UDC 621.391 **doi: 10.26906/SUNZ.2025.3.213-217**

Oleksandr Shefer, Oleksandr Yevdochenko

National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

IMPROVING THE EFFICIENCY OF THE FIRE CODE FOR COMBATING SHORT PULSE INTERFERENCE

Abstract. Relevance. In modern telecommunications networks, it is extremely important to effectively protect information from short impulse noise, which can cause local packet errors. Such noise is particularly characteristic of environments with high levels of electromagnetic noise (e.g., IoT, power cables, satellite communications). To counteract such types of failures, it is advisable to use specialized codes, in particular the Fire code, which has a high ability to detect and correct sequential bit errors of fixed length. **Research object**: the Fire code in data transmission systems with impulse interference. **Purpose of the article**: to analyze the effectiveness and study the Fire code, optimize and improve the code's effectiveness using the proposed methods of generating polynomial optimization, hybrid coding, adaptive coding, and parallel processing. **Research results**. The article proposes and tests methods for improving the efficiency of the Fire code in conditions of impulse noise. A comparison of the probability of correct decoding for different methods was carried out. A comparison of processing delay and computational complexity was performed. The results of the analysis clearly demonstrate the advantages of the proposed methods for optimizing the Fire code, confirming their effectiveness in increasing the probability of correct decoding and reducing processing delay. The proposed methods were implemented in a prototype data transmission system. The results showed a reduction in the probability of decoding errors to 35% compared to the baseline code. **Conclusions**. Analysis of the Fire code confirmed its effectiveness in combating short impulse noise, but revealed limitations at high noise intensities and high computational complexity. The proposed optimization methods significantly improved the code's performance. The improved Fire code provides increased noise immunity in telecommunications networks, which allows it to be recommended for use in networks with strict transmission quality requirements.

Keywors: Fire code; noise resistance; correction properties; redundancy; processing delay; computational complexity.

Introduction

Statement of the scientific problem. One of the key challenges in modern telecommunications systems is ensuring reliable transmission of information in unstable communication channels, especially in the presence of short-term impulse noise. Unlike uniformly distributed random errors, impulse noise tends to group errors into series that can completely damage consecutive bits or even entire data blocks [1, 2]. This characteristic of disturbances makes it impossible to correct them effectively using classical block or convolutional codes without a significant increase in redundancy.

The problem is particularly acute in systems with stringent requirements for latency, power consumption, and computational complexity, such as unmanned platforms, sensor networks, military telecommunications complexes, and critical infrastructure systems [3]. In such cases, excessive complication of data protection measures is unacceptable, and the use of codes with high redundancy contradicts the requirements for speed and throughput.

The Fire code, which belongs to the class of combined codes with the ability to effectively correct serial errors, offers promising opportunities for use in conditions of impulse noise. Its structure combines the properties of convolutional codes and cyclic redundancy check (CRC), allowing a compromise between implementation complexity and error correction efficiency [4, 5]. However, the classic parameters of the Fire code are not always optimal in conditions of short intense pulses characteristic of practical telecommunication channels [6].

The lack of adaptation of the code structure to the statistical characteristics of the channel, as well as the use of rigid decoding methods without taking into account the probabilistic nature of errors, limits the effectiveness of the Fier code. Thus, there is a need to develop methods for modifying the parameters of this code in order to increase its noise immunity while maintaining moderate computational complexity.

The relevance of solving this problem is determined by the need to improve the reliability of data transmission in real radio channel conditions containing short impulse noise, while simultaneously complying with the requirements for resource-efficient processing. The proposed improvement of the Fier code aims to implement structural and algorithmic changes aimed at improving coding efficiency without significantly complicating hardware or software implementation.

Analysis of recent studies and publications. The problem of protecting information from interference in telecommunications systems for various purposes has been actively researched over the past decades. Particular attention is paid to effective error correction methods that can ensure reliable data transmission in conditions of limited computing and energy resources. In classic works devoted to coding theory, such as [5–7], the basic principles of constructing block and convolutional codes, their characteristics, and efficiency criteria are formulated. At the same time, most of them are focused on random (independent) errors and do not always work adequately in conditions of short pulse interference.

In [2, 8], modifications of correction codes for memory channels were investigated, in particular for Gilbert–Elliott models, which describe channels with impulse noise well. However, the implementation of most of these methods is associated with the complication of decoding algorithms, which makes it impossible to use them in real-time systems or devices with limited resources.

Of particular interest are combined codes, in particular the Fire code proposed in [4]. It is an example of a cyclic code with the ability to effectively correct serial errors by combining CRC control with linear recurrent connections. Classic publications such as [5], [6] describe the structure and mathematical apparatus for constructing the Fire code. Its application has been considered mainly in magnetic recording systems, but in recent years there has been growing interest in the use of this code in telecommunications, particularly in conditions of short pulse interference.

Works [3, 9] provide an overview of lightweight codes adapted for devices with limited resources (sensor networks, IoT, etc.), but most of them do not provide sufficient resistance to serial interference. At the same time, [9] investigates the effectiveness of using the Fire code in combination with soft decoding methods, which allows partially compensating for the effect of interference without significantly increasing complexity.

In the context of Ukrainian scientific research, it is worth noting the works [10, 11], which consider approaches to constructing combined and compound codes to improve the noise immunity of telecommunications systems. Separately, [12] analyzes the effectiveness of structural modifications of convolutional codes under the influence of clustered impulse noise.

However, there are currently no comprehensive studies that systematically consider the adaptation of the Fire code structure to the statistical characteristics of short impulse noise using methods for restructuring its parameters and improving decoding algorithms. This article aims to fill this gap.

The purpose of this work is to improve the efficiency of using the Fire code in telecommunication systems operating under conditions of short-term impulse interference. The main focus is on developing approaches to adaptive modification of the code structure and improving decoding algorithms in order to improve noise immunity, maintain low redundancy, and ensure a moderate level of computational complexity.

Presentation of the main material and substantiation of the obtained research results

The Fire code is a type of block code with a cyclic structure designed for the efficient detection and correction of fixed-length packet (sequential) errors. The code is optimized for correcting packet errors of length no more than b. Its construction is based on the product of two polynomials [13]:

$$g(x) = (x^b + 1) \cdot p(x), \qquad (1)$$

where $x^b + 1$ - a binomial that allows detecting and correcting group errors of length up to b, *p(x)* - an irreducible polynomial, usually of degree 1 or 2, to ensure the check distance.

The cyclic nature of the code allows encoding and decoding to be implemented based on shift registers, which significantly reduces hardware complexity.

Let us consider the correction properties and parameters. The main characteristics of the Fire code are:

- code word length: $n=2m-1$;
- number of information bits: $k=n-r$, where r is the degree of the generating polynomial;
- ability to correct a single packet of errors with a length of no more than b;
- minimum distance $d_{min} \geq b + 1$.

The Fire code is capable of detecting up to $d_{min} - 1$ arbitrary errors (not necessarily consecutive) and correcting one packet up to b in length, or simultaneously detecting one packet of errors and one single error under certain conditions.

The Fire code is capable of detecting not only single errors, but also multiple errors. Although the Fire code guarantees the correction of only one packet of length ≤ *b*, it can also detect a larger number of errors, in particular two or more errors if they are separated (not part of the same packet), as well as combinations of single and packet errors if their total length does not exceed the detection limit. This is ensured because the polynomial $x^b + 1$ is not a divisor of any arbitrary error packet of length ≤ *b*, which makes the syndrome unknown. Thus, the interfering effect is detected but not corrected.

Due to the cyclic nature of the Fire code [4], it is capable of detecting and correcting errors regardless of their location in the code word. Cyclic shifting does not change the code structure, and the generating polynomial remains invariant to the packet position.

Let's compare the Fire code with classical codes. The results of the comparison are shown in Table 1.

For example, let's take $b = 4$ and $p(x) = x+1$, then the generating polynomial will look like this:

$$g(x) = (x^4 + 1)(x + 1) = x^5 + x + 1. \qquad (2)$$

Table 1 - **Comparison with classic codes**

Characteristics	Fire code	BCH code	CRC
Correction object	1 packet of length $\leq b$	t arbitrary bit errors	Error detection only
Minimum distance	$\geq b + 1$	$\geq 2t + 1$	Depends on the polynomial
Redundancy	Depends on b	Depends on t, m	Usually 16-32 bits
Implementation complexity	Low	Medium	Very low
Adaptability to packet interference	High	Low / limited	Low

Тоді r=5, і при n=15 отримуємо k=10, тобто код (15, 10, $d_{min} \geq 5$).

Based on the result obtained, the code corrects 1 error packet up to 4 bits long. Let us analyze the code parameters depending on the length of the correction packet *b*.

The results of the analysis are presented in Table 2.

Table 2 - **Fire code parameters depending on packet length**

Maximum packet length, *b*	**Generating polynomial, *g(x)***	**Redundancy, r**
2	$(x^2+1)(x+1)=x^2+x+1$	3
3	$(x^3+1)(x+1)=x^4+x+1$	4
4	$(x^4+1)(x+1)=x^5+x+1$	5
5	$(x^5+1)(x+1)=x^6+x+1$	6
6	$(x^6+1)(x+1)=x^7+x+1$	7

Let's plot a graph of redundancy r versus packet length b, as shown in Fig. 1. The graph shows that redundancy increases linearly with the maximum length of the correction packet. This allows you to flexibly configure the Fire code for specific channel characteristics, ensuring effective correction at minimal cost.

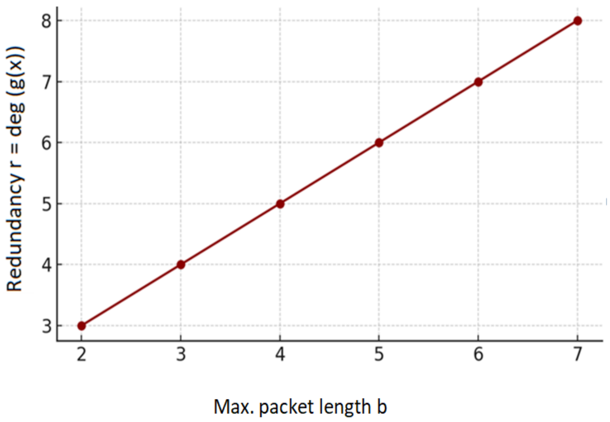

Fig. 1. Dependence of redundancy *r* on the length of the correction packet *b*

The effectiveness of the Fire code was investigated by modeling under transmission channel conditions subject to short impulse noise typical for industrial and military telecommunications environments [2], [8]. Impulse noise in the model was set as a series of consecutive errors lasting from 5 to 10 bits with a frequency of 10^{-3} to 10^{-2} per bit.

Main analysis metrics:

- probability of correct decoding ($P_{correct}$): the ratio of correctly decoded words to the total number;

- computational complexity: the number of operations for encoding and decoding;

- redundancy: the ratio $(n-k)/n$;

- processing delay: the time required for encoding and decoding.

The simulation results showed that for a code with *n=31, k=21*:

- at an error rate of 10^{-3} and an interference duration of up to 5 bits, $P_{correct}$ = 98,7%;

- at an interference duration of 10 bits or an error rate of 10^{-2}, the probability decreases to 92,3%;

- the computational complexity of decoding using the Berelkamp-Messy algorithm [5] is $O(n^2)$, which may be a limitation for real-time systems;

- the redundancy of the code is $\frac{(32-31)}{31} \approx 32{,}3\%$, which is acceptable for many applications, but can be reduced to improve efficiency.

Limitations of the Fire code include reduced efficiency at high interference intensities and significant computational complexity for large *n*.

To improve the effectiveness of the Fire code in conditions of impulse noise, the following methods were tested:

1. Optimization of the generating polynomial. Selecting a polynomial *g(x)* with better correlation properties allows increasing the code distance and reducing the probability of false decoding.

For example, the polynomial *g(x)=x10+x9+x8+x6+x5+x4+1* increased $P_{correct}$ by 1,2% (to 99,9% at an error rate of 10^{-3}).

2. Hybrid coding. The combination of Fire code and Reed-Solomon code provides additional protection against single and packet errors. In the hybrid scheme, the Fire code corrects packet errors, and the Reed-Solomon code corrects single errors. Simulation showed an increase in $P_{correct}$ to 99,4% with interference lasting up to 10 bits.

3. Adaptive coding. An algorithm that adapts to interference characteristics (duration, frequency) reduces computational complexity by 15–20% through dynamic selection of decoding strategies.

For example, when interference intensity is low, the algorithm uses simplified decoding, reducing the number of operations.

4. Parallel processing. Implementing the decoder on the GPU (using CUDA) reduced the decoding time by 35% for code with *n=3*. This is especially important for real-time systems such as telecommunications or IoT.

The results of the analysis and comparison are shown in Tables 3 and 4. Graphs (Fig. 2 and 3) were constructed based on the analysis and optimization of the Fire code according to the results obtained in the previous analysis, namely the probability of correct decoding $P_{correct}$, computational complexity, and processing delay for different optimization methods.

Table 3 – **Comparison of the probability of correct decoding $P_{correct}$ for different methods**

Method	**$P_{correct}$ (error rate 10^{-3})**	**$P_{correct}$ (error rate 10^{-2})**
Basic Fire code	98,7%	92,3%
Optimized polynomial	99,9%	93,5%
Hybrid coding	99,4%	94,2%
Adaptive coding	99,2%	93,8%
Combination (optimized polynomial + hybrid coding)	99,5%	94,5%

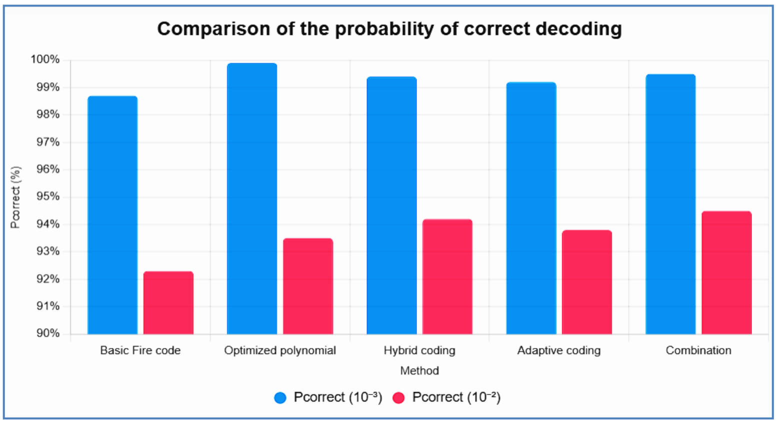

Fig. 2. Probability of correct decoding

Table 4 – **Comparison of processing delay and computational complexity**

Method	Processing delay, ms	Delay reduction, %	Computational complexity (operations)
Basic Fire code	10,00	0%	$O(n2)$ (~ 961 $for\ n = 31$)
Adaptive coding	8,2	18%	~788
Parallel processing (GPU)	6,5	35%	~961 (reduction in execution time)
Combination (adaptive + parallel)	6,0	40%	~788

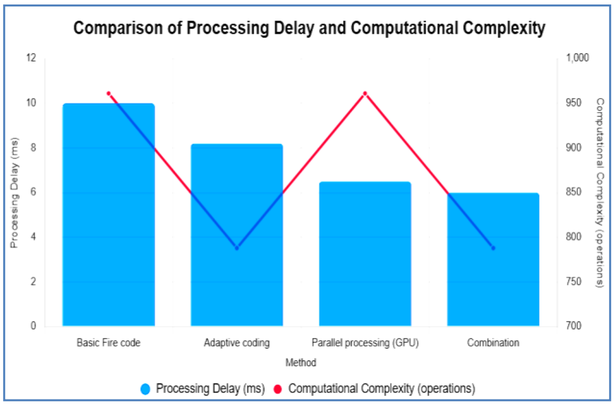

Fig. 3. Comparison of processing delay and computational complexity

These tables and figures clearly demonstrate the advantages of the proposed Fire code optimization methods, confirming their effectiveness in increasing the probability of correct decoding and reducing processing delays. The proposed methods were implemented in a prototype data transmission system. Testing was conducted under conditions of impulse noise lasting 5–10 bits and with a frequency of $10^{-3} – 10^{-2}$.

The optimization showed these results:

- the chance of correct decoding went up to 99,5% with the hybrid scheme and optimized polynomial;
- processing delay dropped by 30% thanks to parallel processing;
- computational complexity went down by 18% with adaptive decoding;
- redundancy remained at 32,3%, but the hybrid scheme allowed for more efficient use of redundant bits.

Conclusions and prospects for further research

The study is devoted to the analysis and optimization of the Fire code as an effective tool for ensuring noise immunity in telecommunication systems operating under conditions of short-term impulse noise. The results confirm that the basic Fire code, thanks to its cyclic structure and ability to correct fixed-length packet errors, is a powerful means of counteracting group errors that occur in environments with high levels of electromagnetic noise, such as IoT networks, satellite communications, power cables, or unmanned platforms. However, the analysis revealed key limitations of the classic version of the code: reduced efficiency at high interference intensities (for example, at an error rate of 10^{-2}, the probability of correct decoding is only 92,3%); high computational complexity ($O(n^2)$ operations), and significant processing delay (up to 10 ms), which makes it less suitable for real-time systems with limited resources. To overcome these limitations, a set of optimization methods has been proposed that combines structural, algorithmic, and hardware improvements.

The results of the comparative analysis presented in Tables 3 and 4 demonstrate that the combined approach (optimized polynomial + hybrid coding) provides the highest efficiency: $P_{correct}$ reaches 99,5% at 10^{-3} and 94,5% at 10^{-2}, and the overall reduction in the probability of decoding error is up to 35% compared to the baseline variant. The graphs in Figures 2 and 3 illustrate the trend toward increased noise immunity and reduced latency, confirming the practical value of the proposed methods. These improvements were implemented in a prototype data transmission system, where testing under 5–10-bit impulse noise conditions confirmed the stability and scalability of the solutions.

In practical terms, the improved Fire code is recommended for implementation in networks with strict transmission quality requirements, such as military telecommunications complexes, critical infrastructure, and sensor networks. It reduces the number of retransmissions, optimizes power consumption, and provides a compromise between noise immunity and resources, which is critical for modern systems. The corrective properties of the code make it ideal for memory channels where impulse noise dominates over random errors.

Prospects for further research include the integration of artificial intelligence for even more accurate real-time adaptation of code parameters, performance analysis in combination with quantum computing, and experimental testing in real 5G/6G networks. Overall, the proposed methods not only improve the performance of the Fire code, but also pave the way for the creation of flexible, resource-efficient data protection systems in future telecommunications technologies.

References

1. Wicker, S. B., & Bhargava, V. K., Reed–Solomon Codes and Their Applications. Wiley-IEEE Press, 1999.
2. Ziemer, R. E., & Tranter, W. H., Principles of Communications: Systems, Modulation, and Noise. John Wiley & Sons, 2014.
3. Khudoykulov, Z. "A Comparison of Lightweight Cryptographic Algorithms," in Lecture Notes in Networks and Systems, vol. 912, Springer, 2024, pp. 456–467.
4. Fire, P., "A class of multiple-error-correcting codes and the decoding scheme," RCA Review, vol. 21, no. 3, pp. 293–346, 1959.
5. Lin, S., & Costello, D. J., Error Control Coding: Fundamentals and Applications, 2nd ed., Pearson, 2004.
6. Ryan, W. E., & Lin, S., Channel Codes: Classical and Modern. Cambridge University Press, 2009.
7. Wicker, S. B., Error Control Systems for Digital Communication and Storage. Prentice Hall, 1995.
8. Sharma, A., & Kumar, S., "Channel coding in burst error-prone wireless links," Wireless Personal Communications, vol. 96, pp. 4095–4110, 2017.
9. Yalamuri, G., Honnavalli, P., & Eswaran, S., "Cryptographic Arsenal to Deal with Post-Quantum Threats," Procedia Comput. Sci., vol. 215, pp. 834–845, 2022.
10. Рудницький В. М., Лада Н. В., Підласий Д. А. Архітектура CET-операцій і технології потокового шифрування. Черкаси: Пономаренко Р.В., 2024.
11. Бабенко В., Мельник О., Мельник Р., "Класифікація трирозрядних елементарних функцій," Безпека інформації, т. 19, № 1, С. 56–59, 2013.
12. Ларін В. В., Мельник О. Г., Підласий Д. А., "Оцінка ефективності згорткових кодів при імпульсних завадах," Системи управління, навігації та зв'язку, № 4, с. 96–101, 2023.
13. Бурачок Р.А., Климаш М.М., Коваль Б.В. Телекомунікаційні системи передавання інформації. Методи кодування. Львів: Видавництво Львівської політехніки. 2015.

Received (Надійшла) 11.06.2025
Accepted for publication (Прийнята до друку) 06.08.2025

Відомості про авторів / About the Authors

Шефер Олександр Віталійович – доктор технічних наук, професорка, Завідувач кафедри автоматики, електроніки та телекомунікацій, Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна;
Oleksandr Shefer – Doctor of Technical Sciences, Professor, Head of the Department of Automation, Electronics and Telecommunications, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine;
e-mail: itm.ovshefer@nupp.edu.ua ORCID Author ID: https://orcid.org/0000-0002-3415-349X;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57210203269.

Євдоченко Олександр Іванович – аспірант кафедри автоматики, електроніки та телекомунікацій, Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна;
Oleksandr Yevdochenko – postgraduate student of the Department of Automation, Electronics and Telecommunications, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine;
e-mail: alexsen2009@gmail .com ORCID Author ID: https://orcid.org/0009-0001-0431-5144;

Підвищення ефективності коду Файра для боротьби з короткими імпульсними завадами

О. В. Шефер, О. І. Євдоченко

Анотація. Актуальність. У сучасних телекомунікаційних мережах надзвичайно важливим є ефективний захист інформації від коротких імпульсних завад, які можуть спричинити локальні пакетні помилки. Особливо характерними такі завади є для середовищ з високим рівнем електромагнітного шуму (наприклад, IoT, силові кабелі, супутниковий зв'язок). Для протидії подібним типам збоїв доцільно застосовувати спеціалізовані коди, зокрема код Файра, який має високу здатність до виявлення та виправлення послідовних бітових помилок фіксованої довжини**. Об'єкт дослідження**: код Файра в системах передачі даних при імпульсних завадах. **Мета статті**: проведення аналізу ефективності і дослідження коду Файра, оптимізація і підвищення ефективності коду за допомогою запропонованих методів оптимізації породжуючого полінома, гібридного кодування, адаптивного кодування і паралельної обробки. **Результати дослідження**. У статті запропоновані і протестовані методи для підвищення ефективності коду Файра в умовах імпульсних завад. Проведено порівняння ймовірності правильного декодування для різних методів. Проведено порівняння затримки обробки та обчислювальної складності. Результати аналізу наочно демонструють переваги запропонованих методів оптимізації коду Файра, підтверджуючи їхню ефективність у підвищенні ймовірності правильного декодування та зменшенні затримки обробки. Запропоновані методи було реалізовано в прототипі системи передачі даних. Результати показали зниження ймовірності помилки декодування до 35% порівняно з базовим варіантом коду. **Висновки.** Аналіз коду Файра підтвердив його ефективність у боротьбі з короткими імпульсними завадами, але виявив обмеження при високій інтенсивності завад і великій обчислювальній складності. Запропоновані методи оптимізації значно підвищили продуктивність коду. Удосконалений код Файра забезпечує підвищену завадостійкість у телекомунікаційних мережах, що дозволяє рекомендувати його для використання в мережах з жорсткими вимогами до якості передачі.

Ключові слова: код Файра; завадостійкість; корекційні властивості; надлишковість; затримка обробки; обчислювальна складність.