Adadurov S.E., Maltsev G.N., Adadurov A.S.

ACCURACY OF VITAL MESSAGES TRANSMISSIOM USING THRESHOLD FRAGMENTATION METHODS AND ANTINOISE CODING

The paper studied the accuracy of transmission of vital messages for railway signalling and train controls systems using threshold fragmentation methods and antinoise coding. A scheme for the implementation of the transmission method of formalized messages with allocation of outer coding (generation of messages based on the principle of secret sharing) and internal coding (antinoise coding of fragments) is presented. The dependences of the probabilities of missing messages and receipt of a false report from the parameters of the fragmentation threshold scheme and antinoise coding with error detection and their correction are analyzed. It is shown that by changing the relation between the parameters of the external and internal encoding we can affect the relationship between the probability of missing a message and receiving a false report in accordance with the requirements made for the transmission of vital messages.

Keywords: *vital messages, threshold fragmentation method, antinoise coding, the probability of undetected errors, protection against unauthorized access.*

Introduction

Under present-day conditions, transportation process management is provided by advanced telecommunications infrastructure of centralized traffic control (CTC) centers with stationary and mobile users [1]. In rail transport, these functions are performed by automatic train control and train protection systems (ATC/ATP). Communication facilities used in ATC/ATP systems feature strict requirements for the accuracy of transmission of the so-called vital messages, i.e. command and control messages that are directly related to the management of railway automation and train safety.

Vital messages include commands for control of train movement and line blocking, operation of switch sections, crossings and signal lights as well as formalized messages of rolling stock dispatcher control. When we specify the requirements for the accuracy of transmission of vital messages, along with the generally accepted indicator, i.e. the total probability of erroneous reception of messages, in some cases we take into account the values of its individual components, in particular the probability of missing a vital message and receiving a false message. And the required values of these probabilities (10^{-8}-10^{-10} and lower) correspond to the so-called quasi-error-free transmission [2]. An additional requirement is the protection against unauthorized access to railway signaling control and simulation of false messages [3].

Implementation of the requirements mentioned in the radio communication systems currently constituting the base of ATC/ATP systems is complicated by interference in radio channels of communication and their electromagnetic availability. This leads to the need to develop methods of vital messages transmission which both ensure the high accuracy of data transmission via radio channels with interference (noise immunity) and the protection against unauthorized access to messages (information security). In this paper we consider one such method based on the combined use of fragmentation threshold schemes and antinoise coding.

1. Description of the method of fragmented transmission of messages using threshold fragmentation schemes and antinoise coding

The considered method of fragmented message transmission is a combination of fragmentation threshold schemes and antinoise coding with error detection or error correction, and it can increase the accuracy of message transmission via train control radio channels with noise as well as the protection against unauthorized access. In this case, the information security is insured by transformation of the original message in the process of fragmentation. The transmission of the excess number of fragments, which allows to recover the transmitted message using only some of them, provides the increase of the accuracy of message transmission in case of the erroneous reception of individual fragments, and the overall probability of erroneous reception of a message and its components depends on the antinoise channel coding of fragments and the parameters of a fragmentation scheme, according to which the message is restored on the basis of the received fragments.

The schemes of threshold fragmentation used to divide a transmitted message into fragments are a type of cryptographic secret sharing schemes [4]. The main function of secret sharing schemes in cryptography is a distributed management of confidence or joint control over the vital actions of users, which is carried out on the principle of participation (consent) of at least V users out of their total number W ($V < W$). The scheme of secret sharing between W users is called a scheme of threshold fragmentation (V, W), if any group of V users can recover the secret according to available fragments (parts of a secret), while no group of a smaller number of users can get any information about the secret.

Generally, the threshold fragmentation scheme (V, W) formally is specified by a set of five users of the type $< \mathrm{X}_W, \Gamma(V), a_0, F, G >$ and includes the following components:

1. The set of scheme participants or subscribers $\mathrm{X}_W = \{x_1, x_2, ..., x_W\}$.

2. The set of subscribers $\mathrm{Y}_Q = \{x_1, x_2, ..., x_Q\}$, forming the access structure

$$\Gamma(V) : [\mathrm{Y}_Q = \{x_1, x_2, ..., x_Q\} \big| (x_i \in \mathrm{X}_W), (x_i \neq x_j, i \neq j),\ i = 1, 2, ..., Q,$$
$$j = 1, 2, ..., Q,\ V \leq Q \leq W].$$

3. The value of the secret a_0, which is to be shared among all the members of the scheme.

4. The transformation of secret sharing F allowing to calculate the fragments (secret shares) b_i, i=1,2,…,W, which is received by the participants of the scheme in the process of sharing the secret a_0. In this case $b_i=F(z_i,a_0)$, where z_i is a characteristic number of the i-th subscriber correlated to him during the process of secret sharing.

5. The transformation of secret recovery G, which allows any set of the participants $Y_Q = (x_1, x_2, ..., x_Q) \in \Gamma(V)$ forming the structure of access to unambiguously recover the original secret value a_0. In this case $a_0 = G(b_1, b_2, ..., b_Q, z_1, z_2, ..., z_Q)$.

If in cryptography the fragmentation of information is used to restrict access to this information, for transmission of messages via communication links, threshold fragmentation provides higher reliability and accuracy of message transmission. The fragmentation of a transmitted message (secret analog S_0) is performed so that it can be restored by combining a predetermined number of fragments. A threshold fragmentation scheme (V, W) means that each message is transmitted in the form of W fragments, and to sort it out in a proper way when receiving you should have at least V ($V < W$) fragments. It is assumed that we use such an algorithm for the formation of W message fragments that when combining all V or more undistorted fragments we can uniquely reconstruct the transmitted message, whereas the combination of less than V of any undistorted fragments do not give any information about the transmitted message. Such secret sharing schemes with the possibility of their unique reconstruction are called perfect, and we know the conditions and the evidence of their existence in particular cases and for the general description (arbitrary access structures) of a threshold fragmentation scheme (V, W) [4].

It should be noted that in the above formal definition, the schemes of secret sharing, the transformation of secret sharing F and the recovery of secret G are unambiguously interrelated, but not symmetrical. The structure of access $\Gamma(V)$ as well as perfection, and other properties implemented by the "secret sharing" scheme, including information secrecy, depend on these transformations (conversions). If fragmented transmission is designed to prevent unauthorized access to transmitted messages, then the algorithm for the generation of transmitted message fragments must be unknown to an intruder.

Antinoise coding is used in this method of fragmented message transmission in the traditional form [5] of channel coding fragments. Fragments of a transmitted message generated using threshold fragmentation schemes are encoded by block noise-resistant codes with error detection or error correction and transmitted over the link. There may be used any (n, k)-codes, which parameters (n is the total number of characters, k is the number of data symbols of a block code) are selected based on the known boundary conditions defining the relationship between these parameters and the multiplicity of detected q_o, or corrected errors q_u. The property of perfect threshold fragmentation is the condition imposed on the number of digits k_1 of the generated fragments of a transmitted message (secret). It can not be less than the number of digits of the original message k_0: $k_1 \geq k_0$, due to the complexity of transformations of secret sharing algorithms that enable to restore (select when receiving) a transmitted message by a smaller number fragments than it was transmitted [4].

The scheme of implementation of the method of message transmission using a threshold fragmentation scheme and antinoise coding is shown in Fig. 1. In this scheme, the generation of W fragments of the original message a_l, $l = 1, ..., N$, with the possibility of its selection upon receipt of fragments share V ($V < W$), is inner coding, and the coding of fragments $(b_m)_l$, $m = 1, ..., W$ using antinoise code is external coding. Accordingly, the generation of code words corresponding to fragments of a transmitted message and its restoration at the reception of a fragments share is carried out with two stages.

The first stage in generating the sequence of code words corresponding to the fragments of a transmitted l-th message consists in its fragmentation corresponding in terms of secret sharing to secret partition. At this stage in accordance with the applied secret sharing algorithm, W code words are generated, which are information blocks $(b_m)_l$, $m = 1, ..., W$, corresponding to the fragments of a transmitted message a_1, $l = 1, ..., N$, which are then serially transmitted via radio channel. In the general case the number of digits of the original message a_n makes up $k_0 = [\log_2 N]$, where $[\cdot]$ means rounding upward to the nearest integer,

and the number of digits of transmitted code words $(b_m)_l$ makes up k_l. In the general case, due to the marked property of perfect schemes of threshold fragmentation, the condition $k_1 \geq k_0$ is satisfied. The second stage in generating the sequence of code words corresponding to the fragments of a transmitted *i*-th message is antinoise coding of *W* information blocks $(b_m)_l$, $m=1,\ldots,W$ generated at the first stage, by using block noise-immune (n,k_1)-code, with all them being further transmitted via communication lines.

When receiving messages, the decoding of a sequence of block (n,k_1)-codes is carried out at the first stage, with error detection or error correction, and the selection of transmitted data blocks $(b_m)_l$ is performed. At the second stage, the restoration of a sent message is performed using selected fragments $(b_m)_l$, according to the applied algorithm of secret sharing. The proper restoration of messages is possible when *V* and more fragments are correctly received, with $V < W$.

In what follows we assume that the fragments of a transmitted message have the following number of digits $k=k_0=k_1$. The relevant schemes of threshold fragmentation are called ideal; their existence is determined by the particular conditions of ideality of specific transformations of secret sharing *F*. The property of ideality allows us to send the fragments of a message with the lowest possible introduction of redundancy and, in terms of time spent, makes fragmented transmission as equivalent to conventional repetition of messages. Specific conditions of ideality are associated with the imposition of restrictions on the number of digits of a transmitted messages and the parameters (coefficients) used in the transformation of secret sharing. Furthermore, there may be found more soft conditions of a nearly ideal transformation of secret sharing, for which $k_1=k_0+1$.

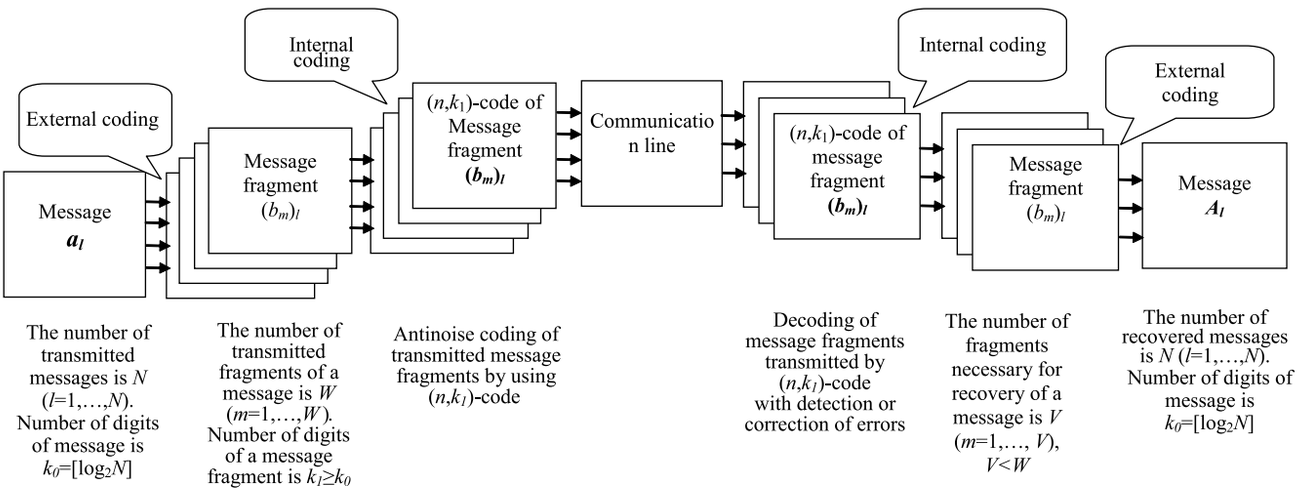

Fig. 1. The scheme of implementation of the method for transmission of messages using the scheme of threshold fragmentation and antinoise coding

2. Study of the accuracy of fragmented transmission of messages using schemes of threshold fragmentation and antinoise coding

Let us consider the general case of fragmented transmission of messages using a scheme of threshold fragmentation (*V, W*) and antinoise coding of fragments by (n,k)-code that detects q_o errors or corrects q_u errors. Interconnection of parameters of the noise-immune code *n* and *k* with multiplicities of known detected and corrected errors q_o, is given by the well-known Hamming boundary [5]. For fixed *n* and *k*, the following expression $q_o > q_u$ is always met.

The baseline characteristic of a communication line, which describes the conditions for information transmission, is the probability of erroneous reception of an information symbol p_0 [2]. The accu-

racy of the transmission of individual fragments by noise-immune codes is generally characterized by the probability of correct reception $P_{пп}$, the probability of detectable errors $P_{оо}$ and undetectable errors $P_{но}$.

In case of antinoise coding of fragments by (n,k)-code with error detection, the probabilities of detectable and undetectable errors are defined by the following expressions:

$$P_{оо} = \sum_{i=1}^{q_o} C_n^i p_0^i (1-p_0)^{n-i}, \tag{1}$$

$$P_{но} = \sum_{i=q_o+1}^{n} C_n^i p_0^i (1-p_0)^{n-i}, \tag{2}$$

and the probability of correct reception makes up: $P_{пп}=1-P_{оо}-P_{но}$.

In case of antinoise coding of fragments by (n,k)-code with error correction, only detectable errors are possible, and the probability of undetected error is defined by the following formula:

$$P_{но} = \sum_{i=q_u+1}^{n} C_n^i p_0^i (1-p_0)^{n-i}, \tag{3}$$

and the probability of correct reception makes up: $P_{пп}=1-P_{но}$.

Equations (1) – (3) correspond to the binomial model of errors in the fragments of transmitted messages [5]. It is the probabilities $P_{оо}$ and $P_{но}$ defined with their help that are the starting point for the calculation of indicators for the accuracy of fragmented transmission of messages using the schemes of threshold fragmentation (V, W). As these indicators, we will consider the probability of missing (non-delivering) a message $P_{пр}$ and the probability of receiving (sorting out) a dummy message. These probabilities are the constituents of the total probability of erroneous reception of a message and characterize the most dangerous types of errors in the transmission of vital messages related to the control of railway automation and train safety operation.

Using the methodology presented in [6] for analyzing the process of serial transmission via communication lines with interference and selection in a reception centre of message fragments generated with the help of the scheme of threshold fragmentation (V,W), we obtain the general expression for the probability of missing messages and receiving a false message:

$$P_{пр} = \sum_{i=W-V+1}^{W} C_W^i (P_{оо}+P_{но})^i (1-P_{оо}-P_{но})^{W-i}, \tag{4}$$

$$P_{лс} = \frac{P_{но}^V}{N^{V-1}} \left[1 + \sum_{i=1}^{W-V} C_{V+i-1}^i \left(1 - \frac{P_{но}}{N} \right)^i \right]. \tag{5}$$

Expressions (4) and (5) correspond to the noise-immune coding of fragments by (n,k)-code with the detection and correction of errors. In case of error detection, the probabilities $P_{оо}$ and $P_{но}$ are determined

by expressions (1) and (2) for the multiplicity of detected errors q_o. In case of error correction, the probability $P_{но}$ is defined by expression (3) for the multiplicity of corrected errors q_u,, and the probability $P_{оо}$ is assumed to be zero: $P_{оо}$=0.

Using expressions (4) and (5) with expressions (1) – (3) taken into account, it is possible to obtain the dependences of probability characteristics of the accuracy of fragmented message transmission $P_{пр}$ and $P_{лс}$ on the probabilities of erroneous reception of an information symbol in the information transmission channel p_0 and the parameters of a threshold fragmentation scheme (V, W) for different (n, k)-codes used to transmit information blocks. Practical interest is in determination under specified conditions of parameters of external (fragmentation scheme) and internal (noise-immune code) coding, providing the required probabilities of missing a message $P_{пр}$ and receiving a false message, which allows us to choose the parameters of fragmentation schemes and noise-immune code that minimizes one of the probabilities $P_{пр}$ and $P_{лс}$ at the maximum acceptable values of the other probability.

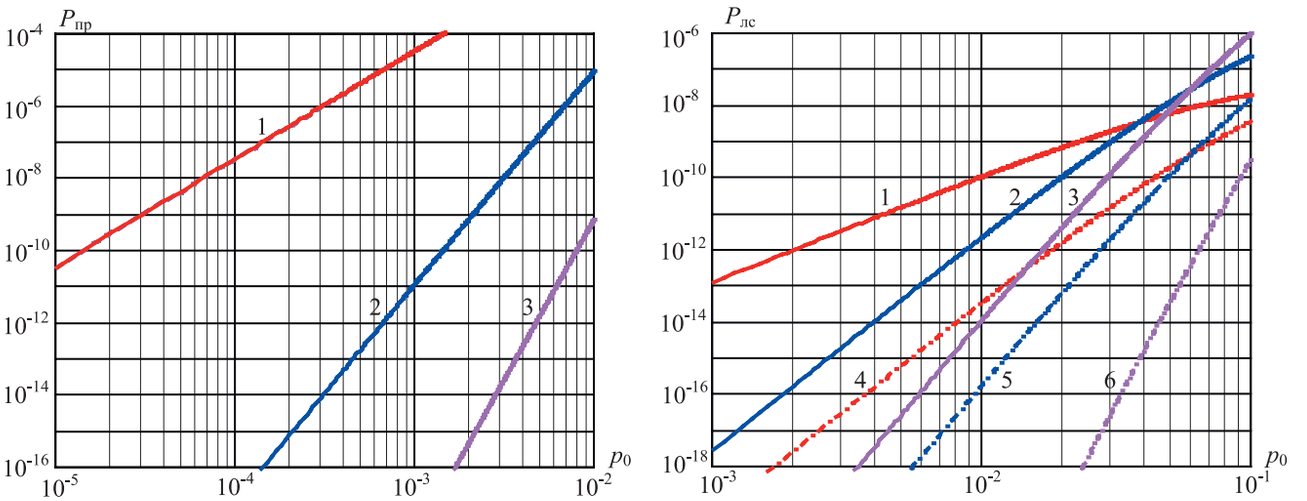

Fig. 2. Dependences of probabilities of missing a message (a) and receiving a false message (b) on the probability of erroneous reception of information symbol for the threshold fragmentation scheme (3,5) using a variety of noise-immune codes

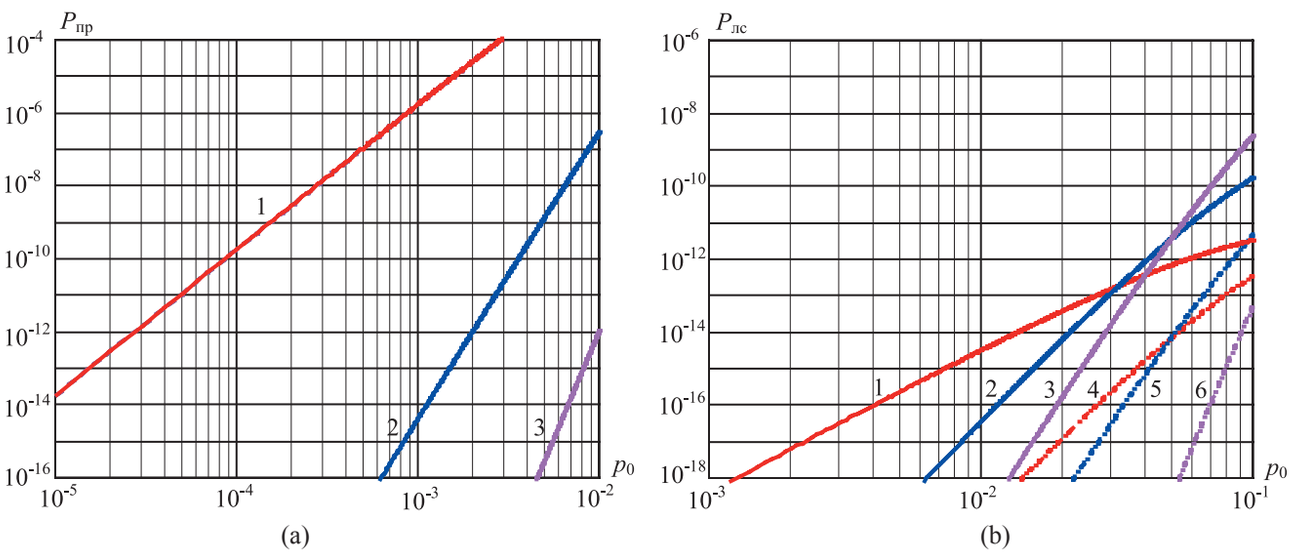

Fig. 3. Dependences of probabilities of missing a message (a) and receiving a false message (b) on the probability of erroneous reception of information symbol for the threshold fragmentation scheme (4,7) using a variety of noise-immune codes

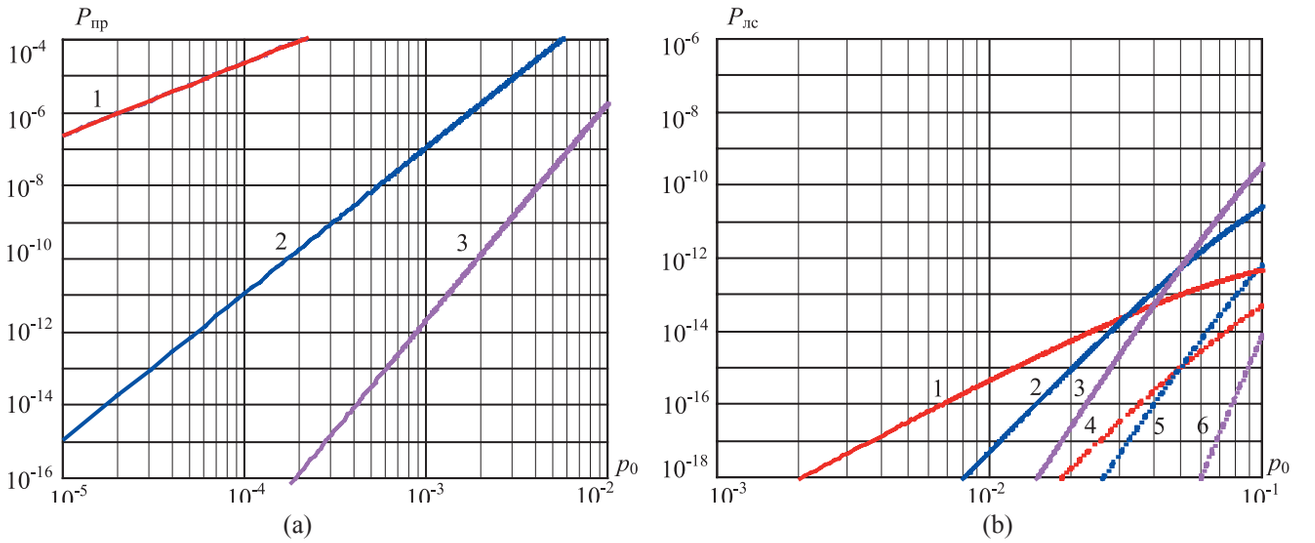

Fig. 4. Dependences of probabilities of missing a message (a) and receiving a false message (b) on the probability of erroneous reception of information symbol for the threshold fragmentation scheme (4,5) using a variety of noise-immune codes

Fig. 2-4 show the results of calculations of the probabilities of missing a message P_{np} and receiving a dummy message, depending on the probability of erroneous reception of the information symbol p_0 using the threshold fragmentation scheme with different parameters V and W, and noise-immune (n, k)-codes with different parameter values q_o and q_u. We considered the following noise-immune codes: code with even parity check (15,14) with code distance $d = 2$ with a multiplicity of detected errors q_o=1 and with a multiplicity of corrected errors q_o=0, the Hamming code (15,11) with code distance $d = 3$ with a multiplicity of detected errors q_o=2 and with a multiplicity of corrected errors q_o=2, the cyclic code (15,8) and minimum distance d = 5 with a multiplicity of detected errors $q_o = 4$, and with a multiplicity of corrected errors q_u=2. Figure 2 shows the dependences of P_{np} (a) and $P_{лс}$ (b) on p_0 for the scheme of threshold fragmentation (3,5). Figure 3 shows the dependences of P_{np} (a) and $P_{лс}$ (b) on p_0 for the scheme of threshold fragmentation (4,7). Figure 4 shows the dependences of P_{np} (a) and $P_{лс}$ (b) on p_0 for the scheme of threshold fragmentation (4,5). Curves 1 in Fig. 2a, 3a, 4a correspond to the code (15,14) with q_u=0 and q_o=1, to the code (15,11) with q_o=2 and to the code (15,8) with q_u=1, curves 2 correspond to the code (15,11) when q_o=1, curves 3 correspond to the code (15,8) for q_u=2.

Curves 1 in Fig. 2b, 3b, 4b, correspond to the code (15.14) with q_u=0, curves 2 correspond to the code (15,11) with q_u=1, curves 3 correspond to the code (15,8) with q_o=2, curves 4 correspond to the code (15,14) with q_o=1, curves 5 correspond to the code (15,11) with q_o=2, curves 6 correspond to the code (15,8) with q_o=4. The value of N, which determines the probability $P_{лс}$, was determined as $N = 2^k$.

The coincidence of the curves corresponding to different alternatives of using noise-immune codes with error detection is conditioned by the fact that the value of the probability of missing a message P_{np} with error detection in accordance with expression (4) is effected by the sum of the probabilities of detectable errors P_{oo} and undetected errors P_{oo} at the transmission of each fragment, which for $q_o \geq 1$ is the same for all considered noise-immune codes with error detection. The magnitude of the probability of receiving a dummy message in accordance with expression (5) is affected by the value of the probability of undetected errors $P_{но}$ at the transmission of each fragment, which is different for all the considered noise-immune codes and alternatives of their use to detect and correct errors.

The analysis of presented dependences shows that the considered method of fragmented transmission of messages even with a sufficiently large probability of erroneous reception of an information symbol in a communication channel (p_0=10^{-2}-10^{-4}) and for small values of the parameters of the fragmentation

scheme V and W, as well as due to identification and correction of errors and repeated transmissions achieves a low probability of missing a message $P_{пр}$ and receiving a dummy message $P_{лс}$ at the level up to 10^{-12}-10^{-16}. The values $P_{пр}$ decrease with the increasing q_u, the values of $P_{лс}$ decrease with increasing q_o and q_u.

The families of dependences in Fig. 2 and Fig. 3 correspond to the assignment of the parameters V and W of the fragmentation scheme, satisfying the ratio $V=[W/2]$, where $[\cdot]$ is rounding upward to the nearest integer. Under these conditions, in case of increase of fragmentation scheme parameters V and W and retention of relationships between them, the probabilities $P_{пр}$ and $P_{лс}$ decrease with the increasing V and W, and the ratio $P_{лс}<P_{пр}$ is always satisfied, therefore in case of decrease of the probability of missing a message, the probability of receiving a dummy message decreases simultaneously. In case of increase of fragmentation scheme parameters V and W, there is a tendency of saturation at some level of the probability values of missing a message $P_{пр}$. Thus, the values $P_{пр}$ for the scheme (4,7) are significantly lower than the values of $P_{пр}$ for the scheme (3,5) but slightly higher than the values for the scheme (5,8). At the same time, the values of the probability of receiving a dummy message $P_{лс}$, with increasing fragmentation scheme parameters V and W, are reduced, without any tendency to saturate. As follows from expression (5), the value $P_{лс}$ also decreases with the increasing number of transmitted messages N. At the same time in the area of large values of the probability of erroneous reception of an information symbol p_0, the effect of the value N on the probability of receiving a dummy message is more noticeable than the effect of values q_o and q_u. With the decreasing values of p_0, the effect practically disappears and the main factor affecting the value of $P_{лс}$ for a fixed p_0 is the multiplicity of detected errors q_o and corrected errors q_u during transmission of message fragments.

The families of dependences in Fig. 2 and Fig. 4 correspond to such an assignment of fragmentation scheme parameters V and W, where the parameter W is fixed and the parameter V increases. Under these conditions, the increase of V does not lead to the simultaneous reduction of probabilities $P_{пр}$ and $P_{лс}$ – the probability $P_{пр}$ increases and the probability $P_{лс}$ decreases, and even with the increase of the V value per unit and a fixed value of W, there is an evident increase of the probability of missing a message $P_{пр}$ and reduction of the probability of receiving a dummy message $P_{лс}$. Therefore, by changing the relationship between the parameters of the fragmentation scheme V and W, it is possible to influence the ratio between the probabilities $P_{пр}$ and $P_{лс}$ in accordance with the requirements imposed on them for transmission of vital messages.

It should be noted that the value of the probability of missing a message defined by expression (4) coincides with the probability of missing a message in case of W-multiple transmission of a non-fragmented message and decision making on V coincidences [7]. In terms of increasing the accuracy of information transmission by introducing redundancy into transmitted messages for repeated transmission, it is equivalent to using the ideal scheme of threshold fragmentation (V, W). However, transmission of messages with simple repetition involves the use of only one step of coding, which can provide only the detection or correction of errors at the expense of correcting abilities of a used noise-immune code that corresponds to the external coding of fragments in fragmented transmission. Multiple transmissions of messages do not have the abilities of information secrecy.

Conclusion

The method of fragmented transmission of vital messages has been analyzed primarily with reference to its use in radio communication systems operating in noisy environments and electromagnetic availability. The accuracy of message transmission is increased by means of introducing considerable redundancy connected with repeated transmission of message fragments, which is the equivalent to

the expense of time spent for their repeating. However, during transmission of formalized messages of train operation and railway automation control, which are, in fact, low informative, a significant introduction of redundancy is justified. First, it allows us to reach low values of the probability of missing messages and receiving false messages (10^{-12}-10^{-16}) in radio channels of low quality with the 10^{-2}-10^{-4} probability of erroneous reception of an information symbol, and second, it allows us to increase simultaneously the accuracy of message transmission via radio channels with interference and protection against unauthorized access.

Besides the possibility of using the considered method in radio communications systems, the method is well consistent with the technology of transmission of signaling messages (commands) to trains via audio frequency track circuits or through spot radio transponders (Eurobalizes) located between rails [6]. Both techniques involve the referencing of transmitted messages to the so-called block sections passed by a train, where one of the fragments of a next message can be transmitted.

References

1. **Kudryashov V.A., Mochenov A.D.** Transport communication. – M.: Route 2005. – p. 294.

2. **Teplyakov I.M.** Fundamentals of telecommunication systems and networks. – M.: Radio and communication, 2004. – p.328.

3. **Maltsev G.N., Adadurov A.S.** Reduction of threats to information security of radio systems / / Automation. Communication. Informatics. – 2011. – # 5. – p..22-24.

4. **Yaschenko V.V., Varnovsky N.P., Nesterenko Yu.V.** et alia. Introduction to Cryptography /Ed. By Yaschenko V.V. – Moscow: MCCME (Moscow Center for Continuous Mathematical Education) – 1998. – p.272.

5. **Werner M.** Coding Basics: Translated from German. – M: Technosphere, p. 2008.-288.

6. **Yakovlev V.A., Adadurov A.S.** Method for safe data transmission to train based on the “secret sharing” principle using additional channels / /Dependability-2012. – # 4. – p..95-104.

7. **Maltsev, G. E., Chernyavsky E.V.** Message encryption in systems of radio control without reverse information channel / /Information and control systems. – 2011. – # 4. – p.60-65.