Quantum technologies in the NGSO class orbits

I N Kartsan¹,²,³, V S Averyanov¹, N A Shumakova¹, A O Zhukov⁴,⁵,⁶, O A Platonov¹ and S V Efremova¹

¹Reshetnev Siberian State University of Science and Technology, 31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russia
²Sevastopol state University, University str., 33, Sevastopol, Republic of Crimea, 299053, Russia
³V.I. Vernadsky Crimean Federal University, prospekt Vernadskogo 4, Simferopol, Republic of Crimea, 295007, Russia
⁴Institute of Astronomy of the Russian Academy of Sciences, 48, street Pyatnitskaya, Moscow, 119017, Russia
⁵Shternberg State Astronomical Institute of Lomonosov Moscow State University, 13, Universitetsky pr., Moscow, 119234, Russia
⁶Russian Technological University, 78, Vernadskogo Av., Moscow, 119454, Russia

E-mail: kartsan2003@mail.ru, aozhukov@mail.ru

Abstract. The article discusses issues in the research and trial operation of satellite communications systems in the following operating modes: "satellite - earth", "earth - earth". The results of this study will serve as the fundamental basis for creating new promising technical solutions, using which it is possible to create and modernize both classical and quantum multifunctional ground-based systems and on-board radio-technical and optical communication systems.

1. Introduction

Modern domestic and world practice on the globalization of communication networks and the organization of broadband access to telematic services should be provided for communication network subscribers, depending on their privilege levels. In addition to individuals there are commercial and government organizations having its own set of confidential data including top secrets. Such messages were laid by the national leader of the Russian Federation and aimed at global digitalization within the country using domestic developments in existing and newly created communication systems. Arranging digitalization should carry a transition to new scientific knowledge, experiments and innovative discoveries in the field of information technology. One of the tasks entrusted to the research teams is active decision making for the secure transmission of data over long distances. These studies and experiments are located in the areas of quantum distribution of access keys. The integration of such systems will significantly increase the overall level of functionality of the equipment of its imitation resistance by introducing new integrated solutions based on the quantum laws of physics, optics and mechanics. Depending on the class of tasks to be solved, such complexes can contain from hundreds to several thousand active modules (AM) participating in the processes of pairing, transmission and processing of critical important data circulating in an automated information system (AIS). The
The introduction of quantum systems will allow the creation of centers for the processing and storage of information obtained as a result of quantum and classical calculations. However, it should be noted that the probability of attacks on information systems built on the model of the quantum distribution of encryption keys, where compared with the application of classical approaches to concealing data, is reduced, and the risks of losing information of a commercial purpose and state level are completely reduced to zero.

Quantum key distribution (QKD) is based on the fundamental phenomena of quantum mechanics, the physics of processes, and quantum optics. This distribution of encryption keys uses separate light quanta in quantum super positions, with the goal of unconditional data protection between network subscribers.

As world practice shows, at present, the achievable distance for the QKD is limited to several hundred kilometers via land lines, which is due to the huge amount of interference imposed on communication channels from the outside, including software and hardware vulnerabilities and the undeclared capabilities of such quantum systems. At the same time, cryptanalysts use a fairly serious set of programs for the penetration test of network from Kali Linux. These are just a few of the dozens of reasons for the emergence of new, modern and high-tech experiments on nanosafe data transmission taking place around the world, including Russia. So, for example, a few years ago the first land-based quantum optical communication line appeared in the country, which connected the two buildings of ITMO University in St. Petersburg. In 2016 scientists from the Kazan Quantum Center KNITU-KAI and ITMO University launched the country’s first multi-node quantum network, achieving a generation rate of sifted quantum sequences of 117 kbit/s on a 2.5-kilometer communication line. Commercial communication lines have been created and exist - the Russian Quantum Center connected Gazprombank’s offices at a distance of about 30.6 kilometers, but the transmission range is still limited due to losses in fiber-optic communication channels. Similar losses exist when transmitting signals in free space between a satellite located in a certain class of the orbit and the equipment of the command and measuring station on the ground, with this, an exponential decrease in the speed of photons with respect to the transmission distance of the signal and, as a result, partial or complete loss of the communication channel. In this case, one of the important points is the class of corner reflectors placed on the spacecraft, as well as the material for their manufacture. During the experiments, it was found that when photons are transmitted to a spacecraft, in which the reflector is metalized, the percentage of losses of the returned signals is ten times smaller. Satellite QKD and the creation of a computer, the architecture of which postulates of quantum technologies are laid down, will make it possible in the next decade to create completely new classes of distributed networks that are part of global quantum networks, the operational features of which will be guided by the minimum photon loss in the communication channel during active connections [1-2, 9].

The analysis of characteristics, the economic effect and commercialization of such projects, opens up significant prospects for the use of new generation communications in such areas as the country’s defense, modernization of early warning and space monitoring systems, banking, medicine, and the provision of telematic services by satellite providers for citizens and organizations in the territory RF in all of the above industries, data security and the legitimacy of encryption keys is one of the primary tasks. The introduction of such systems of high-precision and cryptographic data transmission based on the QKD is a key milestone for the globalization of quantum networks of the 21st century.

In this regard, the aim of the study is the phased development and subsequent testing of the results of a mathematical analysis of the probability of vulnerabilities using classical encryption methods for a small spacecraft in orbits of the NGSO class. An essential argument for the implementation of the QKD will be the pentest of such a communication channel for identifying vulnerabilities and “thin” places of the system during the trial operation of both civilian and military communication satellites at high data rates, generation and transmission of data packets to the ground station in satellite-to-ground modes protected by encryption keys. To achieve this goal, it is necessary to determine the set of tools from the QKD and the possibility of introducing into existing systems using classic encryption keys in landlines when transmitting via optical fiber.
2. Classical encryption and satellite QKD methods

State, private and safe communications in the digital age are integral needs of a person, society and one of the foundations of the dynamic state development as a whole. Classical traditional public-key cryptosystems are based on the inability of computational processes; a set of mathematical functions is the main difficulty here. However, powerful quantum computers, scientists around the world are working at will be considered as a real threat, since its introduction could lead to the crack of any existing cryptosystems based on symmetric encryption. The quantum method is a radically new way of implementing a secure connection by exchanging quantum encryption keys. QKD allows two remote to a limited distance users prior not using a long secret key during data exchange to create a common random string of secret bits called a secret key and use one-time encryption for each data packet. In such cases, the key will be protected by symmetric encryption, a common key for encrypting and decrypting the message, which can be transmitted both through the classical satellite communication channel and through the quantum communication channel. One of the most popular classical symmetric block encryption or conversion algorithms is National standard 28147-89, AES (Advanced Encryption Standard), also known as Rijndael and DES (Data Encryption Standard). A comparative analysis of these encryption algorithms is given in table 1.

Table 1. Classic encryption algorithms specification.

| Parameters       | DES   | AES          | GOST 28147-89 |
|------------------|-------|--------------|----------------|
| Development date | 1977  | 1999         | 1989           |
| Key length       | 56 bit| 128, 192 or 256 bit | 256 bit |
| Cipher type      | Symmetric Block | Symmetric Block | Symmetric Block |
| Block size       | 64 bit| 128 bit      | 64 bit         |
| Security         | Not safe enough | Safe           | Not safe enough |

In quantum theory information is encoded in superposition states of physical information carriers in the form of photons at the mono-quantum level. Photons are stable elementary particles moving with the speed of light in space. Such particles have their own distinctive features from ordinary particles in the form of energy that they possess:

\[ E = h\omega,\ E = hv. \]  
\[ E = \frac{p^2}{2m}c^2 \]  
\[ p = \frac{h}{\lambda} \]  
\[ \rho = \frac{h\omega}{c} = \frac{zmh}{\lambda}, \rho = \frac{hv}{c} = \frac{h}{\lambda} \]  

According to the theory of relativity, each particle with energy E has a mass:

But the photon does not have a rest mass and can exist only in motion while having its own momentum as a particle of light:

Therefore, its momentum will be equal to:

Based on the basic characteristics of a photon one can conclude that the corpuscular properties of light. The higher its frequency \( v \) the higher its energy \( E \) is and accordingly its momentum \( \rho \). At the same time, the photon is resistant to internal decoherence, which allows us to conclude that the control system based on photo effects and the correct perception by users at all levels of its implementation is easy to control.
One of the most common methods for transmitting quantum encryption keys is the direct sending of single photons through optical fibers or by a signal of a certain frequency to the free near-Earth space. Existing losses in the communication channels will reflect exponential deviations from the specified standard calculations.

A distinctive feature of classical telecommunication capabilities, a quantum signal in QKD cannot be amplified noiselessly due to the application of the quantum non-cloning theorem. When using QKD, it should be taken into account that the greatest losses of information photons in communication channels can occur under the influence of turbulent air flows in the lower atmosphere at altitudes of up to 10 km, while the remaining part of the route to the spacecraft is in a vacuum with practically zero absorption of the medium and decoherence of wave propagation. Therefore, a valuation technique is needed, conducting feasibility studies at the design and development stages of new ground-based communication systems with spacecraft, creating processing and storage centers for data obtained as a result of quantum-classical transformations. In this regard, the operation of the experimental systems of the designed complex must initially establish the principle of the bidirectional distribution of entangled photon pairs using a two-link ground-based communication channel in free space. There is a need for a more detailed study, the development of methods for testing quantum communications on moving platforms in data transfer modes with high photon losses. Carrying out such a type of experiments carries great practical significance, primarily because the results of the experiments will serve as a prototype of the product for subsequent integration into existing communication systems. Such studies and their subsequent practical application will make it possible to modernize and provide new ties both in civil society and for weapons, which will positively affect the country's defense and its economic development.

In addition, there is a certain probability of the presence of an attacker, cryptanalyst or quantum hacker both in the classical implementation of encrypted communication channels and in the implementation of quantum methods. In any of the above scenarios, the goal of third parties in the procedure for conducting a pentest of satellite communications systems is to collect information about the system, its border crypto routers, features of flexible local settings and practical application of IPS/IDPS security systems, as a result, development of algorithms, methods, choice and the creation of software products to implement attacks on the security system. In addition to the remote pentest, it is possible to use the method of social engineering to identify relevant data on the existing settings of the IPS/IDPS security systems, as a result, development of algorithms, methods, choice and the creation of software products to implement attacks on the security system. In addition to the remote pentest, it is possible to use the method of social engineering to identify relevant data on the existing settings of the organization’s protection system. In this regard, persons servicing channel-forming equipment, including remote administrators of protection systems, should always be ready for such manifestations on the part of intruders [6-8, 10].

3. Estimation of the probability of the presence of an attacker in classical systems

Consider a mathematical method for detecting an attacker using classical encryption. Let m land complexes be given which are allocated certain frequency ranges for transmitting encryption keys of a communication channel $\Delta K$, sources and receivers of data packets are connected to $S$ nodes of ground stations, where $S \leq m$. Each of the sources connected to the system generates keys for $j$ transceiver modules located both on the spacecraft $j_s$ of the NGSO orbits and on the ground $j_n$, in this case $j_n \leq m$.

The task is to determine several probabilities: pentest, access and, as a result, compromise of access keys of a satellite communication channel, determination and optimal distribution of data packets with keys, as well as their disguise in case of intrusion into a communication channel of third parties. As criteria for the system, traffic minimization by the ratio of received and transmitted packets with data containing critical information is necessary. Each of the ground $S$ nodes involved in the system and located in the coverage area of the spacecraft has bi-directional communication channels for the reception/transmission of discrete signals $\Delta K$, including transceiver modules in the $j_s$ satellite. Then, as a result of decomposition, we have m ground stations and $j_n$ modules having a physical connection to $S$ ground nodes. Critical information in this case will be distributed over a finite number $- N(N \leq S)$ of nodal elements of stations $m$. 


With this approach, for an attacker to perform illegal actions with respect to encryption keys, he needs access to $j_n$ or $j_s$ modules, or data packets with critical information circulating between these modules. Denote it as $i$. As a result of the satellite channel pentest for vulnerabilities, an attacker can gain access to all the information contained in the nodal elements of the ground station and the spacecraft. In this case $i = 1, N$.

We introduce the following arguments:
- $P_{\text{test}}(i)$ – the probability of a pentest by imposing a discrete signal $\Delta K$;
- $P_{\text{acc}}(i)$ – the probability of access to modules $j_i$ ($i = 1, N$);
- $P_{\text{com}}(i)$ – the probability of compromise of access keys and disclosure of confidential information contained in $S$ nodes of stations $m$.

Moreover, we assume that access to modules $j_i$ containing information $i$ ($i = 1, N$), is independent of the likelihood of compromising access keys $P_{\text{com}}(i)$, and $P_{\text{acc}}(i)$ is independent of $P_{\text{test}}(i)$. In this connection, the effective probability of unauthorized access to the satellite system according to the rule of probability is as follows:

$$P_{\text{res}} = P_{\text{test}}(S) \times P_{\text{acc}}(S) \times P_{\text{com}}(S). \quad (5)$$

As can be seen from the expression for determining the effective probability of capturing root rights of a satellite communication channel $P_{\text{res}}$ it is necessary to determine the probabilities of testing communication channels $P_{\text{test}}$ in order to gain access to the modules included in the automated information system with its channel-forming equipment $P_{\text{acc}}$ and, as a result, the probability of compromising access keys to the system $P_{\text{com}}$.

When determining the probability $P_{\text{test}}$, one should take into account such a factor as the imitability of the communication channel and access keys to the system. To assess the level of imitation resistance $I_{\text{st}}$, it is necessary to take into account the dimension of the space of signals $K$ transmitted per unit time $\Delta t$, as well as the number of attempts of the pentest $w$ and possible $q$ scenarios. Then, in general, imitation resistance can be represented as:

$$I_{\text{st}} = \frac{\Delta K \times w \times q}{\Delta t}. \quad (6)$$

The relationship of imitostability and probability of the pentest is:

$$P_{\text{test}} = 1 - I_{\text{st}}. \quad (7)$$

In practice, the simulated resistance of discrete signals is achieved by using signals having a complex internal structure with a specific set of frequencies and presentation forms, including taking into account unmasking signals with similar noise signals in their properties. In this case, the probability of a successful pentest by imposing a side signal will be:

$$P_{\text{test}} = \frac{1}{\Delta K}. \quad (8)$$

For signals without returning:

$$P_{\text{test}} = 1 - \frac{w \times q}{\Delta K}, 1 \leq w \leq \Delta K, \quad (9)$$

where $w$ is the number of attempts to impose a secondary discrete signal, $\Delta K$ is the dimension of the space of all kinds of signals.

To determine the probability of access to modules containing confidential information $P_{\text{acc}}$ by consolidating the results of a pentest to identify existing vulnerabilities and weaknesses of security systems, one can also determine the probability of a possible compromise of access keys to satellite communication systems.

Taking into account that the information is distributed between the transceiver modules of the spacecraft $j_s$ and the ground modules $j_n$, as well as the information flow $i$ circulating between them per
unit time $\Delta t$, where $1 \leq i \leq N$ and denoting $P_{\text{acc}}^i$ as the probability of access to the information stream, the effective probability of access to the system modules will be expressed as:

$$P_{\text{acc}} = \prod_{i=1}^{N} \left\{ (1 - P_{\text{acc}}^i) \times (1 - P_{\text{test}}^i) \times (1 - \delta^i) + P_{\text{acc}}^i \times P_{\text{test}}^i \times \delta^i \right\},$$  \hspace{1cm} (10)

where $\delta^i$ is a binary indicator equal to 1 if the signal is with return and equal to 0 without return, respectively, the attacker does not have the ability to collect information through a pentest with special software from under Kali Linux. So in this expression, the first part $(1 - P_{\text{acc}}^i) \times (1 - P_{\text{test}}^i) \times (1 - \delta^i)$ determines the imitation resistance of the protection system in the complex by imposing side signals, and the second term $P_{\text{acc}}^i \times P_{\text{test}}^i \times \delta^i$ allows to determine the probability of bypassing the protection system and the successful implementation of one of the possible attack scenarios on the AIS [3-7, 11].

4. Conclusion

Based on the data obtained by the methods of mathematical analysis, one can easily reveal existing vulnerabilities in satellite communication systems, in a controlled manner, without disrupting their operation, and simulate external influences in one or more attacking scenarios. The result of such actions will be remote hacking of systems, interception of its root rights and theft of critical data. To ensure its security, the attacker will use fake proxies, baits with access to the global Internet and a wide range of modern hardware and software products.

Thus the use of quantum distribution systems of encryption keys can eliminate the existing problem areas and vulnerabilities of data transmission systems that arise during operation. When using quantum systems, an attacker will inevitably create interference in the existing communication channel and will be detected with 100% probability by interacting users in automatic or manual control modes. When using the classical approach for distributing encryption keys to detect an attacking link, a daily scheduled procedure for checking channel-forming equipment, a systematic in-depth analysis of system event logs, user logs, recent system change logs and other administrative procedures used in the operation of channel-forming cryptographic equipment, including recommended ones, are required regulators in the field of information security.

Acknowledgements

Project № 2686.2020.8 "Models, methods and means for obtaining and processing information about space objects in a wide spectral range of electromagnetic waves".

References

[1] Kartsan I N and Averyanov V S 2019 South Siberian Scientific Bulletin 4 (28) 264–8
[2] Kartsan I N, Malanina Y N, Zhukov A O, Tsarev R Y and Efremova S V 2019 IOP Conference Series: Materials Science and Engineering 537 (2) 022029
[3] Korn G, Korn T 1977 Math reference book for scientists and engineers (Moscow: Nauka) p 752
[4] Feller V 1964 Introduction to Probability Theory and Its Applications (Moscow: Mir) p 484
[5] Bahvalov N S, Zhidkov N P, Kobel’kov G M 1987 Numerical methods (Moscow: Nauka) p 630
[6] Khartman K, Letskiy E, Shefer V 1977 Planning an experiment in the study of technological processes (Moscow: Mir) p 125
[7] Rosenko A P 2012 Scientific reports of Tomsk State University of Control Systems and Radioelectronics vol 1(25) (Tomsk: TUSUR) pp 25-28
[8] Semenenko M G, Kniazeva I V, Beckel L S, Rutskiy V N, Tsarev R Y, Yamskikh T N and Kartsan I N 2019 IOP Conference Series: Materials Science and Engineering 537 (3) 032095
[9] Chebotarev V E, Brezitskaya V V, Kovalev I V, Kartsan I N, Malanina Y N and Shemyakov A O 2018 IOP Conference Series: Materials Science and Engineering 450 (2) 022029
[10] Kartsan I N, Goncharov A E, Zelenkov P V, Kovalev I V, Tyapkin V N and Dmitriev D D 2016
IOP Conference Series: Materials Science and Engineering 155 (1) 012019

[11] Kartsan I N, Malanina Yu N, Zhukov A O, Tsarev R Y and Brezitskaya V V 2019 IOP
Conference Series: Materials Science and Engineering 537 (5) 052006