Algorithms for reliable permutation transmission protocols in noisy communication channels

Emil Faure[1,2,*,†], Alimzhan Baikenov[3,†], Artem Skutskyi[1,†], Denys Faure[4,†]
and Olga Abramkina[5,†]

[1] *Cherkasy State Technological University, 460 Shevchenko ave., 18006 Cherkasy, Ukraine*

[2] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3 M. Zaliznyaka str., 03142 Kyiv, Ukraine*

[3] *Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, 126 Baitursynov str., 050013 Almaty, Kazakhstan*

4 Odesa Polytechnic National University, 1 Shevchenko ave., 65044 Odesa, Ukraine

5 International University of Information Technology, 34A Manasa, 050040 Almaty, Kazakhstan

Abstract

The existing approaches to frame synchronization of non-separable factorial code, as well as the reliable transmission of its codewords, form the basis for creating a protocol for reliable permutation transmission in conditions of intense channel noise and, accordingly, of a high probability of bit error. This study considers a simplex data transmission system. For such a system, algorithms for frame synchronization of permutations, as well as reliable transmission of permutations have been developed, providing processing of fragments of bit sequences with a permutation length of M. A key feature of the proposed approaches is that they are designed for situations where the initial moment of the transmitter's syncword transmission is unknown. It has been shown that to ensure the required level of false synchronization, the number of K blocks, each consisting of l fragments, needs to be increased. An assessment of the probabilistic indicators of the process of transmission and reception of information has been performed. Computer simulation modeling has been carried out, confirming the theoretical results.

Keywords

permutation, synchronization, error correction, security, reliability, factorial coding, protocol, data processing algorithm

1. Introduction

The theory of non-separable factorial data coding [1, 2] allows using permutations as a transport mechanism in communication systems with short packets [3–5], and also to implement joint protection of transmitted data from communication channel errors and unauthorized access [6].

Paper [1] shows that the codewords of a non-separable factorial code belong to a subset of the set of permutations $\{\pi\}$ of length M. The permutation elements are encoded by a fixed-length binary code with a codeword length $l_r = \lceil \log_2 M \rceil$. Then the syncword length is equal to $n = l_r \cdot M$.

Due to the redundancy of the information carriers, permutations, used, and non-separable factorial codes allow detecting and correcting communication channel errors [7–10]. In addition, the permutation structure creates conditions for the code frame synchronization using the operating signal.

At the same time, modern conditions dictate the need [3, 11–14] to achieve high-reliability indicators in difficult signal propagation conditions [15–18]. Three-pass cryptographic protocols [19–22], in particular, based on permutations [23], deserve special attention in this context.

Previously conducted studies on the possibility of using non-separable factorial coding in conditions of a high probability of bit error in a communication channel made it possible to develop:

- Methods of frame synchronization for non-separable factorial codes [24–27].
- Method for reliable permutation transmission in short-packet communication systems [28].

The developed approaches and methods are effective. At the same time, the frame synchronization methods are based on knowledge of the initial moment of the syncword bits

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine

* Corresponding author.
† These authors contributed equally.
e.faure@chdtu.edu.ua (E. Faure);
a.baikenov@aues.kz (A. Baikenov);
a.skutskyi@ chdtu.edu.ua (A. Skutskyi);
highdensityarts@gmail.com (D. Faure);
o.manankova@iitu.edu.kz (O. Abramkina)

0000-0002-2046-481X (E. Faure);
0000-0002-6490-3159 (A. Baikenov);
0000-0002-8632-1176 (A. Skutskyi);
0009-0002-9741-6282 (D. Faure);
0000-0003-0137-1252 (O. Abramkina)

reception, which is not always possible. In addition, the joint use of synchronization and reliable transmission procedures in one protocol has not been studied.

The purpose of this study is to develop algorithms for a protocol of reliable transmission of permutations for simplex data transmission systems with non-separable factorial coding under conditions of high noise intensity in the communication channel.

2. Sliding window algorithm for a frame synchronization system

The first step of the protocol involves establishing frame synchronization for the transmitted permutations. For this purpose, a frame synchronization method [25, 26] will be used. This method employs as a syncword a permutation with the maximum value of the minimum Hamming distance from its binary representation to all its circular shifts.

The receiver accumulates K blocks of l fragments of M symbols from the communication channel, followed by majority [29, 30] and correlation processing [31–33] of the accumulated fragments. The values of K and l change according to the methodology defined in [26]. A pre-established minimum threshold for the probability of correct synchronization P_{true} determines the sufficient number of accumulated fragments.

The frame synchronization method proposed in [25, 26] involves the sequential transmission of a syncword into the communication channel. For example, for $M = 8$, such a syncword is the permutation $\pi = (000,001,111,011,010,101,100,110)$, up to its circular shift by a number of bits that is a multiple of $l_r = 3$, bit inversion, and the reverse order of their sequence.

Let us assume that high noise intensity results in the receiver being unable to determine the initial moment of the transmitter's syncword. In this case, the algorithm for identifying the boundaries of the syncword is modified slightly.

Recall that according to [26], the sufficient number of accumulated fragments to ensure the minimum value of the probability of correct synchronization $P_{true\_\min}$ is chosen as the minimum value of l, at which the probability of correct synchronization for $K = 1$ is not less than the specified $P_{true\_\min}$. Paper [26] denotes this value as $l_{\max}(1)$. In this paper, we will denote it as $l_{\max}$.

Based on the above and the fact that the initial moment of syncword transmission is unknown, the receiver will use a sliding window with a width of $l_{\max}$ fragments to search for synchronization (Figure 1).

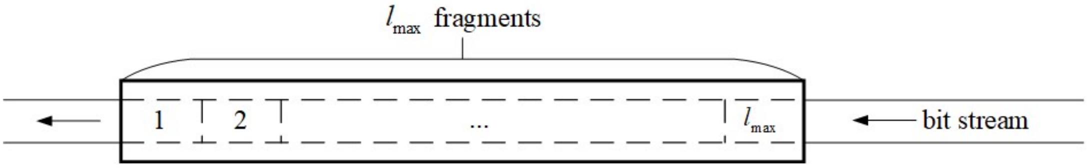


Figure 1: Diagram of the use of a sliding window consisting of $l_{\max}$ fragments

Thus, the receiver, shifting the sliding window 1 bit to the right, continuously analyses $l_{\max}$ fragments received from the communication channel, attempting to establish frame synchronization. It is evident that, in this case, the dynamic adjustment of K and l values is meaningless.

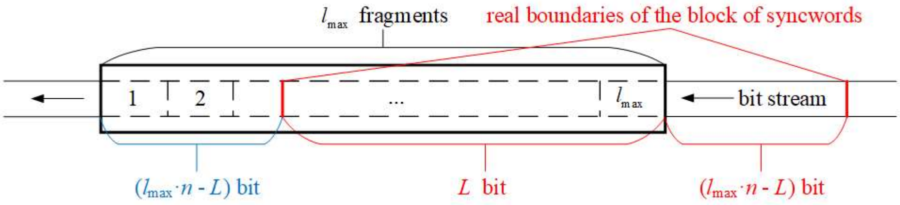
The mathematical model of the syncword reception process will also differ from that presented in [26].

2.1. Probabilistic metrics of the frame synchronization system

The probabilities of correct and false synchronization depend on the probability of bit error p_0^* after majority processing of $l_{\max}$ received fragments. However, the receiver's lack of knowledge about the initial moment of syncword transmission leads to the following.

Since the receiver has to constantly "listen" to the channel, in the absence of a signal from the transmitter, only noise is present in the sliding window. Accordingly, the probability of bit error is equal to 0.5

After the transmitter begins to transmit service signals for the clock (not considered in this study) and frame synchronization into the communication channel, fragments with syncwords begin to appear in the sliding window of the receiver synchronization system (Figure 2).



$l_{\max}$ fragments
real boundaries of the block of syncwords
1
2
...
$l_{\max}$
bit stream
$(l_{\max} \cdot n - L)$ bit
L bit
$(l_{\max} \cdot n - L)$ bit

Figure 2: Diagram of the stage of filling the sliding window with data from the source

Let there be L bits of the source syncword in the sliding window (Figure 2). To provide a clearer view of the majority reception process of the accumulated bits, we represent the fragments in the sliding window as shown in Figure 3. The shaded areas contain only noise bits (error probability is 0.5), while the unshaded areas contain bits of the source syncword (with an error probability of p_0).

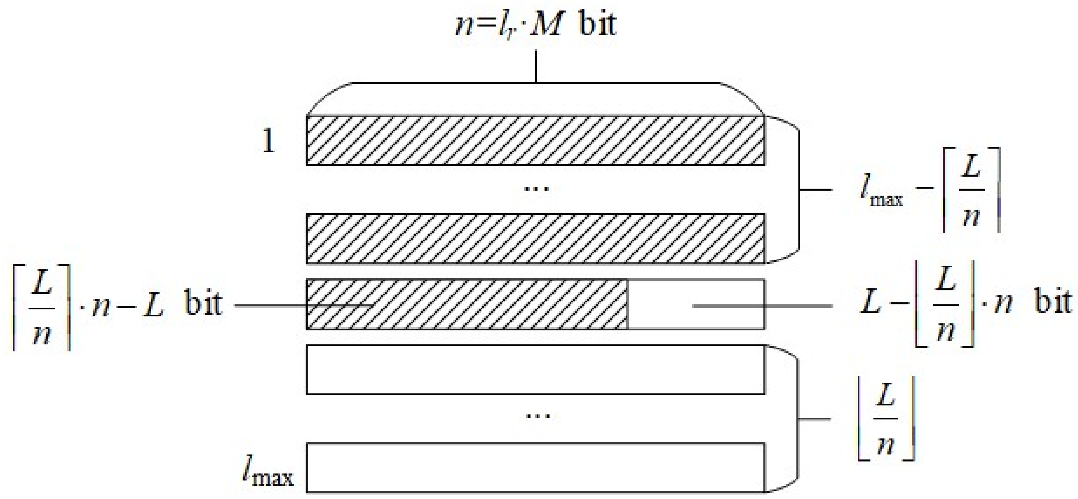

$n = l_r \cdot M$ bit
1
...
$l_{\max}$
$l_{\max} - \left\lceil \frac{L}{n} \right\rceil$
$\left\lceil \frac{L}{n} \right\rceil \cdot n - L$ bit
$L - \left\lfloor \frac{L}{n} \right\rfloor \cdot n$ bit
...
$\left\lfloor \frac{L}{n} \right\rfloor$

Figure 3: Diagram of majority reception of accumulated bits

From the accumulated fragments, a refined sequence R is computed by the majority, in which some errors (if any) are corrected.

It should be noted that the number of bits of the source syncword present in the sliding window of the receiver's synchronization system may not be a multiple of the codeword length $l_r = \lceil \log_2 M \rceil$, as demonstrated in Figure 3. Therefore, the probability of bit error in the refined sequence after majority processing of $l_{\max}$ received fragments can be estimated as follows:

for $L < n \cdot \frac{l_{\max}+3}{2}$:

$$p_0^* \le \sum_{i=0}^{l_1} \left(\begin{array}{l} C_{l_1}^i p_0^i (1-p_0)^{l_1-i} \times \\ \times \sum\limits_{j=(l_{\max}+1)/2-i}^{l_{\max}-l_1} C_{l_{\max}-l_1}^j (0.5)^{l_{\max}-l_1} \end{array} \right) \qquad (1)$$

and for $L \ge n \cdot \frac{l_{\max}+3}{2}$:

$$p_0^* \le \sum_{i=0}^{l_{\max}-l_1} \left(\begin{array}{l} C_{l_{\max}-l_1}^i (0.5)^{l_{\max}-l_1} \times \\ \times \sum\limits_{j=(l_{\max}+1)/2-i}^{l_1} C_{l_1}^j p_0^j (1-p_0)^{l_1-j} \end{array} \right), \qquad (2)$$

where $l_1 = \left\lfloor \frac{L}{n} \right\rfloor$ is the number of complete fragments containing only bits of the source syncword (which may be affected by errors).

Estimates (1) and (2) are formed by replacing the fragment that contains noise bits and bits of the syncword with a fragment that contains only noise bits, as well as taking into account that $p_0 < 0.5$.

Paper [34] defines that for $M = 8$ and $p_0 = 0.4$, the value of $l_{\max} = 75$. For parameters $M = 8$ and $p_0 = 0.4$, the graph showing the dependence of the estimated probability of bit error in the refined sequence R on the value of $L \in [0; 75 \cdot 24]$ is presented in Figure 4.

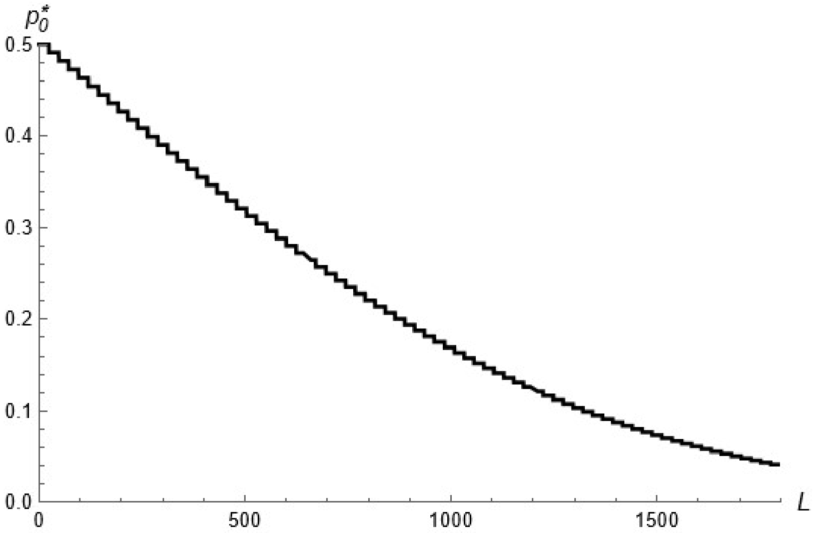


Figure 4: The estimated probability of bit error in the refined sequence on the number of syncword bits in the sliding window for $M = 8$ and $p_0 = 0.4$

The graph has a stepped nature due to the simplifying upper estimates (1) and (2). At the same time, at $L=0$, the value is $p_0^*=0.5$, and at $L=1800$, the value is $p_0^*=0.0396$.

To calculate the exact value of the obtained probability of bit error in the refined sequence, the following statement can be used.

Theorem 1. The probability of bit error in the refined sequence R after receiving L bits of the source syncword is equal to:

1. for $L \le n \cdot \frac{l_{\max}+1}{2}$:

$$p_0^* = \left(1 + l_1 - \frac{L}{n}\right) \times \sum_{i=0}^{l_1} \left(\begin{array}{l} C_{l_1}^i p_0^i \left(1-p_0\right)^{l_1-i} \times \\ \times \sum\limits_{j=(l_{\max}+1)/2-i}^{l_{\max}-l_1} C_{l_{\max}-l_1}^j \left(0.5\right)^{l_{\max}-l_1} \end{array} \right) + \left(\frac{L}{n} - l_1\right) \times \sum_{i=0}^{l_1+1} \left(\begin{array}{l} C_{l_1+1}^i p_0^i \left(1-p_0\right)^{l_1+1-i} \times \\ \times \sum\limits_{j=(l_{\max}+1)/2-i}^{l_{\max}-l_1-1} C_{l_{\max}-l_1-1}^j \left(0.5\right)^{l_{\max}-l_1-1} \end{array} \right); \quad , \qquad (3)$$

2. for $L > n \cdot \frac{l_{\max}+1}{2}$:

$$p_0^* = \left(\frac{L}{n} - l_1\right) \times \sum_{i=0}^{l_{\max}-l_1-1} \left(\begin{array}{l} C_{l_{\max}-l_1-1}^i \left(0.5\right)^{l_{\max}-l_1-1} \times \\ \times \sum\limits_{j=(l_{\max}+1)/2-i}^{l_1+1} C_{l_1+1}^j p_0^j \left(1-p_0\right)^{l_1+1-j} \end{array} \right) + \left(1 + l_1 - \frac{L}{n}\right) \times \sum_{i=0}^{l_{\max}-l_1} \left(\begin{array}{l} C_{l_{\max}-l_1}^i \left(0.5\right)^{l_{\max}-l_1} \times \\ \times \sum\limits_{j=(l_{\max}+1)/2-i}^{l_1} C_{l_1}^j p_0^j \left(1-p_0\right)^{l_1-j} \end{array} \right). \quad , \qquad (4)$$

Proof.

We will use Figure 3. Since the number of bits of the source syncword L in the sliding window is generally not a multiple of the fragment length $l_r \cdot M$, in $L-\left\lfloor \frac{L}{n} \right\rfloor \cdot n$ cases out of n в the formation of a bit based on the majority principle involves $\left\lfloor \frac{L}{n} \right\rfloor + 1$ bits of the source syncword and $l_{\max} - \left\lfloor \frac{L}{n} \right\rfloor - 1$ bits of noise. Accordingly, in $n - L + \left\lfloor \frac{L}{n} \right\rfloor \cdot n$ cases out of n the formation of a bit based on the majority principle involves $\left\lfloor \frac{L}{n} \right\rfloor$ bits of the source syncword and $l_{\max} - \left\lfloor \frac{L}{n} \right\rfloor$ bits of noise. Consider that a bit error occurs when the number of errors in the corresponding bits of the accumulated fragments is not less than the value of $\frac{l_{\max}+1}{2}$. Then we can obtain the necessary expressions (3) and (4) for the bit error probability for $L \le n \cdot \frac{l_{\max}+1}{2}$ and $L > n \cdot \frac{l_{\max}+1}{2}$ respectively. ■

The graph showing the dependence of the probability of bit error in the refined sequence R on the value of $L \in [0, 75 \cdot 24]$ at $M=8$ and $p_0 = 0.4$ is presented in Fig. 5.

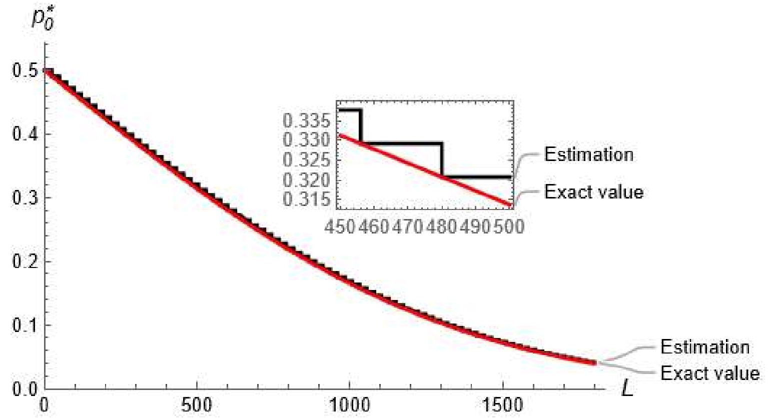


Figure 5: The probability of bit error in the refined sequence on the number of syncword bits in the sliding window for $M=8$ and $p_0=0.4$

To estimate the probabilities of correct and false synchronization, we will use the expressions defined in [26]:

$$P_{true}\left(n,d_{lim},p_0,L\right) \approx \sum_{v=0}^{d_{lim}} C_n^v \left(p_0^*\right)^v \left(1-p_0^*\right)^{n-v} \tag{5}$$

,

$$P_{false}\left(n,d_{lim},p_0,L\right) \approx$$

$$\approx \sum_{j=1}^{n-1} \left(\sum_{v=d_{ij}-d_{lim}}^{d_{ij}} C_{d_{ij}}^v \left(\sum_{w=0}^{v-d_{ij}+d_{lim}} \begin{matrix} C_{n-d_{ij}}^w \left(p_0^*\right)^{v+w} \times \\ \times\left(1-p_0^*\right)^{n-(w+v)} \end{matrix} \right) \right) \tag{6}$$

.

For the syncword $\pi = (000,001,111,011,010,101,100,110)$ expression (5) takes the form: $P_{true}\left(24,5,p_0,L\right) \approx \sum_{v=0}^{5} C_{24}^v \left(p_0^*\right)^v \left(1-p_0^*\right)^{24-v}$, and **Error! Reference source not found.** transforms to

$$P_{false}\left(24,5,p_0,L\right) \approx 19\sum_{v=7}^{12} C_{12}^v \left(\sum_{w=0}^{v-7} \begin{matrix} C_{12}^w \left(p_0^*\right)^{v+w} \times \\ \times\left(1-p_0^*\right)^{24-v-w} \end{matrix} \right) +$$

$$+2\sum_{v=9}^{14} C_{14}^v \left(\sum_{w=0}^{v-9} C_{10}^w \left(p_0^*\right)^{v+w} \left(1-p_0^*\right)^{24-v-w} \right) +$$

$$+2\sum_{v=11}^{16} C_{16}^v \left(\sum_{w=0}^{v-11} C_{8}^w \left(p_0^*\right)^{v+w} \left(1-p_0^*\right)^{24-v-w} \right).$$

The graphs of functions (5) and (6) as a function of L at $M = 8$ and $p_0 = 0.4$ are presented in **Error! Reference source not found.** and Figure 7.

Figure 6 and Figure 7 show that the probability of correct synchronization increases from 0.0033 for $L = 0$ to 0.9997 for $L = 1800$, while the probability of false synchronization decreases from 0.076 for $L = 0$ to $1.198 \cdot 10^{-6}$ for $L = 1800$.

For experimental confirmation of the dependencies $P_{true}\left(24,5,0.4,L\right)$ and $P_{false}\left(24,5,0.4,L\right)$, a computer simulation modeling of the frame synchronization system operation process was performed and the relative frequencies $W_{true}\left(24,5,0.4,L\right)$ and $W_{false}\left(24,5,0.4,L\right)$ of both correct and false synchronization were determined. For each value, 1000 tests were performed. The graphs of the studied dependencies are presented in Figure 8 and Figure 9.

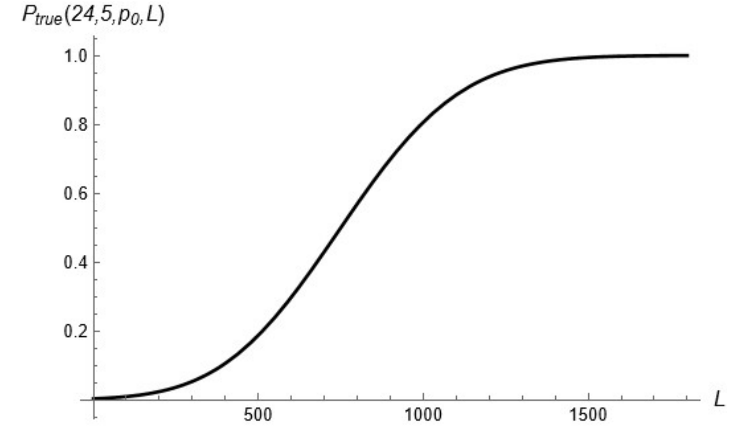


Figure 6: Estimated probability of correct synchronization on the number of syncword bits in the sliding window for $M = 8$ and $p_0 = 0.4$

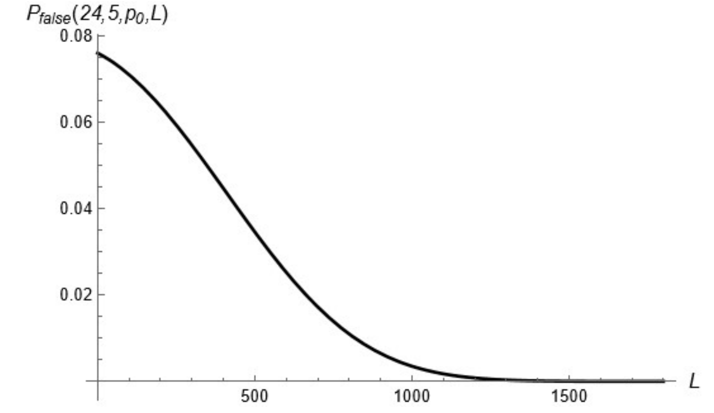


Figure 7: Estimated probability of false synchronization on the number of syncword bits in the sliding window for $M = 8$ and $p_0 = 0.4$

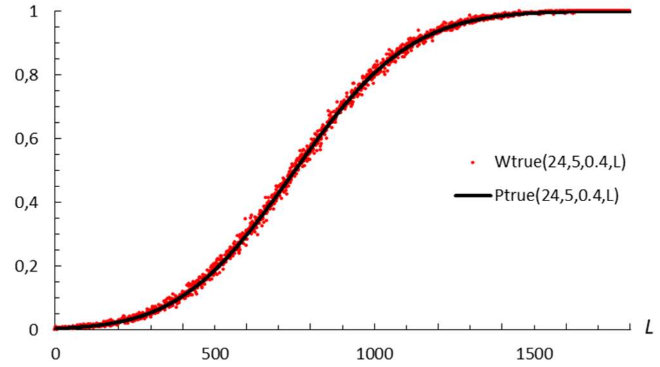


Figure 8: Dependencies $P_{true}(24,5,0.4,L)$ and $W_{true}(24,5,0.4,L)$

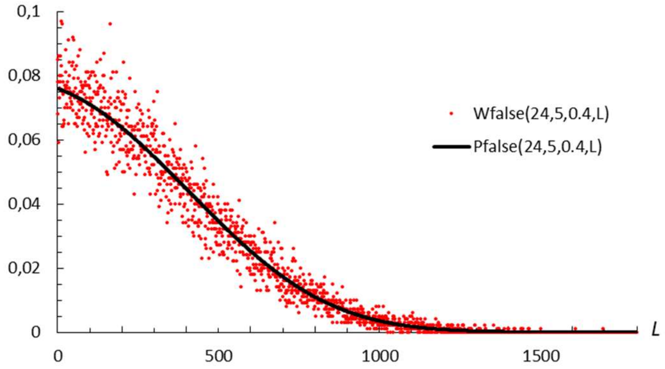


Figure 9: Dependencies $P_{false}(24,5,0.4,L)$ and $W_{false}(24,5,0.4,L)$

A comparative visual assessment of $P_{true}(24,5,0.4,L)$ and $W_{true}(24,5,0.4,L)$, as well as $P_{false}(24,5,0.4,L)$ and $W_{false}(24,5,0.4,L)$, indicates the correctness of expressions (5) and (6), as well as the adequacy of the developed model.

By analogy with [26]:

- The probability P_{true_final} of correct synchronization after receiving L bits of the syncword is estimated below by the probability:
$$P_{true\_final}(n,d_{lim},p_0,L) \geq P_{true}(n,d_{lim},p_0,L) \tag{7}$$;
- The probability P_{true_final} of false synchronization after receiving L bits of the syncword is estimated from above by the sum of the probabilities of false synchronization for all values of the accumulated syncword bits less than L:
$$P_{true\_final}(n,d_{lim},p_0,L) \geq P_{true}(n,d_{lim},p_0,L) \tag{8}$$.

Thus, the probability of false synchronization turns out to be unacceptably high. Figure 10 presents the results of an experimental study of the relative frequency of true W_{true} and false W_{false} synchronization for $M=8$ and $p_0=0.4$.

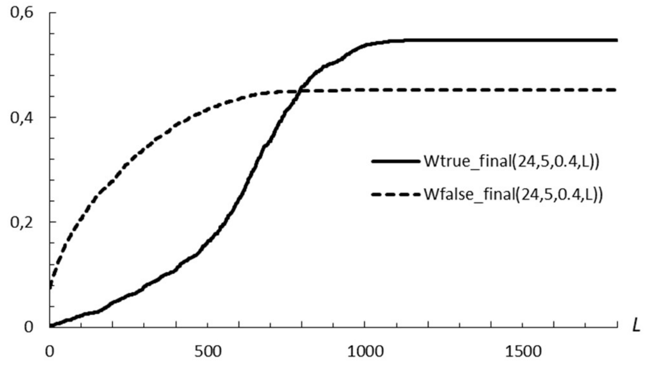


Figure 10: Relative frequency of correct and false synchronization on the number of syncword bits in the sliding window for $M=8$ and $p_0=0.4$

2.2. Parameters of the algorithm for reducing the probability of false synchronization

One way to reduce the probability of false synchronization is to increase the number of K blocks of l fragments.

The approach to increasing the K value [26] involves receiving K blocks consisting of l fragments of n bits. For each block, the refined sequences R_k, $k \in [1, K]$ are independently calculated. If all sequences R_k, $k \in [1, K]$ correspond to the same syncword shift, the decision device of the frame synchronization system decides to establish synchronization.

According to [26, 34], the probability of false synchronization for K blocks of l fragments

$$P_{false}(n, d_{lim}, p_0, L, l, K) = \\ = \sum_{j=1}^{n-1} \left(\sum_{v=d_{ij}-d_{lim}}^{d_{ij}} C_{d_{ij}}^{v} \sum_{w=0}^{v-d_{ij}+d_{lim}} \begin{matrix} C_{n-d_{ij}}^{w} \left(p_0^*\right)^{v+w} \times \\ \times \left(1-p_0^*\right)^{n-v-w} \end{matrix} \right)^{K} \quad (9)$$

monotonically decreases with the increase in both K and l values. On the other hand, the probability of correct synchronization

$$P_{true}(n, d_{lim}, p_0, L, l, K) = \\ = P_{true}^{K}(n, d_{lim}, p_0, L) = \\ = \left(\sum_{v=0}^{d_{lim}} C_n^v \left(p_0^*\right)^v \left(1-p_0^*\right)^{n-v} \right)^{K} \quad (10)$$

also monotonically decreases with the increase in K, but increases with the increase in l. At the same time, $L \in [0; l_r \cdot M \cdot l \cdot K]$, and the probability of bit error in the refined sequences R_k after receiving L syncword bits from the source can be estimated by modifying expressions (3) and (4) as follows:

3. for $\left\lfloor \frac{L}{K} \right\rfloor \le n \cdot \frac{l+1}{2}$:

$$p_0^* \le \left(1 + l_1 - \left\lfloor \frac{L}{K} \right\rfloor \cdot \frac{1}{n}\right) \times \\ \times \sum_{i=0}^{l_1} \left(\begin{matrix} C_{l_1}^{i} p_0^i (1-p_0)^{l_1-i} \times \\ \times \sum\limits_{j=(l+1)/2-i}^{l-l_1} C_{l-l_1}^{j} (0.5)^{l-l_1} \end{matrix} \right) + \\ + \left(\left\lfloor \frac{L}{K} \right\rfloor \cdot \frac{1}{n} - l_1 \right) \times \\ \times \sum_{i=0}^{l_1+1} \left(\begin{matrix} C_{l_1+1}^{i} p_0^i (1-p_0)^{l_1+1-i} \times \\ \times \sum\limits_{j=(l+1)/2-i}^{l-l_1-1} C_{l-l_1-1}^{j} (0.5)^{l-l_1-1} \end{matrix} \right); \quad (11)$$

4. for $\left\lfloor \frac{L}{K} \right\rfloor > n \cdot \frac{l+1}{2}$:

$$p_0^* \le \left(\left\lfloor \frac{L}{K} \right\rfloor \cdot \frac{1}{n} - l_1 \right) \times \\ \times \sum_{i=0}^{l-l_1-1} \left(\begin{matrix} C_{l-l_1-1}^{i} (0.5)^{l-l_1-1} \times \\ \times \sum\limits_{j=(l+1)/2-i}^{l_1+1} C_{l_1+1}^{j} p_0^j (1-p_0)^{l_1+1-j} \end{matrix} \right) + \\ + \left(1 + l_1 - \left\lfloor \frac{L}{K} \right\rfloor \cdot \frac{1}{n}\right) \times \\ \times \sum_{i=0}^{l-l_1} \left(\begin{matrix} C_{l-l_1}^{i} (0.5)^{l-l_1} \times \\ \times \sum\limits_{j=(l+1)/2-i}^{l_1} C_{l_1}^{j} p_0^j (1-p_0)^{l_1-j} \end{matrix} \right), \quad (12)$$

where $l_1 = \left\lfloor \frac{L}{K \cdot n} \right\rfloor$.

To ensure that the probability of false synchronization does not exceed its threshold value $P_{false\_\max}$, that the probability of correct synchronization is at least its threshold value $P_{true\_\min}$, and that correct synchronization occurs as quickly as possible, it is necessary to determine a pair of K and l values, for which $P_{false\_final}(n, d_{lim}, p_0, L, l, K) \le P_{false\_\max}$, $P_{true\_final}(n, d_{lim}, p_0, L, l, K) \ge P_{true\_\min}$, and $K \cdot l$ takes its minimum value. In this case, $P_{false\_final}(n, d_{lim}, p_0, L, l, K)$ and $P_{true\_final}(n, d_{lim}, p_0, L, l, K)$ are estimated as follows:

$$P_{false\_final}(n, d_{lim}, p_0, L, l, K) \le \\ \le \sum_{j=0}^{L} P_{false}(n, d_{lim}, p_0, j, l, K); \quad (13)$$

$$P_{true\_final}(n, d_{lim}, p_0, L, l, K) \ge \\ \ge P_{true}(n, d_{lim}, p_0, L, l, K). \quad (14)$$

Let $l_{true\_\min}(K)$ be the minimum number of fragments in each of the K blocks, at which $P_{true\_final}(n, d_{lim}, p_0, L_{\max}(K), l_{true\_\min}(K), K) \ge P_{true\_\min}$, $L_{\max}(K) = l_r \cdot M \cdot l_{true\_\min}(K) \cdot K$. Then the task of determining the pair of $(K; l)$ values consists of the following:

5. n, d_{lim}, p_0 values are specified, and $K = 1$ is accepted;
6. $l_{true\_\min}(K)$ value is calculated to satisfy $P_{true\_final}(n, d_{lim}, p_0, L_{\max}(K), l_{true\_\min}(K), K) \ge$ $\ge P_{true\_\min}$, where $L_{\max}(K) = l_r \cdot M \cdot l_{true\_\min}(K) \cdot K$;
7. if $P_{false\_final}(n, d_{lim}, p_0, L_{\max}(K), l_{true\_\min}(K), K) \le$ $\le P_{false\_\max}$ is satisfied, the pair of $(K; l_{true\_\min}(K))$ values can be used as necessary parameters for the synchronization procedure;
8. if $P_{false\_final}(n, d_{lim}, p_0, L_{\max}(K), l_{true\_\min}(K), K) >$ $> P_{false\_\max}$, an algorithm for determining $(K; l)$ transits to step 2, incrementing the value of K by one.

We will compute the $l_{true\_\min}\left(K\right)$ values for $K=1,2,3,\ldots$ for the specified parameters and summarize the results in Table 1. In this case, we will assume $P_{true\_\min}=0.9997$, $P_{false\_\max}=0.0003$.

Table 1
Characteristics of the algorithm for reducing the probability of false synchronization

Characteristics	**Value**			
K	1	2	3	4
$l_{true\_\min}\left(K\right)$	75	81	83	85
$P_{false\_final}\left(n,d_{lim},p_0,L_{\max}\left(K\right),l_{true\_\min}\left(K\right),K\right)$	1	0.182	$7.4\cdot10^{-4}$	$2.9\cdot10^{-6}$

Graphs of dependencies $P_{false\_final}\left(n,d_{lim},p_0,L,l_{true\_\min}\left(K\right),K\right)$ P_{false_final} on L for various K, presented in Fig. 11, indicate the behaviour of the estimate (13) and demonstrate the numerical values of the estimate (13) given in Table 9.

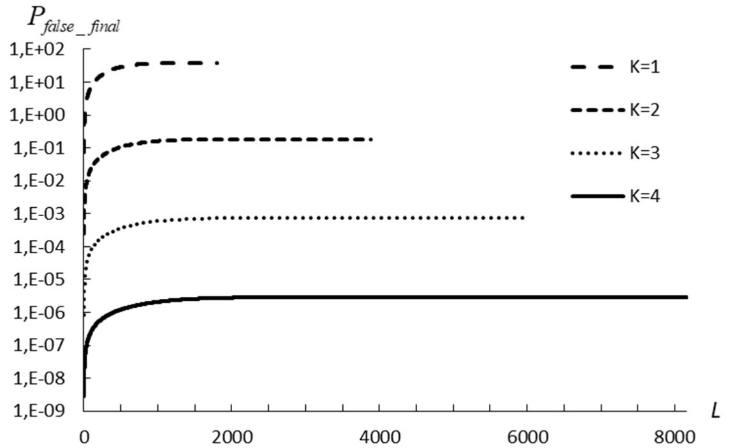


Figure 11: Estimation of the probability of false synchronization on the number of syncword bits in the sliding window for $M=8$ and $p_0=0.4$ for different K values

Based on the values presented in Table 1, for the considered example with $M=8$, $p_0=0.4$, $P_{true\_\min}=0.9997$, and $P_{false\_\max}=0.0003$, it is sufficient to choose the $K=4$ value.

Another potential method for reducing the probability of false synchronization could be to decrease the maximum distance *dlim* to the syncword shifts used in identifying the refined sequence *R*. However, reducing *dlim* leads to a decrease in the probability of correct synchronization, which necessitates increasing the accumulation coefficient *l*. This approach may be effective; however, it is not considered in this paper.

3. Algorithm for reliable transmission of permutations

Frame synchronization establishment initiates the next stage of the protocol, the reliable transmission of permutations.

The algorithm for reliable transmission of permutations based on method [28] consists of the following:

1. The transmitter sends into the communication channel a permutation-word *W* consisting of *N* symbols-letters *Lj*, 1 ≤ *j* ≤ *N*. Each letter is a circular bit shift of permutation *π* of length *M*, which has the maximum value of the minimum Hamming distance from its *n*-bit binary representation to all its circular shifts.
2. Analogous to the procedure of frame synchronization, for each letter, the transmitter sends and the receiver receives, accumulates, and analyses *l* fragments of *n*-bit each.
3. For each letter, the refined sequence *Rj*, *j* ∈ [1,*N*], is computed using the majority processing of the received bits.
4. For each refined sequence *Rj*, the Hamming distances to the letters used by the source are calculated. If the distance does not exceed *dlim*, the *j*th symbol of the word *W* is associated with the corresponding alphabet letter.
5. If the received word is a permutation of the letters of the alphabet used by the source, and this permutation is used by the source, the word is accepted, and the process of recognizing the next word begins.

It should be noted that the function $P_{true\_final}\left(n,d_{lim},p_0,L,l,K\right)$ monotonically increases with an increase in L and, for example, at $L\geq4432$ the value is $P_{true}\left(24,5,0.4,L,85,4\right)\geq0.5$, while at $L\geq5640$ the value is $P_{true}\left(24,5,0.4,L,85,4\right)\geq0.9$. Considering that $P_{false\_final}\left(24,5,0.4,L,85,4\right)\leq2.9\cdot10^{-6}$, this leads to the conclusion that there will be a 90% probability of correct synchronization being established after receiving 5640 fragments containing bits of the source's synchronization word. Since 8160 − 5640 = 2520, n = 24, in 90% of cases, the reliable reception procedure for the permutation, which follows the synchronization procedure and is initiated by the fact of establishing synchronization, will utilize the shifted boundaries of the data block used for transmitting a single permutation (synchronization was completed earlier, the recognition of the permutation began sooner, while the synchronization words are still being transmitted in the channel).

Such desynchronization leads to a decrease in the efficiency of the permutation recognition procedure, which needs to be compensated for with additional procedures. The development of such procedures requires separate research and is beyond the scope of this study.

4. Conclusions

The completed study has led to the development of algorithms for the protocol of reliable permutation transmission for simplex data transmission systems with non-separable factorial coding under conditions of high noise intensity in the communication channel. To achieve this, it was considered the problem of joint application of the frame synchronization algorithm, which uses as a syncword a permutation with the maximum value of the minimum Hamming distance from its binary representation to all its circular shifts, as well as the reliable permutation transmission algorithm. The adaptation of the frame synchronization algorithm for simplex communication systems with an unknown moment of the start of receiving syncwords from the transmitter has necessitated the use of a sliding window.

An example of the reliable permutation transmission protocol algorithms has been considered for a communication channel error probability $p_0 = 0.4$. The defined parameters of the proposed algorithms made it possible to conduct a simulation of the frame synchronization process. The obtained simulation results confirmed the theoretical estimates.

The identified problem areas related to the detection of syncword and data word boundaries have allowed for the formulation of pathways for further research.

Acknowledgments

This research was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23489168).

References

[1] E. V. Faure, Factorial Coding with Data Recovery, Bulletin of Cherkasy State Technological University, 2 (2016) 33–39.

[2] J. S. Al-Azzeh, et al.,, Telecommunication Systems with Multiple Access Based on Data Factorial Coding, International Journal on Communications Antenna and Propagation (IRECAP), 10(2) (2020) 102–113. doi: 10.15866/irecap.v10i2.17216.

[3] A.-S. Bana, et al., Short Packet Structure for Ultra-Reliable Machine-Type Communication: Tradeoff between Detection and Decoding, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2018) 6608–6612. doi: 10.1109/ICASSP.2018.8461650.

[4] C. Feng, H. Wang, Secure Short-Packet Communications at the Physical Layer for 5G and Beyond (2021). doi: 10.48550/arXiv.2107.05966.

[5] C. Feng, H.-M. Wang, H. V. Poor, Reliable and Secure Short-Packet Communications, IEEE Trans. Wireless Commun. 21(3) (2022) 1913–1926. doi: 10.1109/TWC.2021.3108042.

[6] R. Aleksieieva, et al., Software Tool for Ensuring Data Integrity and Confidentiality Through the Use of Cryptographic Mechanisms, in: 5th International Workshop on Modern Machine Learning Technologies and Data Science, vol. 3426 (2023) 259–273.

[7] E. V. Faure, Factorial Coding with Error Correction, Radio Electronics, Computer Science, Control, 3 (2017) 130–138. doi: 10.15588/1607-3274-2017-3-15.

[8] O. A. Borysenko, et al., Noise-Immune Transfer of Decimal Data with Protection Based on Permutations, in: IEEE 13th International Conference on Electronics and Information Technologies (ELIT) (2023) 248–251. doi: 10.1109/ELIT61488.2023.10310685.

[9] O. Borysenko, Protection of Numerical Information Based on Permutations, in: 3rd International Scientific and Practical Conference "Information Security and Information Technologies", vol. 3200 (2021) 62–67.

[10] O. Borysenko et al., Factorial Numbers and Their Practical Applications, Appl. Sci. 14(19) (2024) 8588. doi: 10.3390/app14198588.

[11] B. Lee, et al., Packet Structure and Receiver Design for Low Latency Wireless Communications with Ultra-Short Packets, IEEE Trans. Commun. 66(2) (2018) 796–807. doi: 10.1109/TCOMM.2017.2755012.

[12] H. Lee, Y.-C. Ko, Physical Layer Enhancements for Ultra-Reliable Low-Latency Communications in 5G New Radio Systems, IEEE Comm. Stand. Mag. 5(4) (2021) 112–122. doi: 10.1109/MCOMSTD.0001.2100002.

[13] J. Park, et al., Extreme Ultra-Reliable and Low-Latency Communication, Nat Electron, 5(3) (2022) 133–141. doi: 10.1038/s41928-022-00728-8.

[14] Y. Li, et al., Unmanned Aerial Vehicle-Aided Edge Networks with Ultra-Reliable Low-Latency Communications: A digital twin approach, IET Signal Processing, 16(8) (2022) 897–908. doi: 10.1049/sil2.12128.

[15] A. Traßl, et al., Outage prediction for ultra-reliable low-latency communications in fast fading channels, J. Wireless Com. Netw. 2021(92) (2021). doi: 10.1186/s13638-021-01964-w.

[16] K. Wang, et al., Packet Error Probability and Effective Throughput for Ultra-Reliable and Low-Latency UAV Communications, IEEE Trans. Commun. 69(1) (2021). doi: 10.1109/TCOMM.2020.3025578.

[17] R. Odarchenko, Evaluation and Improvement of QoE and QoS Parameters in Commercial 5G Networks: 5G-TOURS Approach, IJC (2023) 462–474. doi: 10.47839/ijc.22.4.3353.

[18] X. Li, et al., Blocklength Allocation and Power Control in UAV-Assisted URLLC System via Multi-agent Deep

Reinforcement Learning, Int. J. Comput. Intell. Syst. 17(138) (2024). doi: 10.1007/s44196-024-00530-8.

[19] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York: Wiley (1996).

[20] D. M. Nguyen, S. Kim, A Quantum Three Pass Protocol with Phase Estimation for Many Bits Transfer, International Conference on Advanced Technologies for Communications (ATC) (2019) 129–132. doi: 10.1109/ATC.2019.8924514.

[21] A. Badawi, M. Zarlis, S. Suherman, Impact Three Pass Protocol Modifications to key Transmission Performance, J. Phys.: Conf. Ser. 1235 (2018). doi: 10.1088/1742-6596/1235/1/012050.

[22] A. Moldovyan, D. Moldovyan, N. Moldovyan, Post-Quantum Commutative Encryption Algorithm, Comput. Sci. J. Moldova, 81(3) (2019) 299–317.

[23] A. Shcherba, E. Faure, O. Lavdanska, Three-Pass Cryptographic Protocol Based on Permutations, IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT) (2020) 281–284. doi: 10.1109/ATIT50783.2020.9349343.

[24] E. Faure, et al., Method of Cyclic Synchronization Based on Permutations, Bulletin of Cherkasy State Technological University, 4 (2020) 67–76. doi: 10.24025/2306-4412.4.2020.222439.

[25] E. Faure, A. Shcherba, B. Stupka, Permutation-Based Frame Synchronisation Method for Short Packet Communication Systems, in: 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (2021) 1073–1077. doi: 10.1109/IDAACS53288.2021.9660996.

[26] J. Al-Azzeh, et al., Permutation-based Frame Synchronization Method for Data Transmission Systems with Short Packets, Egyptian Informatics J. 23(3) (2022) 529–545. doi: 10.1016/j.eij.2022.05.005.

[27] J. Al-Aazzeh, et al., Efficiency Assessment of the Permutation-based Frame Synchronization Method, Int. J. Commun. Antenna Propagation, 13(4) (2023). doi: 10.15866/irecap.v13i4.23567.

[28] E. Faure, et al., A Method for Reliable Permutation Transmission in Short-Packet Communication Systems, Information Technology for Education, Science, and Technics, 178 (2023) 177–195. doi: 10.1007/978-3-031-35467-0_12.

[29] D. E. Knuth, The Art of Computer Programming: Introduction to Combinatorial Algorithms and Boolean Functions, vol. 4A. Upper Saddle River, NJ: Addison-Wesley (2008).

[30] I. Yoshinori, Majority Circuit, JPH01296825A (1989).

[31] T. J. Terrell, L.-K. Shark, Digital Signal Processing. London: Macmillan Education UK (1996). doi: 10.1007/978-1-349-13735-0.

[32] L. Tan, J. Jiang, Digital Signal Processing, Fundamentals and Applications, 3rd ed. Elsevier (2019). doi: 10.1016/C2017-0-02319-4.

[33] G. Galati, G. Pavan, C. Wasserzier, Signal Design and Processing for Noise Radar, EURASIP J. Adv. Signal Process. 52 (2022). doi: 10.1186/s13634-022-00884-1.

[34] E. V. Faure, B. A. Stupka, Evaluation of Frame Synchronization Efficiency for Non-Separable Factorial Codes Depending on Synchronization Parameters, Èlektron. Model. 44(6) (2022) 21–35. doi: 10.15407/emodel.44.06.021.