Optimization of the encryption and signal processing algorithm of the functional testing device in communication with control modules of the aerial vehicle ground launch system

Pham Duc Thong[1*], D.V. Tarlakovsky[2], Nguyen Huu Phuong[1]

[1]Institute of Missile, Academy of Military Science and Technology, 17 Hoang Sam, Nghia Do, Hanoi, Vietnam;
[2]Moscow Aviation Institue, №4 Volokolamskoe shosse, Moscow, Russian Federation.
[*]Corresponding author: dtstudio.pro@gmail.com
Received 10 Nov. 2025; Revised 28 Dec. 2025; Accepted 19 Jan. 2026; Published 25 Apr. 2026.
DOI: https://doi.org/10.54939/1859-1043.j.mst.110.2026.3-11

ABSTRACT

This paper proposes a solution to enhance the reliability and security of the data transmission channel between the Functional Testing Device and control modules of the aerial vehicle ground launch system under harsh operating conditions, where both intentional and random electromagnetic interference may occur. Based on the principles of game theory, the study models the problem of optimizing encryption parameters and feedback mechanisms as an adversarial interaction between the communication system and the interference source. The objective is to maximize the guaranteed data transmission rate under an average interference power constraint. An optimization algorithm is proposed to select the most suitable set of parameters (code block length, error correction capability, and signal basis) adapted to the specific characteristics of command and status data in the missile system. Simulation results demonstrate that the proposed solution significantly improves anti-jamming capability compared to conventional methods, thereby enhancing readiness and safety in the missile launch preparation and firing process.

Keywords: Ground launch system; Data transmission optimization; Intentional jamming; Error-correcting coding; Game theory.

1. INTRODUCTION

In advanced launch systems, particularly aerial vehicle ground launch systems, the Functional Testing Device (FTD) is responsible for monitoring system status, diagnosing faults, and transmitting control commands to functional modules. The reliability and timeliness of these transmission channels are therefore critical to mission success. In this paper, the term "encryption" is used in a system-level sense, referring to the protection of control and diagnostic data against intentional interference at the physical and data-link layers.

Such systems operate in complex electromagnetic environments, where communication is affected not only by random noise but also by deliberate jamming aimed at disrupting data exchange. Ensuring guaranteed noise immunity under adversarial conditions has long been a central research challenge. From early work on transmission over channels with unknown parameters [1–3] to studies of spread spectrum systems under arbitrary interference [3, 5–7], game theory has proven effective for modeling the interaction between communication systems and hostile jammers [6, 9–12]. These studies established the foundations of modern anti-jamming communication through optimal receiver design, ε-optimal strategies, and minimax formulations.

More recently, machine learning–based and hybrid signal processing approaches have been explored for denoising and signal enhancement, achieving improved performance under various noise conditions [8, 13, 14]. However, these methods are typically optimized for average-case scenarios and do not explicitly address guaranteed performance under worst-case intentional jamming.

Furthermore, much of the existing literature focuses on generic or civilian systems, without considering the stringent requirements of aerial vehicle ground launch architectures, which

demand low latency, high safety, and continuous command availability under intensive electronic warfare conditions. Motivated by these requirements, this paper proposes a game-theoretic framework to optimize encryption and signal processing parameters of the FTD when interfacing with control modules. Building on the foundations in [11] and [12], a dynamic optimization algorithm is developed to select appropriate coding parameters, error-correction capability, and signal basis, thereby enhancing the reliability and anti-jamming resilience of the data transmission channel under intentional electromagnetic interference.

2. PROBLEM FORMULATION AND PROPOSED OPTIMIZATION ALGORITHM

2.1. Physical system model, signal processing and transmission protocol

The communication system under consideration consists of a Functional Testing Device (FTD) acting as the transmitter and a set of control modules of the aerial vehicle ground launch system acting as receivers. The FTD is responsible for collecting system status information, generating control commands, and transmitting these data to the target modules through a wireless communication channel. Each receiving module decodes the received data and provides a feedback signal in the form of an acknowledgement (ACK) or negative acknowledgement (NAK), enabling retransmission when necessary.

The communication channel is assumed to be time-varying and affected by additive white Gaussian noise (AWGN) as well as intentional jamming. The transmitted data are packetized into information words of length *k*, encoded using linear error-correcting codes of length *n* and minimum Hamming distance *d* [12], and subsequently modulated and spread using a pseudo-noise sequence with signal base *b*. At the receiver, despreading, demodulation, and decoding are performed in an ARQ-based framework with a flexible error-correction threshold. This model captures the essential characteristics of the data exchange process between the FTD and control modules under adversarial interference conditions.

2.2. Game-theoretic problem modeling

The interaction between the communication system and the jammer is modeled as a **two-player non-cooperative zero-sum game** $G(q,U,V)$ **[**11, 12**].**

– **Strategy Space of Player 1 (System – FTD):** Θ, a strategy $U \in \Theta$ is a vector of optimizable system parameters:

$$U = (b,k,r) \tag{1}$$

where: $b \in \mathbb{Z}^+$ - signal base (processing gain), $k \in \{1,2,...,n-1\}$ - information word length, $r \in \{0,1,...,t\}$ - flexible error-correction threshold, with $t = \left\lfloor (d-1)/2 \right\rfloor$.

– **Strategy Space of Player 2 (Jammer):** Υ, a strategy $V \in \Upsilon$ is a probability distribution function $F_v(z)$ of the instantaneous JSR δ_v, belonging to the set of distributions constrained by the average jamming power:

$$\Omega(\delta) = \left\{ F_v(\cdot) \middle| E_{F_v}[\delta_v] = \int z dF_v(z) \le \delta \right\}$$

– **Utility Function:** Defined as the **guaranteed effective information rate,** which depends on both players' strategies:

$$q(U,V) = \frac{k}{n \cdot b} \cdot \left(1 - P_{\text{retrans}}(U,V)\right) \tag{2}$$

where: k/n is the code rate, $1/b$ reflects the spreading-induced rate reduction, $P_{\text{retrans}}(U,V)$ is the retransmission probability, determined by channel quality (affected by V) and system parameters U.

2.3. Optimization problem statement

The system designer (FTD) seeks the optimal parameter set U^* that maximizes the worst-case guaranteed information rate, even when the jammer selects its best counter-strategy.

Formally, the optimization problem consits in finding:

$$U^* = \left(b^*, k^*, r^*\right) = \arg\max_{U \in \Theta} \left[\inf_{V \in \Omega(\delta)} q\left(U, V\right) \right] \tag{3}$$

The optimal guaranteed value is:

$$Q^* = \max_{U \in \Theta} \left[\inf_{V \in \Omega(\delta)} q\left(U, V\right) \right] \tag{4}$$

where $\inf_{V \in \Omega(\delta)} q\left(U, V\right)$ is the **guaranteed value function** $Q\left(U\right)$, representing the worst-case transmission rate achievable under all admissible jamming strategies with average power less than or equal to δ.

The strategy U^* that achieves Q^* is referred to as the **optimal guaranteeing strategy.**

This optimization problem requires solving two nested subproblems:

1. **Worst-case jamming strategy** V^* for a given system configuration U.
2. **Best system configuration** U^* that withstands the worst-case jamming strategy.

2.4. Proposed optimization algorithm

Directly solving the nonlinear nested optimization problem formulated in section 2.4 is highly complex. The proposed algorithm adopts a controlled grid-search approach combined with approximation formulas for parameter adjustment, thereby enabling a feasible method to determine the optimal parameter set $\left(b^*, r^*, k^*\right)$.

2.4.1. Core components of the algorithm

The algorithm relies on three main calculation formulas:

a) Bit error probability in the physical channel (p_e):

The error probability depends on the total interference-to-signal ratio $\delta_\Sigma = \delta_v + \delta_\xi$ and the signal base b. Under optimal pulsed jamming, the upper convex envelope of the function $\varphi\left(\delta_\Sigma\right)$ is used to approximate the worst case:

$$p_e \approx \varphi_\delta^-\left(\delta, b\right) = \begin{cases} c_b \cdot \left(\delta / b\right), \delta / b \le \gamma_b \\ \varphi\left(\delta / b\right), \delta / b > \gamma_b \end{cases} \tag{5}$$

where c_b and γ_b are constants depending on b and the modulation scheme.

b) Retransmission probability (P_{retrans})

This is the probability that an n-bit codeword contains more than r errors. Assuming independent bit errors, a binomial distribution is applied:

$$P_{\text{retrans}} = \left(n, r, p_e\right) = 1 - \sum_{i=0}^{r} \binom{n}{i} p_e^i \left(1 - p_e\right)^{n-i} \tag{6}$$

c) Undetected error probability ($P_{\text{undetected}}$):

This is the most critical case, when errors exceed the detection capability of the code. A tight estimate based on code structure is used:

$$P_{\text{undetected}}(n,k,r) \approx \frac{2^k - 1}{2^{n-k} - \sum_{i=0}^{r} \binom{n}{i}} \tag{7}$$

This formula reflects the ratio between the number of invalid codewords potentially confused and the total number of available syndromes for error detection.

2.4.2 Algorithm description

- Input Parameters: n : codeword length (fixed, defined by protocol or hardware); δ : average jamming-to-signal power ratio; $p_{U,\text{target}}$: target bit error probability for the entire system (e.g., 10^{-9} or 10^{-12} for critical commands); List_b : set of available signal base values (e.g., [16, 32, 64, 128]); Code_Table: lookup table of available codes (n,k,d) for each n.

- Output Parameters: b_{opt} : optimal signal base; k_{opt} : optimal information word length; r_{opt} : optimal error-correction threshold; $Q_{\max}$: optimal guaranteed information rate.

The proposed optimization procedure is summarized in the flowchart shown in Figure 1.

2.4.3. Discussion on computational efficiency

- Complexity: The computational complexity is: $O(|\text{List\_b}| \cdot |\text{List\_k}| \cdot t \cdot n)$. With fixed n and moderate list sizes (e.g., 5–10 values), the algorithm is feasible for offline execution or when channel conditions change significantly.
- Optimizations:
  + Use distribution approximations (e.g., Poisson) when nnn is large and p_e is small.
  + Prioritize search with decreasing k and increasing b when δ is large, based on observed trends.
  + Precompute binomial coefficients $\binom{n}{i}$ and cumulative sums to avoid repeated calculations.
- Practical Relevance: The algorithm provides a systematic method for adaptive tuning of coding and transmission parameters based on measured channel quality (δ), instead of relying on manual experience. The outputs can be directly applied to reconfigure the encoder and communication protocol of the FTD in real time, thereby improving resilience against intentional jamming.

3. SIMULATION RESULTS AND DISCUSSION

To evaluate the effectiveness of the proposed optimization algorithm, a series of simulations were conducted in the MATLAB environment. The main parameters and scenarios are as follows:

- **System scenario:** The simulation models the communication channel between the FTD and an engine control module of the APPiP system. The transmitted data are high-priority, high-reliability control commands.
- **Fixed parameters:**
  + Codeword length: $n = 63$ (bits), chosen to balance coding efficiency and transmission latency.
  + Background noise power: $\delta_{\xi} = 0.01$ (baseline SNR = 20 dB, representing a good channel condition).

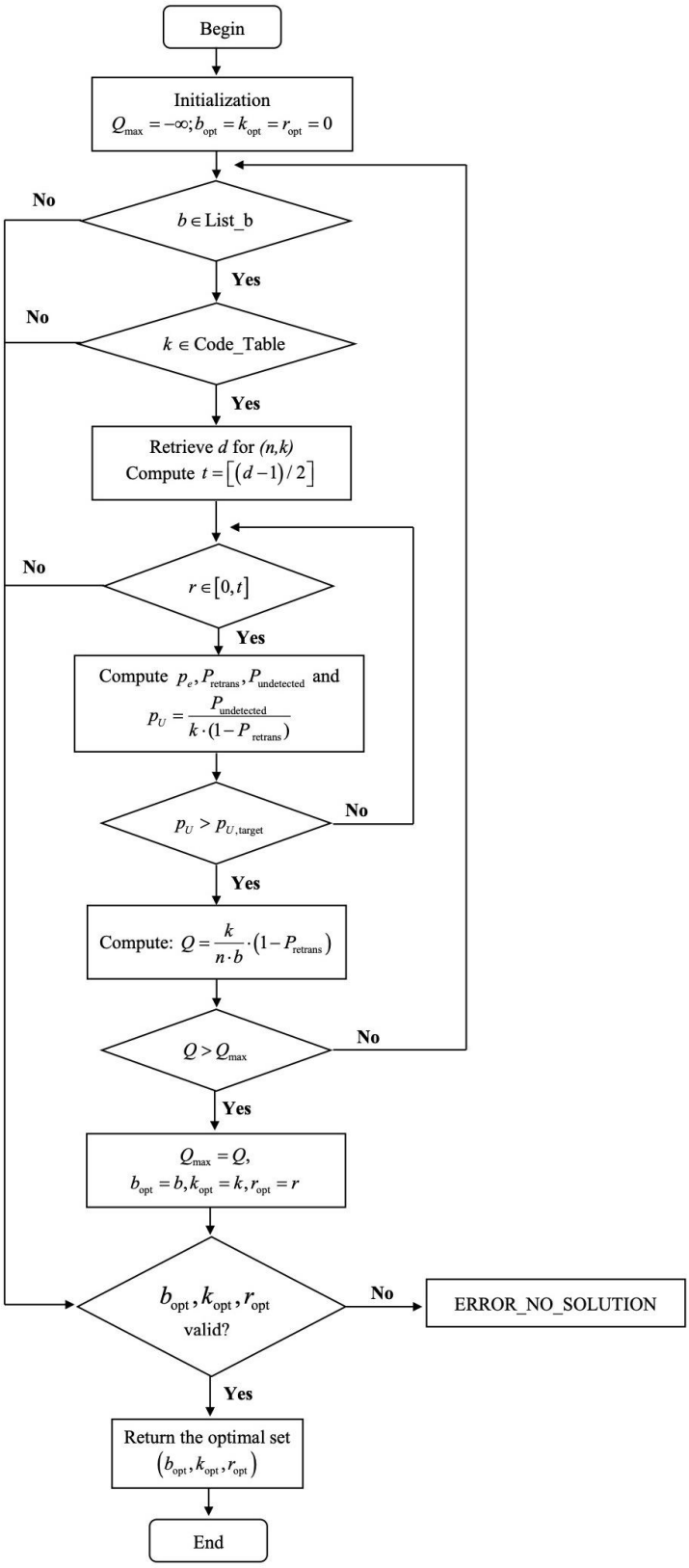

Figure 1. *Flowchart illustrating the main steps of the proposed optimization algorithm.*

+ Target bit error probability: $p_{U,\text{target}} = 10^{-9}$, ensuring ultra-high reliability for control commands.
+ Coding schemes: BCH codes with available sets (n,k,t) : (63, 36, 5), (63, 45, 3), (63, 51, 2), (63, 57, 1).
+ Signal base values under consideration: [16, 32, 64, 128].

– **Independent Variable:** The average jamming-to-signal power ratio δ was varied from 0 dB to 12 dB in 1 dB steps.
– **Comparison Methods:** The performance of the **Proposed Adaptive Algorithm (PAA)** is compared with two conventional fixed strategies:
+ **PP1 – Maximum Error-Correction Mode:** Always uses $r = t$, attempting to correct the maximum number of errors allowed by the code. This is common in many systems.
+ **PP2 – Pure Error Detection Mode:** Always uses $r = 0$, relying solely on ARQ retransmission. This strategy prioritizes safety.

3.1. Results and Discussion

3.1.1. Performance analysis of information rate

– *Quantitative Results:* Figure 2 shows Guaranteed Information Rate (GIR): Q versus jamming ratio δ. The proposed adaptive algorithm (PAA) consistently achieves higher throughput compared to the baseline methods.

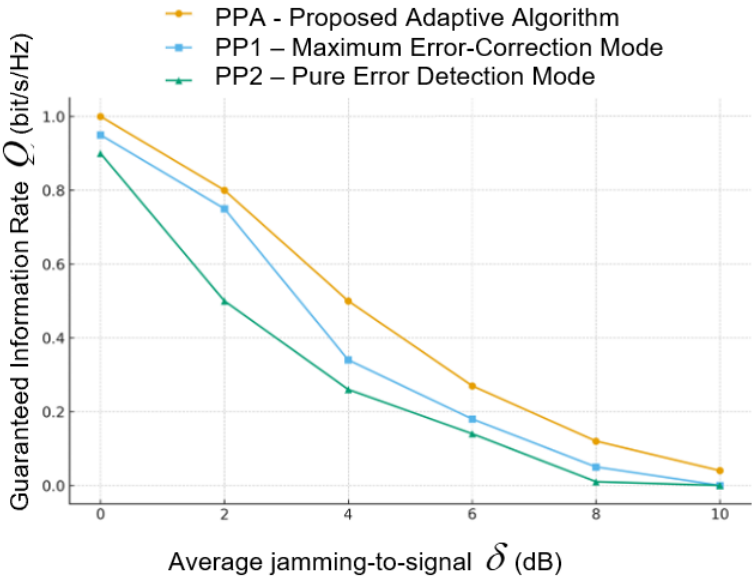

Figure 2. *GIR versus average jamming-to-signal ratio δ for the PAA, PP1 and PP2.*

+ At **low jamming levels (**δ < 4 dB**)**, all three methods achieve high throughput. PAA and PP1 (error correction) perform almost equivalently and outperform PP2, thanks to lower retransmission probability.
+ At **moderate jamming levels (4 dB ≤** δ **≤ 8 dB),** PAA demonstrates a clear advantage. At δ = 6 dB, PAA maintains $Q \approx 0.25$ bit/s/Hz, while PP1 and PP2 drop to ~0.17 and ~0.13 bit/s/Hz, respectively - corresponding to 47% and 92% improvement.
+ At **high jamming levels (**δ > 8 dB**),** all systems degrade severely. However, PAA still sustains a meaningful non-zero rate, while fixed strategies fail to maintain reliable transmission ($Q \to 0$).

– *Explanation:* The superiority of PAA stems from its adaptive capability. The algorithm dynamically adjusts parameters (b,k,r) to optimize the trade-off between spectral efficiency $k/n, 1/b$ and reliability P_{retrans}.

3.1.2. Trends in optimal parameter selection

Analysis of the optimal parameters $(b_{\text{opt}}, k_{\text{opt}}, r_{\text{opt}})$ across different δ levels reveals trends consistent with theory:

– **Signal base (b_{opt}):** Increases with δ. At δ=2 dB, b_{opt} = 16 is chosen for higher throughput. At δ = 10 dB, b_{opt} = 128 is selected to provide greater processing gain against interference.

– **Information word length (k_{opt}):** Decreases with δ. At δ = 2 dB, BCH(63, 57, 1) (low redundancy) is selected to exploit good channel quality. At δ = 10 dB, the system switches to BCH(63, 36, 5) (high redundancy) to improve robustness.

– **Error-correction threshold (r_{opt}):** The most interesting observation. At low-to-moderate jamming, PAA often selects $r_{\text{opt}} < t$ (e.g., $r = 2$ instead of $t = 3$ for BCH(63, 45, 3)). This indicates that, beyond a certain jamming level, sacrificing part of the correction capability in favor of error detection and ARQ retransmission yields better overall throughput. Only at very high jamming levels does PAA shift to $r = 0$, prioritizing absolute error detection — consistent with theoretical analyses of ARQ superiority over FEC in heavy-error environments.

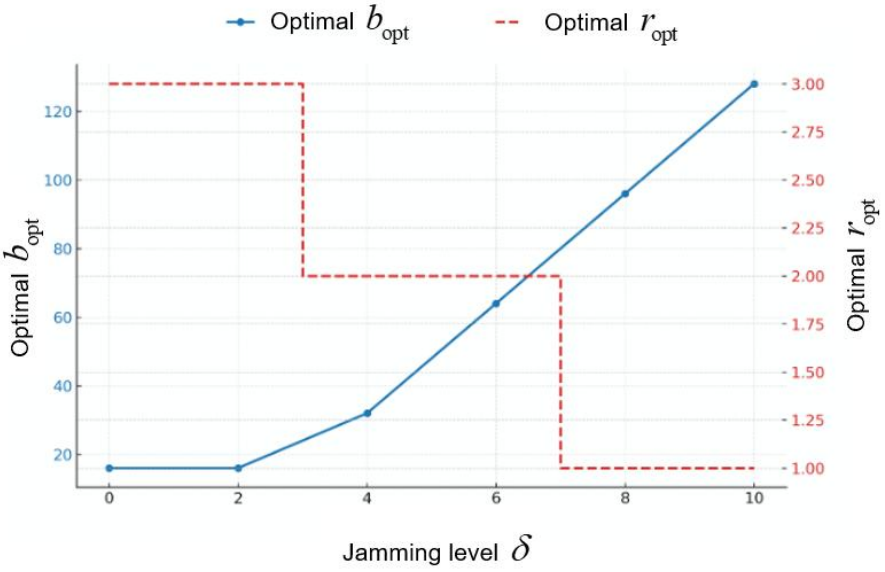

Figure 3. *Optimal values of the signal base b_{opt} and error-correction threshold r_{opt} as functions of the jamming level δ.*

The evolution of the optimal parameters b_{opt} and r_{opt} with respect to the jamming level δ is depicted in Figure 3, indicating the system's shift from correction-based to detection-dominant strategies as interference grows.

The simulation results confirm the validity and efficiency of the proposed algorithm:

– **Optimality:** PAA consistently selects parameters that match channel conditions, improving GIR by up to 47–92% under moderate jamming compared with fixed strategies.

- **Adaptability:** The trends of parameter adjustment ($b\uparrow$,$k\downarrow$,$r\downarrow$) are fully aligned with theoretical expectations: stronger defense against interference and adaptive error-handling strategies under increased jamming.
- **Reliability guarantee:** The algorithm always ensures compliance with strict reliability requirements of weapon control systems, which fixed strategies fail to achieve under strong interference.

Therefore, integrating the proposed algorithm into the FTD design is both feasible and beneficial, significantly enhancing the survivability and effectiveness of the aerial vehicle ground launch system in complex electronic environments.

4. CONCLUSIONS

This paper has proposed a parameter optimization method for transmission and coding in the communication channel between the FTD and the control modules of the aerial vehicle ground launch system under intentional jamming conditions. These results confirm that integrating the proposed optimization algorithm into FTD is both feasible and practically meaningful, enhancing the reliability, readiness, and combat effectiveness of the aerial vehicle ground launch system in complex electronic environments.

REFERENCES

[1]. Дубровин, В. И., и др. *"Онтология методов и стратегий защиты радиоканалов от преднамеренных помех"*. Вестник связи, (2010).

[2]. Huang T., Liu Y., Liu X., and Wang M. *"A new improved multi-sequence frequency-hopping communication anti-jamming system"*. Electronics, vol. 14, No.3, p. 523, (2025).

[3]. Р.Р. Биккенин, И.В. Макаров. *"Передача информации сигналами с расширенным спектром и самокодированием"*. Информация и Космос., № 3, С. 6–10, (2023).

[4]. Xiao Y., Ren H., Wu S., Liu L., Meng X., and Ding P. *"Anti-jamming method of cognitive radio based on Q-learning"*. 12th International Conference on Electronics, Communications and Networks (CECNet 2022), Frontiers in Artificial Intelligence and Applications, vol. 363, pp. 97–104, (2022).

[5]. К.С. Григорян, Е.С. Басан. *"Онтология методов и стратегий защиты радиоканалов от преднамеренных помех"*. Инженерный вестник Дона, No.11, 29 с, (2025).

[6]. Jia L., Qi N., Su Z., Chu F., Fang S., Wong K. K., and Chae C. B. *"Game theory and reinforcement learning for anti-jamming defense in wireless communications: Current research, challenges, and solutions"*. IEEE Communications Surveys & Tutorials, in press, pp. 1798-1838, (2024).

[7]. de Curto J., de Zarza I., Cano J. C., and Calafate C. T. *"Enhancing communication security in drones using QRNG in frequency hopping spread spectrum"*. Future Internet, vol. 16, no. 11, p. 412, (2024).

[8]. S. Zhang and M. Yu. *"Machine Learning-Driven Innovation in Denoising and Enhancement for Signal Processing"*. 2025 4th International Conference on Electronic Information Technology (EIT), Chengdu, China, pp. 1-5, (2025).

[9]. L. Jia et al. *"Game-Theoretic Learning Anti-Jamming Approaches in Wireless Networks"*. IEEE Communications Magazine, vol. 60, no. 5, pp. 60-66, (2022).

[10]. L. Kubiavka, V. Zaremba and V. Ziuziun. *"Application of Game Theory Methods to Optimize the Stakeholder Management Process"*. IEEE 4th International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, pp. 647-651, (2024).

[11]. Воробьев Н.Н. *"Основы теории игр. Бескоалиционные игры"*. М.: Наука, 496 с, (1984).

[12]. Han Z., Niyato D., Saad W., Başar T., Hjørungnes T. *"Game Theory in Wireless and Communication Networks"*. Cambridge University Press, 554 p, (2011).

[13]. A. Kumar, R. G. Tiwari and N. K. Trivedi. *"Hybrid Deep Learning Framework for Road Surface"*. 2025 International Conference on Intelligent Control, Computing and Communications (IC3), Mathura, India, pp. 487-492, (2025).

[14]. P. V. Ramana, G. J. Reddy, V. S. Krishna, Y. Y. Reddy and V. V. Reddy. *"A Hybrid Signal Denoising Approach using Wavelet Decomposition and Neural Network-based Thresholding"*. 5th International Conference on Trends in Material Science and Inventive Materials (ICTMIM), Kanyakumari, India, pp. 1400-1404, (2025).

TÓM TẮT

Tối ưu hoá thuật toán mã hoá và truyền dữ liệu của thiết bị kiểm tra chức năng khi giao tiếp với một số mô đun điều khiển của hệ thống phóng thiết bị bay từ mặt đất

Bài báo trình bày phương pháp tối ưu hóa thuật toán mã hóa và chế độ xử lý tín hiệu của thiết bị kiểm tra chức năng (TBKT) khi giao tiếp với các mô-đun điều khiển của hệ thống phóng thiết bị bay từ mặt đất. Đặc biệt, bài báo xem xét bài toán tối ưu trong điều kiện có nhiễu có chủ đích, nhằm đảm bảo độ tin cậy và tốc độ truyền gói tin khi trao đổi dữ liệu kiểm tra, giám sát và điều khiển. Dựa trên mô hình toán học và lý thuyết trò chơi, bài báo đề xuất thuật toán lựa chọn tối ưu các tham số mã hóa, độ trải phổ tín hiệu và chế độ giải mã nhằm nâng cao khả năng chống nhiễu và giảm suy hao công suất tín hiệu.

Từ khoá: Hệ thống phóng; Tối ưu hóa truyền dẫn dữ liệu; Gây nhiễu có chủ đích; Mã sửa lỗi; Lý thuyết trò chơi.