Analysis of information encryption methods in multichannel telecommunication systems

Bayram Ibrahimov[1], Ramiz Humbatov[2], Rufat Ibrahimov[3]

[1]Azerbaijan Technical University, Baku, Azerbaijan

[2,3]Institute of Control Systems NASA, Baku, Azerbaijan

[1]i.bayram@mail.ru

Abstract — **An analytical review of works devoted to the issues of transmission and cryptographic information in multi-channel telecommunication systems is presented. The methods of improving the cryptographic protection of messages from unauthorized access to communication channels during the transmission of information of a mixed type of traffic are analyzed. A new approach to the protection of information from unauthorized access in multichannel telecommunication systems, taking into account the peculiarities of the cryptographic method of encrypting and encoding transmitted messages via communication channels, is proposed.**

Keywords — *information security, cryptography, encryption, unauthorized access, cryptographic protection*

I. INTRODUCTION

Intensive development of multichannel telecommunication systems (MTS) using the architectural concept of NGN/IMS (Next Generation Network & Internet Protocol Multimedia Subsystem) requires a new approach to effectively protect information, which is based on modern cryptography methods [1].

Effective information protection in the era of the information space for achieving the goals of the digital economy is one of the main prerequisites for the development of modern information and telecommunication technologies. Therefore, the issues of information security in telecommunication systems are becoming increasingly relevant with the development of information and network technologies [2].

It is known [3, 4] that for many years in all countries of the world information protection was the prerogative of the state, and a state monopoly was established on the development and use information protectıon technologies. Informatıon security tools and algorithms were mainly used in military, government and diplomatic communication under tight government control. In these conditions, the development of the science of information security - cryptology.

Based on the system-technical analysis, it was established in [2, 5, 6] that cryptology dialectically unites two sciences:

1. Cryptography - a new science that studies methods protecting information from unauthorized access;
2. Cryptanalysis is the science methods of unauthorized access to protected information.

Consequently, the development banking technologies, the activities of commercial structures, election campaigns of competing political parties, inventive and other activities that require the protection of information. The latter determined the current demand for cryptographic technologies and cryptology specialists in the country [6].

In view of the above, an important question arises - the study of the description of the most frequently used algorithms, methods and protocols for cryptographic protection of information and the features of their use in telecommunications engineering.

In this paper, the solution of the above formulated problem is considered - the creation of a new approach to information security, which allows analyzing the methods transmitting and encrypting information in multichannel telecommunication systems.

II. GENERAL FORMULATION OF THE PROBLEM

The problem of the quality of transmission and protection of information in the telecommunications system is investigated with a certain model of message transfer and with a certain scenario of the attacker's actions.

In order to analyze and review the protection of information, a new approach is proposed that takes into account the algorithms of coherent network coding, when certain linear operations are performed on incoming messages and the attacker's script on the network nodes

In the attacker's scenario, there are subsets MTS communication available to the attacker, that is, he can eavesdrop on or record the information transmitted through them with the intention of identifying source messages.

This problem was first considered in [6, 7] by the team of authors in the first fundamental work on network coding.

DOI: 10.25045/NCInfoSec.2018.03

In MTS, when transmitting information in open communication channels (CC), cryptographic methods for protecting information from unauthorized access to subscriber lines are widely used, as is the encryption method and the encryption method.

To achieve this goal, a new approach to cryptographic protection information from unauthorized access to MTS is proposed, taking into account the peculiarities of the cryptographic method of encrypting and encoding transmitted messages via communication channels.

III. ANALYSIS OF THE NEW APPROACH TO PROTECTING INFORMATION FROM UNAUTHORIZED ACCESS

In order to analyze the methods of transferring and encrypting information, consider the description of the most frequently used algorithm and protocols, sufficient for the implementation of existing cryptosystems.

To create a new approach, figure 1 presents a structural diagram that describes functionally the process of cryptographic protectıon of information from unauthorized access to the MTS.

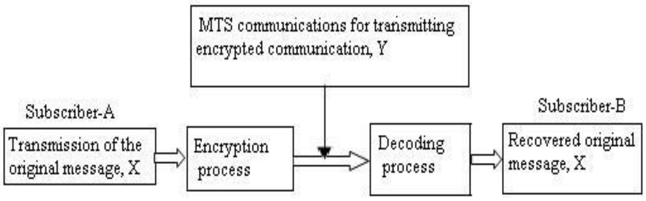
MTS communications for transmitting encrypted communication, Y
Subscriber-A
Subscriber-B
Transmission of the original message, X
Encryption process
Decoding process
Recovered original message, X

Fig.1. Structural and functional scheme of protecting information from unauthorized access

From figure 1 it follows that the system for protecting information from unauthorized access consists of two important system functional blocks — the system for transmitting and encrypting the original messages and the reverse. In a generalized form, the task of protecting information from unauthorized access based on Fig. 1 can be formulated as follows.

Subscriber-A, being the source and initiator of message X, intends to transmit this message to subscriber-B, called the recipient of the message, while subscriber-A wants to be sure that in the process of transmitting the message no one can read it, that is, reveal the content, modify, or create another similar message and transmit it to the subscriber-B on behalf of the subscriber-A.

In turn, the subscriber-B, having received the message, wants to be sure that it is possible to establish and prove its receipt from subscriber A at any time, as well as the fact that this message is not a repeat of the earlier one.

In this case, the transmitted message is information of a mixed type of traffic (information file, speech, documentary message, etc.). In a schema, X a message is usually called a source or open message or text.

The message X may be, for example, a digitized speech of a telephone conversation, a text or other information file, a facsimile message, and other types information subject to protection from unauthorized access.

To protect the message X from unauthorized access, some transformation of the original message, called the encryption process, is applied.

This transformation involves the comparison of the original message X of a certain function $E(X)$ that turns it into an unreadable without special means encrypted message Y :

$$Y = E(X), \qquad X \in (x_1, x_2, ..., x_i) \ , \qquad (1)$$

However, the encrypted message Y is usually related to the original X structure, i.e. message length Y is usually equal to or greater than the length of the message X :

$$L_{\partial c}(Y) \geq L_{\partial c}(X) \qquad (2)$$

It should be noted that in some cases the encryption process uses information compression in message X, in order to reduce message Y redundancy, while the message X may be shorter than the message, but this is not a consequence of encryption as such.

From fig. 1, expressions (1) and (2), it follows that the studied approach of cryptographic protection of information takes into account also two types of unauthorized access:
1) to the communication channel;
2) to the information transmitted over the communication channel.

At the output of the communication channel, to recover the original message X from the encrypted message Y , a decryption operation is used using the D (Y) function:

$$X = D[E(X)] \Rightarrow D(Y) = X \qquad (3)$$

Expression (3) characterizes a set of algorithms for encryption and decryption processes, which is the algorithm for encrypting information as a whole.

IV. RESEARCH AND CALCULATION PARAMETERS CRYPTOGRAPHIC METHODS FOR PROTECTING INFORMATION IN THE MTS

It is known [4, 6, 8] that the main modern cryptographic methods for protecting messages are encryption methods (replacement, rearrangement, analytical transformation, gamming and combined) and encoding methods (meaning and symbolic). Here, the encryption method refers to the process in which each plaintext character is subjected to cryptographic transformation. In this method, the cipher always distinguishes between two elements: an algorithm and a key.

In the scheme of figure 1, it follows that the algorithm that implements the encryption function $E(X)$ is called the encryption algorithm. Accordingly, the decryption algorithm is the algorithm that implements the functions $D(Y)$. The combination of encryption and decryption algorithms will be called the cryptographic algorithm of the telecommunications system.

The persistence of these algorithms is based on the computational complexity of solving some problems. If the protection of information using some kind encryption algorithm is provided by secrecy, i.e. the inaccessibility of the structure of the algorithm itself, such an algorithm is called limited. Limited algorithms cannot be exploited by a wide range of users, since leakage of information about the structure of the algorithm leads to irreversible loss of secrecy for all users at once, depriving the entire protection system of meaning [4, 7].

The algorithm for encryption methods allows the use of a relatively short key for encrypting arbitrarily large text are considered. To protect messages in multichannel telecommunication systems, the cipher method is mainly used.

In the system of transmission and protection of information (fig. 1), the key used is usually external to the encryption and decryption algorithms information that determines the specific type of encrypted message Y for a given initial message X .

Based on the new approach, the general formula for using the encryption methods for the i-*i*-th alphabet character is expressed as follows:

$$Y_i = k_1 x_i + k_2 (\bmod n) \quad , \tag{4}$$

where k_i and $k_2 -$ are constants; $x_i -$ *i*-th plain text character, i.e. letter number in alphabet; $n-$ alphabet length.

Expression (4) defines a widely used replacement method in cryptography. When replacing each letter of the plaintext alphabet, one letter is assigned to the cipher of the text from the same alphabet.

Based on the research, it was established in [1, 6] that the approach to information security in multichannel telecommunication systems from unauthorized access should provide:

- confidentiality - information should be protected from unauthorized reading both during storage and when sending a message to the MTS;
- access control - information should be available only for the person for whom it is intended;
- authentication - the ability to uniquely confirm the authenticity of the information and identify the sender in the multichannel telecommunication systems;
- integrity - the information should be protected from unauthorized modification during storage and transfer to the MTS;
- non-repudiation - the sender cannot refuse the fact sending this message to MTS

Taking into account the peculiarities of the new approach, cryptographic information protection is described by the following formula:

$$Y_i(x_i, k_i) = x_i + k_i (\bmod n), \tag{5}$$

where $k_i -$ *i*-th letter of the key, which is used as a word or phrase.

Based on the method being studied and the information encryption algorithm, it is possible to check the adequacy using any plaintext.

Thus, on the basis of the proposed approach to information security, the transmitted message via communication channels is conditionally divided into two mutual sequences with the help of which perfect secrecy is ensured - the statistical independence of the transmitted message X from the original message from M .

V. ANALYSIS OF INFORMATION SECURITY IN MTS USING CRYPTOGRAPHIC CODING METHODS

One of the important cryptographic methods and information security algorithms in MTS is the network coding method. Coding is the process of transforming messages in a combination discrete signals, i.e. the process of replacing plain text elements (symbols, combination of codes and words) with codes. In this paper [7, 8], the authors consider uncast transmission on the network and apply random network coding based on correction codes, $N_k(n)$.

Considering the above algorithms, the essence of the proposed approach is that when a message is transmitted, the network coding design consists of several operations:

- Selection of suitable elements and code parameter

$$N_k(n) = G(n, m, d, r),$$

where r, $m-$ number of check and information symbols in code combinations; $n-$ total length of code combination; $d-$ code distance.

- Analysis and selection of a sequence of network coding symbols over a field.

$$Q_{ck}(n, q, r) = GF^{(n-r)}(q, m), \quad m = (n-r) \in M \ , \tag{6}$$

Taking into account the parameters, the design of the network code for the transmitted message is described as follows:

$$X = D[E(X)] = N_k(n) + GF^{(n-r)}(q, m), \tag{7}$$

From (7) it follows that the source generates a message m from a common set M , which is a sequence of characters over a field $GF^{(n-r)}(q, m)$ and consists of two terms. The source also generates a session key from the set.

Thus, approaches to building an information security system based on cryptographic coding methods should consider each of the structural elements of the communication channels in the MTS.

Further, it is still necessary to solve one of the important tasks arising from the combination of several terminal devices of communication channels and the creation of a telecommunications network.

VI. CONCLUSIONS

As a result of the research, a new approach to cryptographic information protection in MTS from unauthorized access was proposed, taking into account efficient encoding and encryption methods.

In this method of transferring information of a mixed type of traffic, there are quite a few interesting options for ensuring anonymity depending on the choice of the network code design.

REFERENCES

[1] Korzhik, V.I. Basics of Cryptography. - SPb. : IC Intermedia, 2016. – 296 p.

[2] Ibrahimov B.G., Ismaylova S.R. The Effectiveness NGN/IMS Networks in the Establishment of a Multimedia Session // American Journal of Networks and Communications. Vol. 7, №. 1, 2018. – pp.1-5.

[3] Peeters, E. Advanced DPA Theory and Practice: Towards the Security Limits of Secure Embedded Circuits / E. Peeters. New York : Springer-Verlag New York, 2013. – 139 p.

[4] Shafali Agarwal. Image Encryption Techniques Using Fractal Function: A Review// International Journal of Computer Science &Information Technology. Vol 9, No 2, 2017. – pp.53-68.

[5] Cai N., Yeung R.W. Secure Network Coding on a Wiretap Network//IEEE Trans. On Information Theory. - 2011. V. 57, N 1. – pp. 424– 435.

[6] Ibrahimov B.G. Cryptographic Methods and Means Protection Transmitted Information in Telecommunication Systems// The Proceedings 18-th – IFAC Conference on Technology, Culture and International Stability.IEEE Xplore, № 43613. Sept.13 - 15, 2018. – pp.224-227.

[7] Gabidulin E.M., Pilipchuk N.I. Error and Erasure correctingalgorithms for Rank Codes //Designs, Codes and Cryptography. 2008. - V. 49, N 1–3. - pp. 105–122.

[8] Zhang S., Yeung R.W. A General Security Condition for Multi-Source Linear Network Coding // Proc. 2009 IEEE Int. Sympos. On Information Theory (ISIT’2009), Korea. - pp. 1155–1158.