e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 3
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 3

UDC 004.056

INCREASING THE SECRECY OF TRANSMISSION INFORMATION BASED ON COMBINED RANDOM CODING

Korchynskyi V. V. – Dr. Sc., Associate Professor of the Department of Information Security and Data Transmission, O. S. Popov Odessa National Academy of Telecommunications, Odessa, Ukraine.

Kildishev V. I. – PhD, Associate Professor of the Department of Information Security and Data Transmission, O. S. Popov Odessa National Academy of Telecommunications, Odessa, Ukraine.

Holev D.V. – Seniour lecturer of the Department of Information Security and Data Transmission, O. S. Popov Odessa National Academy of Telecommunications, Odessa, Ukraine.

Berdnikov O. M. – Post-graduate student of the Department of Information Security and Data Transmission, O. S. Popov Odessa National Academy of Telecommunications, Odessa, Ukraine.

ABSTRACT

Context. The task of increasing the secrecy of information transmission based on combined random coding is considered. The object of research is the integration processes of stochastic, block and timer coding.

Objective. The aim of the article is to develop a method of increasing the secrecy transmission based on combined random coding.

Method. The method of increasing the secrecy of information transmission based on combined random coding with three steps of code converters: internal, intermediate and external is proposed. The internal converter is implemented based on stochastic coding with various numbers of random code combinations. The number of random combinations depends on the probability of the character of the symbol in the message text. The information secrecy of the transmission is ensured by equalizing the probabilities of the occurrence of code combinations from the output of the statistical coder. Intermediate coding is implemented using a noise immunity block code. Information secrecy and noise immunity leads to the increasing the length of the code block at each stage of coding, which reduces the code rate. To solve this problem, an external converter based on timer coding is used. At this stage, binary combinations are converted into timer signal structures, which allows for the implementation of a structural transmission secrecy, increase the code rate and improve noise immunity. When the stochastic encoding and a timer used codebooks.

Results. The developed method of combined random coding allows to increase the main indicators of noise immunity: interference protection, information and structural secrecy.

Conclusions. The proposed method of combined random coding allows to eliminate the main disadvantages of stochastic coding, in which the choice of the number of random code combinations does not take into account the entropy of the discrete source of information. For solving this problem, it was proposed to use different number of random combinations, in view of the probability of an alphabet symbol appearing in the text. From the theoretical point of view, this will allow the output of the statistical coder to form a stream of combinations with equal probabilities of occurrence. Due to the usage of timer signal constructions, the problem of redundancy compensation is solved, which appears during stochastic and noise-immune coding.

KEYWORDS: information protection, secrecy, coding, timer signal, noise immunity.

ABBREVIATIONS

BDC is a bit digital code;
SC is a statistical coder;
PA is a probabilistic analyzer;
SI is a source of information;
TSC is a timer signal construction;
SC is a source coder;
CB is a code book;
RNG is a random number generator;
SRC – shaper random combinations;
ED is a encoding device;
RNG is a random number generator;
C TSC is a TSC coder.

NOMENCLATURE

d_0 is a minimum code distance;
T_c is a time interval of formation TSC;
n is a number of Nyquist elements;
l is a number of additional elements with stochastic coding;
k_1 is a number of additional elements with stochastic coding;
r is a number of check bits;
γ_1 is a code rate of the stochastic coder;
γ_2 is a code rate of the noise-resistant coder;
γ_3 is a code rate at the output of the timer coder;
P_{UE} is a probability of an undetected error in a code combination;
$H_{NS}(U)$ is a entropy of a discrete source of information;
S is a potential structural secrecy of signal constructions;
L is a number of signal constructions;
t_0 is a Nyquist time interval;
Δ is a basic element of the constructing of the TSC;
s is a number of elements Δ the number of elements t_0;
N_{pTSC} is a number of TSC;
A_k is a weight coefficients of the quality equation.

INTRODUCTION

The search of new methods of information protection, from unauthorized access is due to the requirement to increase the interference protection of modern radio transmission systems, operating in conditions of electronic conflict. [1]. The main components of interference protection are noise immunity and secrecy. As a rule, a given noise immunity is provided by means of correction codes [2], what leads to decrease the code rate due to the

DOI 10.15588/1607-3274-2019-3-12

introduction of additional redundant elements. To increase the secrecy of transmission, various methods are used to convert confidential information. Depends on the belonging of the communication system, the transfer of secrecy can be provided at various levels of the OSI model [3]. When developing a special purpose communication system, as a rule, several types of secrecy are used [5]. In addition to information secrecy, the structural [6] and energy secrecy [7] (channel and physical layers of the OSI model) can also be involved. Obviously that each stage of the conversion requires certain energy and time costs, which influence on the delay of the transmitted signal and power consumption.

Therefore, for the improving the main indicators of noise immunity, it is advisable to use an integrated approach in which various methods for transforming the transmitted information and signal structures are combined into a single process. In this article, it is proposed to use combined random cascade coding based on timer signal constructions in combination with stochastic and noise-immunity coding to solve this problem. With the appropriate choice of code parameters, this method of protecting information will allow the transmission of confidential messages over a communication channel by signals with a complex and variable structure and increasing the fidelity of transmission due to the additional function of monitoring fidelity of transmission, which is provided by timer coding.

The timer signals [8] are non-positional signal constructions, based on which can be implemented noise immunity coding without the use of additional verification elements. Using timer coding at the given time interval, it`s possible to form a greater number of signal constructions as compared to digit-digit codes (BDC). It could be achieved by reducing the energy distance between the timer signal construction (TSC).

The structure of the timer signals and their correcting ability is given by using the parameters for constructing combinations. Based on the TSC, it is possible to create various algorithms for increasing the structural secrecy [7]. For realization this, the transmission of information through the channel uses arrays of signal constructions with different structures. This justifies the expediency of using timer signals when implementing the method of combined random coding. Therefore, the search for effective methods of protecting information based on the TSC is an actual task.

The object of study is the integration processes of stochastic, block and timer coding. The process of stochastic coding usually does not consider the entropy of a discrete source of information and accompanies with an increase in code redundancy. For solving this problem, it was proposed to use a variable number of random code combinations, taking into account the probability of symbols appearing in the text, and for reducing redundancy was proposed to use timer signals.

The subject of study is the methods of increasing informational and structural secrecy based on stochastic and timer coding.

The known methods of stochastic coding [9, 10] are distinguished by a low information secrecy of transmission, and are also characterized by high redundancy when using random code combinations.

The purpose of the work is to increase the informational and structural secrecy of the transmission based on the sharing of stochastic, block and time coding.

1 PROBLEM STATEMENT

Consider cascade coding with three steps of code converters: external is a stochastic coding; intermediate block error-correcting coding based on the BDC; internal is a timer encoding.

The width of the cascade converter n is determined by the width n_1 of the external, intermediate n_2 and n_3 internal code. Code transmission rate at each step of the code converter is $\gamma_1 = k_1/n_1$; $\gamma_2 = n_1/n_2$; $\gamma_3 = n_2/n_3$, where k_1 is the number of information elements from the output of the source coder; $n_1 = k_1 + l$ is the number of elements from the output of the statistical coder; $n_2 = n_1 + r$ is the number of elements at the output of the noise-immunity code; r is the number of check bits. With stochastic and block noise-immunity coding, the length of the code block increases, which leads to decrease the code rate in these converters, i.e. $\gamma_1 < \gamma_2$. The solution of this problem is proposed due to the time coding, which will allow to reduce the code length of the code word n_2 due to the TSC, i.e. $n_3 < n_2$. Therefore, $\gamma_3 > \gamma_2$.

With stochastic coding, the total number of random combinations is $N_1 = 2^z$, which is proposed to be redistributed for the coding problem, taking into account the probability of the alphabet character appearing in the message text, which will increase the information secrecy of the transmission.

For increasing the structural secrecy, it is proposed to use a set of TSC from two combinations, one of which is allowed with a minimum code distance d_0, and the other combination is selected using a random number generator.

The improving noise immunity is accomplished through the using of block noise immunity and timer coding. The total probability of the undetected error in the code block $P_{UE} = P_{UE1} \times P_{UE2}$, where P_{UE1} is the probability of the undetected error in block noise immunity coding; P_{UE2} is the probability of the undetected error during timer encoding.

2 REVIEW OF THE LITERATURE

In telecommunication systems, methods of channel coding and information protection from unauthorized access [2, 4] are applied, as a rule, independently of each other. At the same time, the relationship is not taken between the required level of noise immunity and the secrecy of information transfer [3]. It is known [2, 4, 8] that the noise immunity of transmission is mainly provided by means of correction codes. Consider the conditions for the transmission of information through the channel, using

DOI 10.15588/1607-3274-2019-3-12

the Hilbert model [8]. As a rule, the required reliability of transmission is achieved by increasing the transmission time of the message, since test elements are added to the information bits, the number of which is determined taking into account the worst state of the channel. For this reason, the channel is in good condition, i.e. with a low level of interference, the transmission of information will be carried out with great redundancy [2]. It is obviously that due to the introduction of the maximum correcting ability of the code, high reliability of the transmitted information over the communication channel is ensured over a wide range of interference levels. However, in the case of radio interception of the transmitted message, the enemy's cryptanalyst does not have any especial problems in recognizing the semantic content of confidential information.

The method of combined random coding [9, 10] is based on the combined use of stochastic and immunity coding. The information secrecy of the transmission is provided due to the random change of the ensemble of transmitted code combinations. This coding method refers to non-cryptographic methods for protecting information. The required level of transmission security is ensured by the uncertainty of the choice of the ensemble of code combinations for the transmitted message symbols. However, the following disadvantages of stochastic coding should be noted. When choosing an ensemble of random code combinations, the entropy of a discrete source of information [9] is not considered, which increases the vulnerability of this method of protecting information from unauthorized access. Another disadvantage of stochastic coding is the large redundancy, which appears due to the operation of replacing the character combination of the used alphabet with some random combination from a given ensemble [9, 10]. Besides, the check bits of the noise immunity coding are also added to the information sequence [2, 4].

In order to eliminate the drawbacks of these coding methods, it is proposed to determine the size of the sample random code combinations with the probability of a symbol appearing in a message to increase the information secrecy. This will provide an approximately equal probability of the occurrence of code combinations from the output of the stochastic coding. The time coding [8] will reduce the redundancy of stochastic and block noise immunity coding, as well as increase the structural secrecy of signal constructions [6]. Thus, the research in this direction is an actual task.

3 MATERIALS AND METHODS

The method of combined random coding is realized by three stages of code converters: internal, intermediate and external. The internal converter uses stochastic coding, based on which information secrecy of transmitted messages is provided. With the help of a block code (internal converter) the required noise immunity of transmission over the channel is achieved. The external converter is realized on the basis of timer coding, with the help of which the structural secrecy of signal constructions is provided [3, 7], and the compensation of redundant elements with stochastic and block coding is carried out. With the help of timer signals it is also possible to implement noise immunity coding [8].

To increase the information secrecy of transmission in stochastic coding, it is proposed to take into account the entropy of a discrete source of information when choosing the number of random combinations. In accordance with the Shannon expression, the entropy for the case with non-equiprobability states is determined by the formula [8]:

$$H_{NS}(U) = -\sum_{j=1}^{L} p_j(u_j) \times \log_2 p_j(u_j). \quad (1)$$

For example, the entropy of the alphabet of the russian language with the probability of the appearance of characters in the text, is $H_{NS}(U)$ = 4,42. The entropy for equiprobable alphabetic characters is $H_P(U)$ = 5. It is obviously, for increasing the information secrecy of transmission with stochastic coding could be possible with equiprobable appearance of random combinations of the transmitted encoded message, i.e.

$$H(U) \to H_p(U), \quad (2)$$

and also provided that

$$n_1 \to \infty, \quad (3)$$

where $n_1 = k + l$ is the number of binary elements in a random code combination; k is the number of information elements; l is the number of additional bits that are added to the information elements during stochastic coding.

Condition (2) can be ensured if the number of random combinations is chosen with the probability $p_j(u_j)$ of each symbol b_j of the used alphabet. Condition (3) significantly reduces the code rate, so the choice of the value of n_1 should be made with the requirements for transmission speed and information secrecy.

In block coding, the length [12] of a random code combination is increased by r elements, i.e. $n = k + l + r$, where r is the number of test elements. The use of stochastic coding significantly reduces the code rate, because

$$\gamma_{cr} = \frac{k}{k + l + r_2} < \gamma_c = \frac{k}{k + r_1}, \quad (4)$$

where γ_{cr} is a code rate when stochastic and block coding are used together; γ_c is a code rate for block coding; r_1 is the number of verification elements for the length of information combinations of k elements; r_2 is a number of test elements for combinations of z elements.

It is obviously that the secrecy of transmission can be enhanced by increasing the number of combinations from ensemble C, which means $n_1 = [\log_2 N]$ also increases. For comparative analysis in the Table 1 shows the structure of the generated code block, depending on the coding variant of the information sequence k. Apparently, for the block structure $n = k + r_1$, only noise immunity coding can be implemented (Table 5, № 1). With stochastic coding ($n_1 = k + l$), only information secrecy is provided.

DOI 10.15588/1607-3274-2019-3-12

For the block structure $n_2 = k + l + r_2$, comprehensive protection of the channel against interference and unauthorized access is implemented (Table 5, №3). The noise immunity coding based on the TSC allows with the data Tables 2–4 reduce the code rate $\gamma_к$. It is explained by the fact that the interval for constructing the TSC is less than for the information sequences of the BDC, i.e. $m_{TSC} \le k$ (Table 5, №4).

The combined random cascade coding based on the BDC and the TSC replaces the structure of the combination $n = k + l + r_2$ on the timer $x_{TSC}(t)$, the bit width of which $m_{TSC} < k + l + r_2$ (Table 1, №5). The combined combination of two TSCs from one allowed combination and another, which is selected using the second codebook, will ensure the structural secrecy of the transmission. In this case, the capacity of two TSCs is less than the binary combination, i.e. $m_{TSC1} + m_{TSC2} < k + l + r_2$.

Table 1 – Variants of the formation code combinations

№	Variant of coding	The composition of the code block		
1	Noice immunity coding based on BDC	k	r_1	–
2	Stochastic coding	k	l	–
3	Combined random coding based on BDC	k	l	r_2
4	Noice immunity coding based on TSC	$m_{TSC} \le k$		
5	Combined random cascade coding based on BDC and TSC	k	l	r_2
		$x_{TSC}(t)$: $m_{TSC} < k + l + r_2$		
6	Random cascade coding based on the BDC and two TSC	k	l	r_2
		$m_{TSC1} + m_{TSC2} < < k + l + r_2$		

Structural secrecy characterizes the ability to resist actions that are aimed at disclosing the structure of the signal [13]. In this case, recognition of the form and measurement of signal parameters is carried out. The potential structural secrecy depends on the number of signal constructions N, which are used to transmit information symbols [13]:

$$S = \log_2 N . \qquad (5)$$

To increase the structural secrecy, it is necessary to expand the ensemble of the used signals [6, 7, 13].

4 EXPERIMENTS

In Fig. 1 shows a block diagram of a transmitter with combined random coding with three stages of information conversion. In the proposed scheme of stochastic coding (SC) use a probabilistic analyzer (PA), with the help of which the probabilistic parameters of the symbols b_i of the used alphabet of the source of information (SI) are determined.

The source coder (SC) encodes the character b_i with a binary code of k elements. Further, with $p_j(u_j)$ and l, for each symbol b_i, are defined the number of random code combinations, which are written to the random combination generators (SRC_j) using the code book (CB1). In stochastic coding (internal converter), each character of the b_i message is coded with a certain binary combination Q_i of k binary elements. Next, each combination Q_i is associated with a combination c_j, randomly selected using a random number generator (RNG) from some given ensemble C ($c_j \in C$). In this case, the width of the code word k is increased by l elements, i.e. $n_1 = k + l$. To fulfill condition (2), it is necessary that the symbols of the alphabet with a higher probability of occurrence of $p_j(u_j)$ in the text use fewer random combinations and vice versa. The total number of random combinations used is $N_{tot}=2^z$ in the ensemble C, which is distributed among the SRC_j blocks of the stochastic coder.

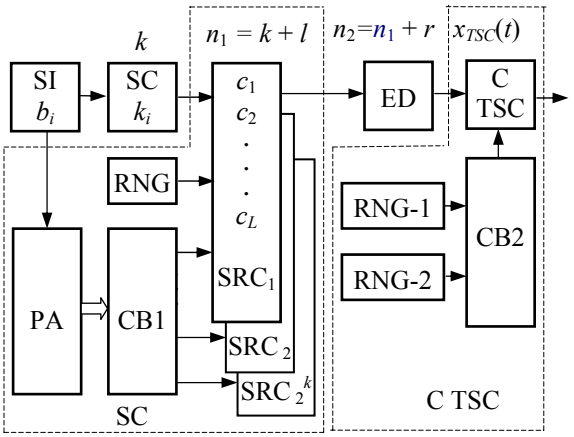

Figure 1 – Structural block diagram with combined random coding

Encoding device (ED) performs the functions of noise immunity coding (intermediate converter), in which the length of the code block z is increased by $n = z + r$.

The external converter is implemented based on timer coding, with the help of which an increase in the code rate is carried out, as well as the structural secrecy of signal structures is provided. According to the formula (5), in order to increase the structural secrecy, it is necessary to use the largest possible ensemble of signal constructions [13]. It is known [3, 4, 8] that in a binary channel, it is possible to increase the number of implementations of signal structures at a given time interval using timer signals. Also, on the basis of the TSC, you can control the accuracy of the received information [8]. For this reason, when studying the possibilities of timer coding on the synthesis of various sets of allowed signaling constructions d_0, and it is necessary to consider the value of the minimum code distance d_0, which determines the correcting capacity of the code.

Consider the features of the synthesis of timer signals. Such signals are formed on the time interval $T_c=nt_0$, where n is the number of Nyquvi-elements with duration t_0. The basic element of constructing the signal construction is the element $\Delta = t_0/s$, $s \in 1, 2, \dots l$ is integers. The information in the TSC is located in the durations of the individual time intervals of the signal $t_c = t_0 + k\Delta$ ($k \in 1, 2, \dots s\ (n–2)$) and their relative position on the plotting interval T_c. In Fig. 2 shows an example of constructing binary TSCs on Δ of the same sign ("1" or "−1"). The time interval $T_c = 4t_0$ и $s = 4$ with the base element Δ. The figure shows that the timer signals refer to bit digitals codes in which the signal construction contain pulse durations t_c not less than s in a row of transmitted elements.

DOI 10.15588/1607-3274-2019-3-12

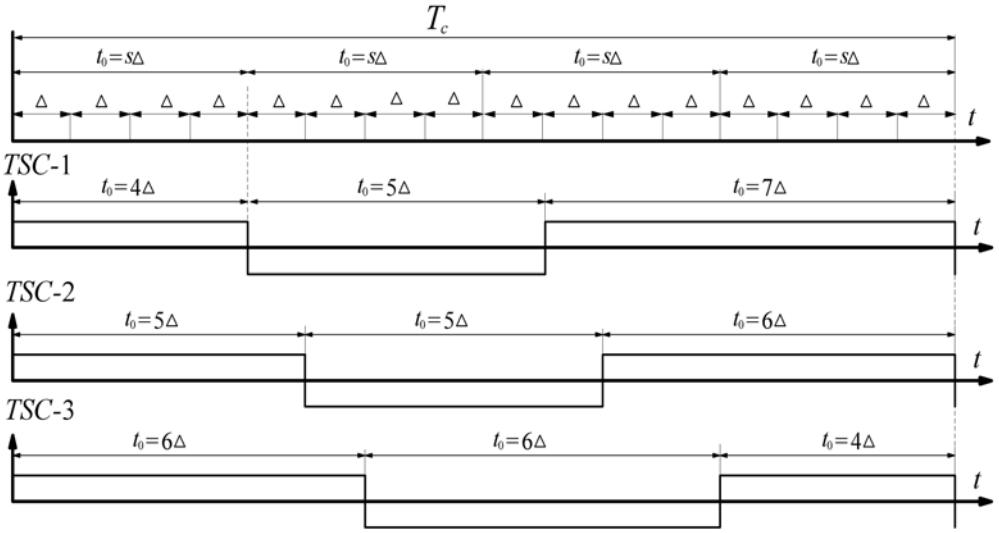

Figure 2 – Timer signal constructions with parameters $n = 4$, $s = 4$, $i = 2$

To the channel are transmitted the pulses with time intervals of $t_c \geq \Delta\,(s + i)$ (i = 1, 2, 3, …), which eliminates intersymbolic distortions. The pulses with a duration t_c are not multiples of t_0, which reduces the energy distance between the signal structures to Δ and increases the number of realizations of the TSC N_{pTSC} in the interval $T_c = nt_0$ [8]:

$$N_{pTSC} = \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!}, \qquad (6)$$

where i is a number of informational significant modulation moments in the signal construction.

In table 2 shows the implementation of the timer signals for the parameters s, n і i = 1, 2, …, n with the minimum code distance $d_0 = 1$. Obviously, with the timer coding, a larger number of allowed signal constructions. is formed than with the BDC. For example, in the time interval $T_c = 5t_0$ and $s = 4$, $N_{pTSC} = 344$ timer signals can be obtained, and for the BDC coder such a number of implementations will be formed with a larger value $n = \lceil \log_2 344 \rceil = 9$. It should be noted that the sets of signal constructions with $d_0 = 1$ do not have corrective properties. If $d_0 \geq 2$, then with the help of timer signals it is possible to implement noise immunity coding. For the TSC, it was proposed to use the Hamming code distance with the base element Δ:

$$d_0 = \sum_{j=1}^{W} x_j \oplus z_j \,, \qquad (7)$$

where x_j and z_j is a logical state of the segments of the TSC ("0" or "1") on the element Δ; $W = n \cdot s$ is the number of elements Δ on the time interval T_c. In Fig. 2 combinations of TSC-1 and TSC-2 have $d_0 = 2$, between TSC-1 and TSC-3 is $d_0 = 5$, TSC-2 and TSC-3 is $d_0 = 3$.

Table 2 – Number of implementations of TSC N_{pTSC} depending on the s and n

n \ s	1	2	3	4	7
5	31	88	188	344	1293
8	255	1596	5895	16492	153400
10	1023	10945	58424	217224	3705000

Table 3 – Number of implementations of TSC N_{pTSC} depending on the d_0, n, s and i

№	Parameters TSC			Selections allowed TSC d_0			
	n	i	s	1	2	3	4
1	7	3	5	1771	891	248	146
2	7	3	6	2925	1469	395	231
3	7	3	7	4495	2255	591	344
4	8	3	5	3276	1638	438	252
5	8	3	6	5456	2736	714	408

When constructing TSC ensembles, it is important to choose the optimal values n, s and i, for which the maximum number of realizations can be obtained. Let us estimate the change in the ensemble of realizations of the TSC N_{pTSC} depending on the parameters n and i at a constant value of s. In Fig. 3 shows the dependences of N_{pTSC} on i, n = 8, 10, 12 and s = 4. It can be seen that with increasing i, the number of implementations of N_{pTSC} first increases and then, having reached its maximum, decreases. For optimal values $i_{opt1} = 5$, $i_{opt2} = 6$, $i_{opt3} = 7$, respectively, for n = 8, 10, 12, you can get the maximum values of realizations N_{pTSC}.

The method of coding and decoding of timer signals according to (6) and (8) suggests a tabular method of storing all allowed and unresolved combinations. Another method of generating signal constructs uses the quality equation (9), which greatly simplifies the procedure for finding the allowed combinations with time-based coding. The decoding process is also simple, as the analysis shows that the number of implementations in Table 4 is much smaller than with full enumeration (Table 3). how similar, as in coding, the quality equation is used [8]:

DOI 10.15588/1607-3274-2019-3-12

$$\sum_{k=1}^{i} A_k x_k \equiv 0 (\mathrm{mod}\, A_0), \qquad (9)$$

where $A_k(k=1, i)$ are weights that are a set of prime numbers; A_0 is a modulus values; x_k are the numbers of reports of the significant modulation moments (SMM) of pulses t_{ci}. If the signal construction according to the decoding results satisfies the quality equation (9), then it is resolved.

The quality equation is a convenient tool for the synthesis of allowed signal constructions with a specified minimum code distance d_0.

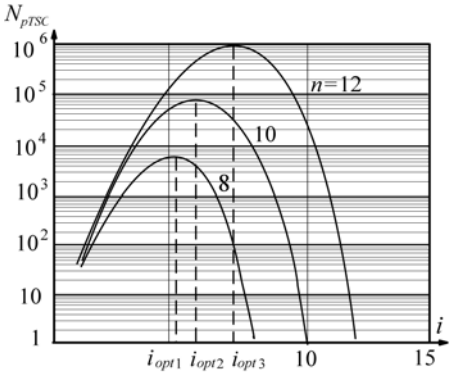

Figure 3 – The number of implementations N_{pTSC} depending on the i at s = 4, n = 8, 10, 12

Table 4 – The number of allowed TSCs, depending on n, s, i, d_0 and quality equation coefficients A_0=19, A_1=2, A_2=3, A_3=7

№	Parameters TSC			General quantity implementations	Selections allowed TSC d_0		
	n	i	s		4	5	6
1	7	3	5	1771	93	37	27
2	7	3	6	2925	154	59	43
3	7	3	7	4495	236	88	68
4	8	3	5	3276	173	65	52
5	8	3	6	5456	288	106	82
6	8	3	7	8436	444	156	123

In tab. 4 shows the implementation of the TSC, which are obtained using the quality equation (9) with coefficients A_0=19, A_1=2, A_2=3, A_3=7. Comparative analysis shows that the number of implementations in the table. 4 is much smaller than with full brute force (Table 3).

5 RESULTS

The results of the researching of timer signals have shown the possibility of increasing the structural secrecy of transmission due to the combined use of signal constructions. In this case, in order to control the transmission fidelity, it is advisable to use allowed TSC with a certain minimum code distance d_0. So for d_0 = 4 and n = 7, i = 3, s = 5 with the help of (9) from the total number of implementations N_{pTSC} = 1771, you can get N_{pTSC} = 93 (Table 4) resolved structures, and with full enumeration, N_{pTSC} = 146 (Table 3). An increase in $d_{0.}$ leads to a decrease in the sampling of signal constructions. For example, when $d_{0.}$ = 5, the number of allowed combinations N_{pTSC} = 37 (Table 4), and with full enumeration, N_{pTSC} = 79 (Table 3). Consequently, such features of the formation of permitted TSCs should be considered when developing methods for enhancing the structural secrecy of transmission and ensuring the required reliability. In Table 5 for the quality equation (9), the values of the coefficients A_0, A_1, A_2 and A_3 are presented, at which TSC implementations with different values of d_0 can be formed.

Table 5 – The coefficients of the quality equation for the formation of allowed TSC with a certain value d_0

№	d_0	A_0	A_1	A_2	A_3
1	4	19	2	3	7
2	2	7	2	3	5
3	2	11	2	3	7
4	3	13	2	3	7
5	–	17	2	3	7

Consider the possibility of increasing the code rate with the following parameters of the combined coding: k = 8, l = 7, r = 6. In the quality of the noise-immunity code it is proposed to use the cyclic code (21, 15). The number of allowed combinations for this code is $N_p = 2^{15}$ = 32768, and the code rate γ_{cdc} = 15/21 = 0,714. As can be seen from the Table 3 and 4, the number of implementations of allowed TSCs is less than the value of 32768. Therefore, it is proposed to use a combination of two TSCs (Table 5) to transmit BDC combinations using timer signals. For the parameters of the TSC from the Table 6, №1 for d_0 = 4, you can form N_{pTSC} = 93 × 1771 = = 164703 combinations, for d_0 = 5 N_{pTSC} = 37 × 1771 = = 65527, for d_0 = 5 N_{pTSC} = 27 × 1771 = 47817, etc.

As can be seen from the Table 5, the usage of a combination of two TSCs at the stage of timer coding, one of which is permitted, can significantly increase the number of implementations for transmitting BDC combinations. The presence of at least one allowed TSC ensures the preservation of the value of the minimum code distance d_0.

Table 6 – The number of allowed combinations depending on n, s, i, d_0 and A_0=19, A_1=2, A_2=3, A_3=7 for the combination of two TSC

№	Parameters TSC			N_{pTSC}	Samples of two vehicles depending on the d_0		
	n	i	s		4	5	6
1	7	3	5	1771	65527	47817	42504
2	7	3	6	2925	172575	125775	119925
3	7	3	7	4495	395560	305660	260710
4	8	3	5	3276	212940	170352	131040
5	8	3	6	5456	578336	447392	371008
6	8	3	7	8436	1316016	1037628	826728

The increase in the transmission interval of the TSC in two times ($m_{TSC} = 2n$) provides compensation for the redundancy of stochastic and noise immunity coding. Considering the fact, that the binary code from n_{dc} = 21 bits is replaced by the TSC from m_{TSC} = 14 elements, then the code rate increases 1.5 times.

Obviously, it is possible to use TSC sets with a large value s, however the room resistance will decrease, which

DOI 10.15588/1607-3274-2019-3-12

is necessary to consider when choosing the parameters for constructing signal constructions.

6 DISCUSSION

Combined random coding allows to effectively protect information from unauthorized access and random noise [9, 10]. In stochastic coding, the information secrecy depends on the number of combinations used in the SRC block, which significantly reduces the code rate (4). The disadvantage of this method is the uneven appearance of random code combinations (1). Therefore, in the proposed stochastic coding scheme (Fig. 1), the number of random combinations is selected with the probability of characters appearing in the message, under which condition (2) is fulfilled.

The noise immunity coding at the intermediate stage is aimed at ensuring the required fidelity of the transmission, however, as with stochastic coding, this problem is solved by reducing the code rate (4). To compensate for the redundant elements of the BDC, it is proposed to use the TSC, which it is advisable to use for the channels that describe the Hilbert model [8].

Using the TSC on the given Nyquist interval n, could construct the larger number of realizations (Table 2) than with the BDC, i.e. $m_{TSC}>2^n$. The application of TSC as a noise immunity code requires the use of allowed combinations with a minimum code distance $d_0 > 1$, which reduces the number of implementations with increasing d_0 (Tables 3 and 4). There are two ways to form TSC [8]. With the help of (6) and (7) the quantity of TSC is determined, which can be implemented in a tabular way. Reducing the time of formation of the TSC provides the quality equation (9), on the basis of which coding and decoding can be implemented. However, using (9), the number of allowed combinations is less than with (6) and (7). This limits the capabilities of the TSC, which can be used to transfer binary combinations with small lengths $n = 10 – 13$, which is clearly not enough for the implementation of stochastic and noise immunity coding based on BDC. That's why, to solve this problem, it was proposed to use a combination of two TSC at the stage of external coding. For saving the set value d_0, the combination must include at least one allowed TSC. A twofold increase in the TSC transmission time interval will allow increasing the number of implementations hundreds of times, which is enough for transmitting BDCs with $n > 13$. One more advantage of using a combination of two TSCs is the ability to create different sets of implementations by combining allowed and unresolved signal designs. This will require to use of the second code book CB2(Fig. 1), which is used to determine the correspondence between the BDC and TSC. Generators of random numbers RNG-1 and RNG-2 provide filling of CB2 by choosing combinations of TSK.

The further research in this direction should solve the problem of determining the complex indicators of interference protection: noise immunity, information and structural secrecy. It is necessary to determine the optimal length of random code combinations and timer signals, taking into account the given values of information and structural secrecy. It is also necessary to ensure the coordination of parameters between the stages of stochastic, noise immunity, and timer coding.

CONCLUSIONS

The actual task of improving the methods of increasing information and structural secrecy has been solved with the help of stochastic, noise immunity, and timer coding.

The scientific novelty of the results is concluded in that, the first time a method of stochastic coding was proposed, which considers the entropy of the appearance of characters in the message when forming random combinations. The use of TSC will provide compensation for redundant elements in stochastic and noise immunity coding. Also, the timer coding is an additional cascade to increase transmission fidelity. The increase in the number of implementations of signal constructions at Nyquist intervals makes it possible to use them to ensure the structural secrecy of transmission. The greatest effect of increasing the set of signal constructions is achieved with the use of two TSCs, which should include at least one allowed code construction.

The practical significance of the obtained results is that the software has been developed with which could be possible to implement various stages of cascade random coding. The results of the experiment allow recommend the proposed indicators for the development of real interference protection communication systems with random coding, as well as determine the boundary conditions for the application of the parameters of stochastic, noise immunity and timer coding.

The prospect of further research is the studying of the proposed set of indicators for building communication systems that provide increased noise immunity, information and structural secrecy.

ACKNOWLEDGEMENTS

The article is supported by the state budget scientific research project of O.S. Popov Odessa National Academy of Telecommunications «Increasing the security of telecommunication systems based on methods of coding, encryption and spectrum expansion» (state registration number 0118U00595).

REFERENCES

1. Sha'ameri A. Z., Kanaa A. Robust multiple channel scanning and detection of low probability of intercept (LPI) communication signals / A. Z. Sha'ameri, // *Defense S&T technical bulletin,* 2016, Vol. 9, Issue 1, pp. 1−17.
2. MacKay D. Fountain codes, *IEEE Proceedings Communications,* 2005, Vol. 152, No. 6, pp. 1062−1068.
3. Zakharchenko M., Korchynskii V., Kildishev V. Integrated methods of information security in telecommunication systems, *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library, Odessa, 11–15 September 2017 : proceeding*. Odessa, IEEE, 2017, pp. 78–81.

DOI 10.15588/1607-3274-2019-3-12

4. Information technology. Security techniques. Code of practice for information security controls. ISO/IEC 27002:2013. [Effective from 2013-09-25]. Geneva, ISO, 2013, 80 p.
5. Glisic S. Adaptive WCDMA: Theory and Practice. John Wiley & Sons, 2003, 357 p.
6. Zakharchenko N., Korchinsky V., Radzimovsky B. Information security of Time-Controlled Signals in Confidential Communication Systems, *Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, Lviv-Slavske, 21–24 February 2012*. Lviv, Publishing House of Lviv Polyteshnic, 2012, P. 317.
7. Korchinskyi V., Hadzhiyev M., Kildishev V. et al. Development of the procedure for forming non-stationary signal structures based on multicomponent lfm signals, *Eastern-European Journal of Enterprise Technologies*, 2018, No.6/9 (96), pp. 29–37.
8. Zakharchenko N., Korchinskiy V., Radzimovsky B. et al. Assessing the Impact of the Noise on the Throughput Communication Channel with Timing Signals, *Eastern European Scientific Journal: AURIS Communications und Verlagsgesellschaft mbH*, 2015, No. 4, pp. 209–214.
9. Maltsev G. N. Immunity and secrecy of transmitting information over radio channels based on combined random coding, *Information control systems,* 2016, Vol. 19, Issue 2, pp. 126−139.
10. Lu Yu. Stochastic Tools for Network Security: Anonymity Protocol Analysis and Network Intrusion Detection : thesis … doctor of philosophy. Clemson, Clemson University, 2012, 101 p.
11. Zhu Y., Bettati R. Anonymity v.s. Information Leakage in Anonymity Systems, *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, Columbus, June, 2005 : proceedings*. Texas, IEEE, 2005, pp. 86−97.
12. Banket V., Toporkov F. Efficiency of Forvard Error Correcting Methods for Optical Telekommunications, *Proceedings of SPIE «Integrated Optics: Theory and Applications, Warsaw, September, 2005 : proceedings.* Warsaw, SPIE 2005, pp. 12.2–12.4.
13. Freeman R. Radio System Design for Telecommunications. New York, John Wiley & Sons, 1997, 880 p.

Received 19.03.2019.
Accepted 28.05.2019.

УДК 004.056

ПІДВИЩЕННЯ ПРИХОВАНОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ КОМБІНОВАНОГО ВИПАДКОВОГО КОДУВАННЯ

Корчинський В. В. – д-р техн. наук, доцент, доцент кафедри інформаційної безпеки і передачі даних Одеської національної академії зв'язку ім. О. С. Попова, Одеса, Україна.

Кільдішев В. Й. – канд. техн. наук, доцент, доцент кафедри інформаційної безпеки і передачі даних Одеської національної академії зв'язку ім. О. С. Попова, Одеса, Україна.

Голев Д. В. – старший викладач кафедри інформаційної безпеки і передачі даних Одеської національної академії зв'язку ім. О. С. Попова, Одеса, Україна.

Бердніков О. М. – аспірант кафедри інформаційної безпеки і передачі даних Одеської національної академії зв'язку ім. О. С. Попова, Одеса, Україна.

АНОТАЦІЯ

Актуальність. Розглянуто задачу підвищення прихованості передавання інформації на основі комбінованого випадкового кодування. Об'єктом дослідження є процеси інтеграції стохастичного, блокового і таймерного кодування. Метою роботи є розробка методу підвищення прихованості передавання на основі комбінованого каскадного кодування.

Метод. Запропоновано метод підвищення прихованості передавання інформації на основі комбінованого випадкового кодування з трьома ступенями кодових перетворювачів: внутрішнього, проміжного і зовнішнього. Внутрішній перетворювач реалізується на основі стохастичного кодування з різною кількістю випадкових кодових комбінацій.

Кількість випадкових комбінацій залежить від ймовірності появи символу алфавіту в тексті повідомлення. Інформаційна прихованість передавання буде забезпечуватися за рахунок зрівнювання ймовірностей появи кодових комбінацій з виходу статистичного кодера. Проміжне кодування реалізується за допомогою завадостійкого блокового коду. Інформаційна прихованість та завадостійкість забезпечується за рахунок збільшення довжини кодового блоку на кожному етапі кодування, що зменшує кодову швидкість. Для вирішення цієї проблеми використовуються зовнішній перетворювач на основі таймерного кодування. На цьому етапі двійкові комбінації перетворюються в таймерні сигнальні конструкції, що дозволяє реалізувати структурну прихованість, збільшити кодову швидкість та завадостійкість. При стохастичному і таймерному кодуванні використовуються кодові книги.

Результати. Розроблений метод комбінованого випадкового кодування дозволяє підвищити основні показники завадозахищенності: завадостійкість, інформаційну та структурну прихованість.

Висновки. Запропонований метод комбінованого випадкового кодування дозволяє усунути основні недоліки стохастичного кодування, в якому при виборі кількості випадкових кодових комбінацій не враховується ентропія дискретного джерела інформації. Для вирішення цієї проблеми запропоновано використовувати різну кількість випадкових комбінацій з урахуванням ймовірності появи символу алфавіту в тексті. З теоретичної точки зору це дозволить на виході статистичного кодера сформувати потік комбінацій з рівними ймовірностями появи. Також за рахунок використання таймерних сигналів вирішується проблема компенсації надлишковості, яка з'являється при стохастичному і завадостійкому кодуванні.

КЛЮЧОВІ СЛОВА: захист інформації, прихованість, кодування, таймерний сигнал, завадостійкість.

УДК 004.056

ПОВЫШЕНИЕ СКРЫТНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ КОМБИНИРОВАННОГО СЛУЧАЙНОГО КОДИРОВАНИЯ

Корчинский В. В. – д-р техн. наук, доцент, доцент кафедры информационной безопасности и передачи данных Одесской национальной академии связи им. А. С. Попова, Одесса, Украина.

DOI 10.15588/1607-3274-2019-3-12

Кильдишев В. Й. – канд. техн. наук, доцент, доцент кафедры информационной безопасности и передачи данных Одесской национальной академии связи им. А.С. Попова, Одесса, Украина.

Голев Д. В. – старший преподаватель кафедры информационной безопасности и передачи данных Одесской национальной академии связи им. А. С. Попова, Одесса, Украина.

Бердников А. М. – аспирант кафедры информационной безопасности и передачи данных Одесской национальной академии связи им. А. С. Попова, Одесса, Украина.

АННОТАЦИЯ

Актуальность. Рассмотрена задача повышения скрытности передачи информации на основе комбинированного случайного кодирования. Объектом исследования являются процессы интеграции стохастического, блокового и таймерного кодирования. Целью работы является разработка метода повышения скрытности передачи на основе комбинированного случайного кодирования.

Метод. Предложен метод повышения скрытности передачи информации на основе комбинированного случайного кодирования с тремя ступенями кодовых преобразователей: внутреннего, промежуточного и внешнего. Внутренний преобразователь реализуется на основе стохастического кодирования с различным количеством случайных кодовых комбинаций. Количество случайных комбинаций зависит от вероятности появления символа алфавита в тексте сообщения. Информационная скрытность передачи обеспечивается за счет уравнивания вероятностей появления кодовых комбинаций с выхода статистического кодера. Промежуточное кодирование реализуется с помощью помехоустойчивого блокового кода. Информационная скрытность и помехоустойчивость приводит к увеличению длины кодового блока на каждом этапе кодирования, что уменьшает кодовую скорость. Для решения этой проблемы используется внешний преобразователь на основе таймерного кодирования. На этом этапе двоичные комбинации преобразуются в таймерные сигнальные конструкции, что позволяет реализовать структурную скрытность передачи, увеличить кодовую скорость и повысить помехоустойчивость. При стохастическом и таймерном кодировании используются кодовые книги.

Результаты. Разработанный метод комбинированного случайного кодирования позволяет повысить основные показатели помехозащищённости: помехоустойчивость, информационную и структурную скрытность.

Выводы. Предложенный метод комбинированного случайного кодирования позволяет устранить основные недостатки стохастического кодирования, в котором при выборе количества случайных кодовых комбинаций не учитывается энтропия дискретного источника информации. Для решения этой проблемы предложено использовать различное количество случайных комбинаций с учетом вероятности появления символа алфавита в тексте. С теоретической точки зрения это позволяет на выходе статистического кодера сформировать поток комбинаций с равными вероятностями появления. За счет использования таймерных сигнальных конструкций решается проблема компенсации избыточности, которая появляется при стохастическом и помехоустойчивом кодировании.

КЛЮЧЕВЫЕ СЛОВА: защита информации, скрытность, кодирование, таймерный сигнал, помехоустойчивость.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Sha'ameri A. Z. Robust multiple channel scanning and detection of low probability of intercept (LPI) communication signals / A. Z. Sha'ameri, A. Kanaa // Defense S&T technical bulletin. − 2016. − Vol. 9, Issue 1. − P. 1−17.
2. MacKay D. Fountain codes. / D. MacKay // IEEE Proceedings Communications. − 2005. − Vol. 152, № 6. − P. 1062−1068.
3. Zakharchenko M. Integrated methods of information security in telecommunication systems / M. Zakharchenko, V. Korchynskii, V. Kildishev // 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library, Odessa, 11–15 September 2017 : proceeding. – Odessa: IEEE, 2017. – P. 78–81.
4. Information technology. Security techniques. Code of practice for information security controls. : ISO/IEC 27002:2013. [Effective from 2013-09-25]. – Geneva, ISO, 2013. – 80 p.
5. Glisic, S. Adaptive WCDMA: Theory and Practice / S. Glisic. – John Wiley & Sons, 2003. – 357 p.
6. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, Lviv-Slavske, 21–24 February 2012. – Lviv : Publishing House of Lviv Polyteshnic, 2012. – P. 317.
7. Development of the procedure for forming non-stationary signal structures based on multicomponent lfm signals / [V. Korchinskyi, M. Hadzhiyev, V. Kildishev et al.] // Eastern-European Journal of Enterprise Technologies. – 2018. – № 6/9 (96). – P. 29–37.
8. Assessing the Impact of the Noise on the Throughput Communication Channel with Timing Signals / [N. Zakharchenko, V. Korchinskiy, B. Radzimovsky et al.] // Eastern European Scientific Journal: AURIS Communications- und Verlagsgesellschaft mbH. – 2015. – № 4. – P. 209–214.
9. Maltsev G. N. Immunity and secrecy of transmitting information over radio channels based on combined random coding / G. N. Maltsev // Information control systems. − 2016. − Vol. 19, Issue 2. − P. 126−139.
10. Lu Yu. Stochastic Tools for Network Security: Anonymity Protocol Analysis and Network Intrusion Detection : thesis … doctor of philosophy / Lu Yu. – Clemson : Clemson University, 2012. – 101 p.
11. Zhu Y. Anonymity v.s. Information Leakage in Anonymity Systems / Y. Zhu, R. Bettati // Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, Columbus, June, 2005 : proceedings : – Texas: IEEE, 2005. – P. 86−97.
12. Banket V. Efficiency of Forvard Error Correcting Methods for Optical Telekommunications / V. Banket, F. Toporkov // Proceedings of SPIE «Integrated Optics: Theory and Applications, Warsaw, September, 2005 : proceedings : – Warsaw: SPIE 2005. – P. 12.2–12.4.
13. Freeman R. Radio System Design for Telecommunications / R. Freeman. – New York : John Wiley & Sons, 1997. – 880 p.

DOI 10.15588/1607-3274-2019-3-12