 01011.$$

The calculated value of E2 is transmitted to the OSC, which checks the answers according to (21)

$$W = \left| \left(\frac{(E_1)^{Y_2}}{(E_1)^{Y_1}} \right)^{(Y_2-Y_1)^{-1}} \right|^{+}_{p(x)} = \left| \left(\frac{(x^4)^{17}}{(x^3 + x + 1)^5} \right)^{(Y_2-Y_1)^{-1}} \right|^{+}_{x^5+x^2+1} = x^4 + x^2 + x.$$

Since the calculated value does not match the public key of the satellite, this means that the session keys change in a timely manner.

5 Conclusion

The article presents an imitation-resistant authentication protocol based on proof with zero knowledge disclosure, which allows to determine the status of a spacecraft with minimal time costs. A comparative analysis showed that with a response depth of L = 72 bits, the probability of a satellite passing by an identification system based on the Fiat-Shamir protocol will be $P_{PS}(1) = 2.1 \cdot 10^{-22}$, and using the developed protocol, the probability of a satellite passing by an identification system will be $P_{PS}(2) = 6.7 \cdot 10^{-24}$. Thus, the use of the developed protocol makes it possible to increase the simulated resistance of a satellite communication system in comparison with the Fiat-Shamir protocol.

6 Acknowledgments

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

References

[Feg03] Ferguson N., Schneier B. *Practical Cryptography.* - New York: John Wiley & Sons, 2003. - 432 p.

[Feg10] Ferguson N., Schneier B., Kohno T. *Cryptography Engineering.* New York: John Wiley & Sons, 2010. - 382 p.

[Gos15] Gostev D.V., Kalmykov M.I., Stepanova E.P., Toporkova E.V. *Customer authentication protocol based on zero-disclosure evidence for electronic systems //* Certificate of state registration of computer programs No. 2015612379, 2014

[Iri18] *Iridium Satellite Communication* https://www.iridium.com/services/iridium-certus

[Lap18] Lapina, M., Kalmykov, I., Kononova, N., Kalmikov, M. *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. - p. 147-153.

[Mcd17] McDermott, Roger N. *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic.* - Jermalavicius, Tomas, September 2017. - 48 p.

[Pas18] Pashintsev V.P., Zhuk H.A. *Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication //* International Journal Issue 15, May, pp. 958-965, of Mechanical Engineering and Technology (IJMET), 2018, Volume 9, Article ID: IJMET_09_05_106

[Poi12] Poisel R. *Antenna Systems & Electronic Warfare Applications.* - Artech House, 2012. - 1036 p.

[Shr96] Schneier B. *Applied cryptography. Second edition.* - New York: John Wiley & Sons, 1996. - 784 p.

[Sha03] Shafi Goldwasser, Shafi and Yael Kalai, 2003: On the (In) security of theFOCS 2003. - pp. 102-114. *Battlefield Combat Identification System*: http://www.globalsecurity.org/military/systems/ground/bcis.htm *cash" with inspection correction rules of the electronic e-cash number for e-commerce //* EUR Workshop Proceedings 2254, 2018. - pp. 147-153.

[Smi02] Smith R. *Authenticaton: From Passwords to Public Keys.* - New York: Addison-Wesley Publishing Company, Inc., 2002. - 352 p.

[Sta99] Stallings W.*Network and Internetwork Security: principles and practice*, Second Edition, Prentice-Hall, Inc., 1999. - 459 pp.

[Wha18] *What Is Iridium NEXT.* http://www.argo.ucsd.edu/sat_comm_AST13.pdf