ISSN 3083-7715 (online) *Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)*
ISSN 3083-7650 (0135-1710)(print) *Management Information System and Devices. 2026. No. 1 (188)*

UDC 004.89:004.05:004.7 DOI: https://doi.org/10.30837/0135-1710.2026.188.044

Volodymyr Panchenko, Heorhii Kuchuk

THEORETICAL-ALGEBRAIC BASICS OF EVOLUTIONARY TEST SYNTHESIS FOR GATEWAYS COMPONENTS OF HIGH-DENSITY IOT SYSTEMS

Relevance. *The modern Internet of Things (IoT) paradigm is undergoing a fundamental transformation, shifting from simple telemetry collection networks to complex, High-Density IoT ecosystems, where Intelligent IoT Gateways play a pivotal role. The architectural heterogeneity creates a "state explosion" problem, where the space of possible configurations and failure scenarios exceeds the capabilities of traditional deterministic testing methods, which are unable to effectively detect deeply hidden vulnerabilities.* ***Object of research:*** *processes of automated synthesis of diagnostic tests and reliability verification for multi-layer heterogeneous components of intelligent IoT gateways.* ***Purpose of the article:*** *development of theoretical foundations and a mathematical model for evolutionary test synthesis for intelligent IoT gateways.* ***Research objectives****: formalization of the adaptation of genetic algorithms to the specifics of IoT architecture; improving the efficiency of critical defect detection.* ***Research methods****: apparatus of the theory of universal algebras and category theory.* ***Research results.*** *The article proposes and mathematically substantiates a generalized model of test synthesis based on the use of a pair of universal algebras describing the test scenario space and evolutionary operators. An extended conceptual apparatus is introduced and systematized, mapping population genetics terminology to the field of technical diagnostics of cyber-physical systems. The existence of a homomorphism between algebraic models of classic genetic algorithms and vulnerability search processes in IoT devices is proven. A test synthesis method based on the mathematical apparatus of modern algebra has been developed. The application of category theory to describe morphisms between gateway state spaces and evolutionary operators is substantiated, guaranteeing the correctness of test set transformations.* ***Conclusions.*** *The proposed approach allows to create a universal testing methodology that provides a significant increase in code coverage and defect detection. Scope of application of the obtained results: computer-aided design and diagnostics systems for IoT, testing platforms for cyber-physical systems, development of toolkits for QA engineers in the Embedded Systems and Edge AI fields.*

Keywords: *Internet of Things; intelligent gateway; genetic algorithms; universal algebra; category theory; test synthesis.*

Introduction

Statement of the problem

The evolution of digital ecosystems over the past decade has been characterized by unprecedented growth in the number of connected devices that form the global infrastructure of the Internet of Things (IoT). According to analysts' forecasts, the number of active IoT connections continues to grow exponentially, transforming industry, healthcare, and urban infrastructure within the concepts of Industry 4.0 and 5.0. The central hub that provides functional compatibility, security, and manageability in these heterogeneous networks is the Intelligent IoT Gateway. Unlike traditional network bridges, modern gateways are complex computing platforms that integrate routing, protocol conversion, cryptographic protection, and edge analytics (Edge AI) functions [1].

The architectural complexity of such devices creates unique challenges for ensuring their reliability. The gateway must simultaneously handle thousands of concurrent connections through various physical interfaces (Ethernet, Wi-Fi, BLE, Zigbee, LoRa, etc.), manage message queues (MQTT, AMQP), maintain data integrity during power outages, and withstand cyberattacks. This multidimensionality of the system state space leads to a phenomenon known as "state explosion", which makes exhaustive testing physically impossible and economically impractical. As noted in [2], traditional test generation methods focused on deterministic digital circuits are powerless against the dynamic nature of the IoT.

Research confirms that critical failures in such systems often arise from complex temporal correlations and resource contention when processing asynchronous interrupts [3], or require the reproduction of specific, deep sequences of network packets that cannot be generated by stateless fuzzing methods [4].

Therefore, there is a pressing scientific need to develop new, intelligent methods for automated test synthesis that can effectively explore the solution space and identify critical vulnerabilities within an acceptable time frame. The most promising direction is the use ofevolutionary computing, in particular genetic

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

algorithms (GA), which demonstrate high efficiency in optimization tasks where the device under investigation is presented as a "black box". However, the direct, unadapted application of classical GAs for testing gateways faces problems of premature convergence, generation of syntactically incorrect tests, and low learning speed. Solving these problems requires the creation of a rigorous theoretical basis that will allow formalizing the process of adapting biological metaphors of evolution to engineering tasks of technical diagnostics.

Analysis of recent research and publications

The issue of testing IoT systems and the application of evolutionary methods is the subject of active research by the global scientific community. Systematic literature reviews in recent years indicate a transition from testing individual components to comprehensive end-to-end testing that covers devices, gateways, and cloud platforms.

Researchers Minani et al. [2] propose testing taxonomies that take into account the heterogeneity and distributed nature of IoT, but note the lack of formalized methods for automatically generating test data that would take into account the semantics of protocols.

Considerable attention is paid to the use of genetic algorithms for cybersecurity tasks in IoT, in particular for intrusion detection. Works [5–8] demonstrate the successful application of GA for optimizing neural network parameters (CNN, LSTM) and feature selection in attack detection systems. However, these studies focus primarily on traffic classification rather than on the generation of test scenarios capable of causing system failure, which is the goal of stress testing and fuzzing (the introduction of invalid, inappropriate, or randomly generated inputs).

The theoretical aspects of formalizing complex systems are considered through the prism of algebraic approaches and category theory. Studies [9, 10] demonstrate the effectiveness of algebraic methods for verifying arithmetic schemes and synthesizing program invariants. The application of category theory to model-based systems engineering (MBSE) and architecture modeling is discussed in [11]. The authors argue that category theory provides a powerful toolkit for describing the composability of systems, allowing the interaction of components to be modeled as morphisms. However, as noted in the work, there is a gap between abstract theory and engineering testing practice, especially in the context of evolutionary methods.

Thus, the task of creating a mathematical model that combines the heuristic power of evolutionary algorithms with the rigor of algebraic structures for the purposeful synthesis of tests for complex IoT gateways remains unresolved.

The aim of this work is to develop the theoretical foundations and mathematical model of evolutionary test synthesis for intelligent IoT gateways based on the use of universal algebra and category theory to formalize the processes of adapting genetic algorithms to the multilayer architecture of cyber-physical systems.

Main material

1. Correspondence of evolutionary theory conceptual frameworks and technical diagnostics

Genetic algorithms are a class of stochastic search and optimization methods based on the mechanisms of natural selection and genetics. For the correct application of this mathematical apparatus in the field of technical diagnostics, it is necessary to establish a clear isomorphism between biological entities and the objects of testing of intelligent gateways.

Classic GAs, which operate on fixed-length bit strings, are ineffective for IoT gateways due to their complex heterogeneous structure. The gateway operates with data at different levels of abstraction: from physical parameters (RSSI signal level, battery voltage, etc.) to high-level data structures (JSON objects in the MQTT protocol, binary CBOR format in the CoAP protocol [12]). Therefore, the concept of an "individual" in a test population must be transformed from a simple vector to a complex, hierarchical data structure that describes the scenario of interaction with the system.

Analysis of the structure of smart gateways and the specifics of their testing [1, 2] allows us to form an extended list of terminology correspondences, which is the basis for further formalization, the main concepts of which are given in Table 1.

The specificity of IoT requires the introduction of new concepts that are absent in classical digital automata theory. In particular, the concept of a "multi-protocol chromosome" describes a scenario that includes a sequence of actions in different protocols (for example, receiving data via Zigbee and sending via MQTT), while an "energy phenotype" reflects an energy consumption profile that is critical for battery-powered devices.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

Table 1. *Systematization of the correspondence between the concepts of population genetics and test diagnostics of IoT systems*

The concept of genetics	The concept of IoT technical diagnostics	Interpretation and implementation in the context of the gateway
Allele	Permissible set of parameter values	A set of valid and invalid values for a specific gateway component
Gene	Elementary test impact parameter	Atomic configuration within a scenario
Chromosome	Parameter vector / Test set	Complete, ordered specification of a single test case
Genotype	Coded representation of the test	Data structure subject to genetic operations
Phenotype	System behavior under load	Observed gateway response to the test
Population	Set of tests	A set of test scenarios executed in parallel or sequentially at the current stage of evolution (generation)
Fitness	Test effectiveness / Coverage	Numerical metric that aggregates: code coverage percentage, number of detected failures, degree of resource load
Mutation	Parameter modification	Stochastic change of values: bit inversion, change of numerical values, substitution of data types
Crossover	Combination of scenarios	Creation of a new test by recombining parts of parent scenarios
Locus	Parameter location in the structure	Semantic binding of a gene to a specific gateway component

2. Development of evolutionary test synthesis mathematical model

To ensure the rigour of transferring evolutionary search methods to the field of diagnostics, it is proposed to use the apparatus of universal algebra. This allows us to abstract from the specific physical nature of signals and work with generalised operations on sets, which is particularly relevant for heterogeneous systems [10, 13].

Let us define an algebra as a pair (M, D), where M is the algebra carrier (a non-empty set of elements), and D is the signature (a set of operations of a given arity). It is proposed to describe the process of evolutionary test synthesis using a system of two interrelated algebras:

1. Algebra of scenario generation (individual level) $A_1^T\left(M_1^T, D_1^T\right)$, where $M_1^T = \{c_1, ..., c_i, ..., c_n\}$ – is the set of all n acceptable and unacceptable input vectors (test sets) for the gate; the elements of this set are chromosomes c_i; $D_1^T = \left\{d_{1\tau}^{T1}, d_{2\tau}^{T1}, ..., d_{k\tau}^{T1}\right\}$ – signature containing generation operations $\left(d_{1\tau}^{T1}\right)$, unary mutation operations $\left(d_{2\tau}^{T1}\right)$, binary crossover operations $\left(d_{3\tau}^{T1}\right)$ and other specific operators (e.g., translocation).

2. Algebra of population evolution (population level): $A_2^T\left(M_2^T, D_2^T\right)$, where M_2^T – the set of all possible subsets of tests (populations); $D_2^T = \left\{d_{1\tau}^{T2}, d_{2\tau}^{T2}, d_{3\tau}^{T2}\right\}$ – selection, reproduction, and reduction (selection of the best) operations.

Similarly, a classical genetic algorithm can be described by a pair of algebras $A_3^\Gamma\left(M_3^\Gamma, D_3^\Gamma\right)$ та $A_4^\Gamma\left(M_4^\Gamma, D_4^\Gamma\right)$. The key idea of the proposed approach is to establish homomorphism. $f_1 : A_3^\Gamma \to A_1^T$ та $f_2 : A_4^\Gamma \to A_2^T$.

The presence of homomorphism guarantees that applying an abstract genetic operator (e.g., bit string crossover) to the test model corresponds to a correct operation in the real space of gateway parameters (e.g., correct merging of protocol configurations), which generates a valid test for execution. If this principle is violated (e.g., crossover creates a packet with an incorrect checksum that is rejected by the driver), then homomorphism is absent, and the efficiency of the algorithm degrades to a random search.

For a more in-depth modeling of structural relationships, we suggest using category theory [11, 14, 15]. This allows us to consider the testing process as a mapping between categories of states.

Let K_T is a category where $Ob\,K_T$ objects are the states of the gate during testing (memory configurations, queues, registers, etc.), and the morphisms $Mor\,K_T$ are transitions between states caused by test influences. Let K_{Ev} – be the category of the evolutionary process, where the objects $Ob\,K_{Ev}$ are test populations, and the morphisms $Mor\,K_{Ev}$ are evolutionary transformations. The existence of a functor $F = \left(K_{Ev}, K_T\right)$ allows us to automatically translate fitness function optimization strategies into strategies for finding paths to erroneous system states.

The conclusion about the nesting of categories is particularly important. If we consider the category of simple tests K_1^* (changing one parameter) and the category of complex stress tests K_2^* (simultaneous change of a group of parameters), then K_1^* is

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

a subcategory of K_2^*. This theoretically justifies the advantage of genetic algorithms operating in space K_2^* (with macro-mutation operators) over local search methods, as they are capable of detecting complex, correlated defects that are unattainable for simple morphisms.

3. Application of universal algebras and category theory for creating test synthesis methods

Based on the developed mathematical foundation, a number of modified test synthesis methods adapted to the specifics of IoT gateways are proposed.

Heuristic combination method. Given the high uncertainty of IoT environment behavior, no single heuristic (e.g., bit inversion alone) can guarantee effective vulnerability discovery. The method of combining heuristics is described by an extended signature D^E of $A^E\left(M^E, D^E\right)$ algebra, which includes a set of heterogeneous heuristics $d_1^E, d_2^E, \ldots, d_n^E$ based on mutation, crossover, and other

$$D^E = \left\{d_1^E, d_2^E, \ldots, d_n^E\right\}. \quad (1)$$

The algorithm adaptively selects an operator at each step based on its current effectiveness (probabilistic approach). For the specifics of gateways, it is proposed to use a specialized combined crossover operator with translocation. The principle of its operation is as follows: during crossover, one of the offspring receives part of the genes from the first parent (inheritance), and the other part – inverted or logically opposite values from the second parent (entropy introduction). When applied in the IoT field, this allows for the automatic generation of "contrast" load scenarios. For example, the system simultaneously attempts to transmit valid critical priority data via MQTT and a stream of damaged packets via the CoAP interface. This approach effectively detects errors in the prioritization and isolation mechanisms of processes in the gateway operating system.

A test synthesis method that takes into account a priori information about the structure. One of the main problems with applying classical GAs to network protocols is the destruction of data structure. Simple crossover operators break bit strings at arbitrary locations, leading to a violation of the integrity of JSON/XML structures or checksums (CRC). Such tests are rejected by the gateway's input parsers even before the main logic is executed, which makes testing ineffective.

To solve this problem, a hierarchical chromosome structure with the introduction of control genes is proposed. The chromosome is represented as a tuple:

$$C = \langle G_{ctl}, G_{data} \rangle, \quad (2)$$

where G_{ctl} – higher-level control genes that determine testing strategy; G_{data} – information genes containing specific parameters.

A structurally adaptive crossover operator d_{StrAw}^{Γ} is also introduced, which allows breaking a chromosome exclusively at the boundaries of logical blocks (between the header and body of a packet, between configuration records, etc.). This guarantees that the test remains syntactically correct when its semantics change, ensuring that the test penetrates deeply into the logic of the device.

Evolutionary method on parallel computing structures. Testing IoT gateways is an extremely time-consuming process. A single test can take from seconds to minutes due to the need to wait for network timeouts and system stabilization. Thus, sequential execution of a population of 100 tests can take hours.

The algebraic model is extended by introducing parallel operations. Let algebra $A^{\Pi}\left(M^{\Pi}, D^{\Pi}\right)$ be given, the operation of evaluating the fitness $\mu(x)$ of an individual x, which is the most computationally complex, is transferred to parallel streams. In the proposed method, the population P_t is divided into subsets $\left\{P_{t,1}, ..., P_{t,k}\right\}$, which are processed by independent nodes in a cloud or fog environment.

Each node emulates a virtual instance of the gateway or interacts with a separate physical interface of the test bench. The central orchestrator performs only selection and reproduction operations. This allows for nearly linear acceleration of the test synthesis process, which is critical for ensuring continuous integration (CI/CD) in IoT development [16].

Method based on evolutionary strategies. Many parameters of gateway operation are continuous rather than discrete in nature: supply voltage level, processor temperature, time intervals for maintaining persistent connections, sensor thresholds, etc. For such parameters, the bit representation of classical GA is unnatural and inefficient. A method based on evolutionary strategies is used, where a chromosome is a vector of real numbers.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

The mutation operator is implemented by adding a random variable x_i with a normal distribution to each parameter:

$$x_i^{'} = x_i + N(0, \sigma_i), \quad (3)$$

where σ_i – the mean square deviation (mutation step), which is also part of the genotype and adapts during evolution (self-adaptation).

This allows for hardware-level stress testing by finding the limit values of parameters (for example, the minimum permissible voltage at which the gateway still functions but begins to allow errors in writing to flash memory), which is impossible to do using combinatorial logic methods [17].

Test synthesis using non-homologous chromosomes. Gateways work with variable-length data streams (message queues, fragmented IP packets). Classic crossover works with chromosomes of fixed length (homologous), which limits its applicability. The concept of non-homologous chromosomes with different lengths and structures is introduced.

In this case, it is proposed to apply a modified crossover algorithm with a correction phase:

1. Selection of breakpoints at arbitrary (even asymmetrical) locations on the parent chromosomes.

2. Exchange of sections, which leads to a change in the length of the offspring.

3. Correction phase:

– if the length of the offspring exceeds the permissible MTU (Maximum Transmission Unit), truncation or fragmentation of the packet is performed;

– if the length is insufficient (mandatory fields are lost), neutral fillers are added. This approach allows for the evolutionary study of specific classes of vulnerabilities, such as buffer overflows and attacks on packet fragmentation mechanisms.

4. Test synthesis based on the mathematical apparatus of modern algebra

Integrating all the methods we've looked at lets us build a single, generalized test synthesis scheme for smart gateways (Fig. 1).

The process is described as an iterative procedure in the multidimensional space of gateway states, controlled by a multifactorial fitness function $\mu(x)$.

The formula for the fitness function for the IoT gateway looks like this:

$$\mu(x) = w_1 \cdot S_{cov} + w_2 \cdot E_{detect} + w_3 \cdot R_{usage} - w_4 \cdot T_{exec} \quad (4)$$

where S_{cov} – code coverage or protocol state space coverage; E_{detect} – the weight of the detected errors (depending on their criticality); R_{usage} – peak resource usage (memory, central processing unit), which stimulates the search for DoS attacks; T_{exec} – penalty for test execution time (to optimize the length of the set); w_i, $i = \overline{1,4}$ – weight coefficients that can be adjusted depending on the testing objective.

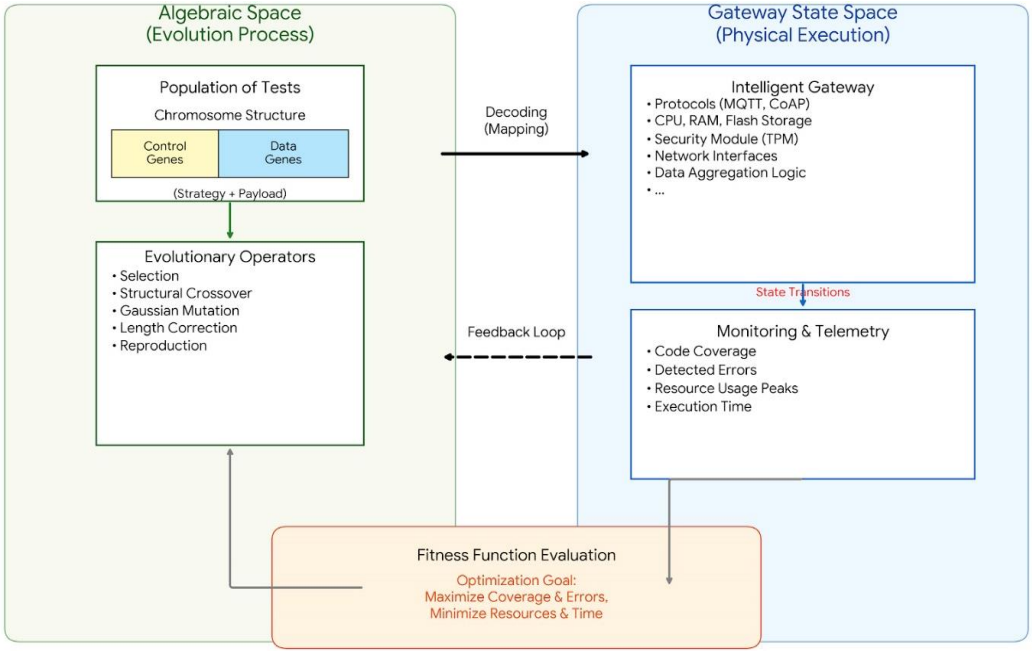

Fig. 1. Generalized scheme of test synthesis based on an algebraic approach

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

As a result of the analysis, the following generalized algorithm for synthesizing tests for IoT gateway components is proposed:

1. Initialization. Formation of the initial population of scenarios using templates and taking into account the structure (2).

2. Evaluation. Parallel launch of tests on digital twins or physical devices. Collection of metrics via telemetry interfaces (4).

3. Selection. Selection of tests that caused anomalies or reached deep branches of the code.

4. Recombination and mutation. Application of an adaptive set of operators (1) from algebra A^E, including combined crossover and mutations of evolutionary strategies (3) for physical parameters.

5. Correction. Restoration of the structural integrity of tests for non-homologous chromosomes.

6. Termination condition. Achievement of the target reliability level or exhaustion of the time budget.

Research results and their discussion

To experimentally verify the proposed model, a software package was developed that implements adapted genetic algorithms. Testing was performed on a model of an intelligent gateway with heterogeneous interfaces operating under realistic load conditions [18].

The effectiveness of the proposed method was evaluated in comparison with three existing approaches:

– classical random testing [19–21];

– testing based on rules created by experts (heuristic expert) [22, 23];

– methods based on state-of-the-art FSM models [4, 24, 25].

Fig. 2 shows comparative histograms of the final error coverage for five key gateway components.

Analysis of the diagrams shows a significant advantage of the proposed method for all system components.

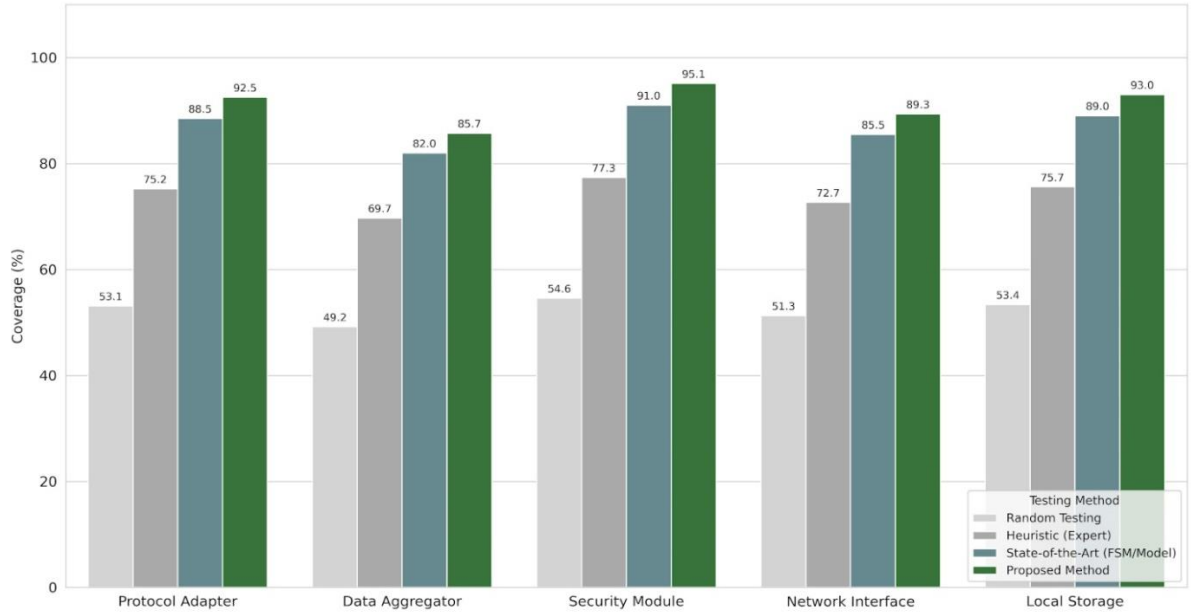

Fig. 2. Comparison of gateway component coverage

Thus, for the protocol adapter, the best coverage is 92.5%, which is explained by the use of a structurally adaptive crossover that preserves the syntactic correctness of packets. For local storage and network interface, the coverage also exceeds 89%, which indicates the successful operation of evolutionary strategies with real numbers when testing resource constraints.

An important aspect is not only the final result, but also the speed at which it is achieved. Figure 3 shows the generalized dynamics of the testing process, averaged across the entire system. The graph shows that the proposed method is characterized by the steepest slope in the initial stages (0–40% of the process duration). This indicates the high convergence speed of the algorithm due to the use of a priori information about the gateway structure. While random testing methods show almost linear, slow growth, the proposed approach quickly reaches a coverage level of over 90%. The use of non-homologous chromosomes made it possible to avoid the population stagnation observed in the heuristic method graph.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

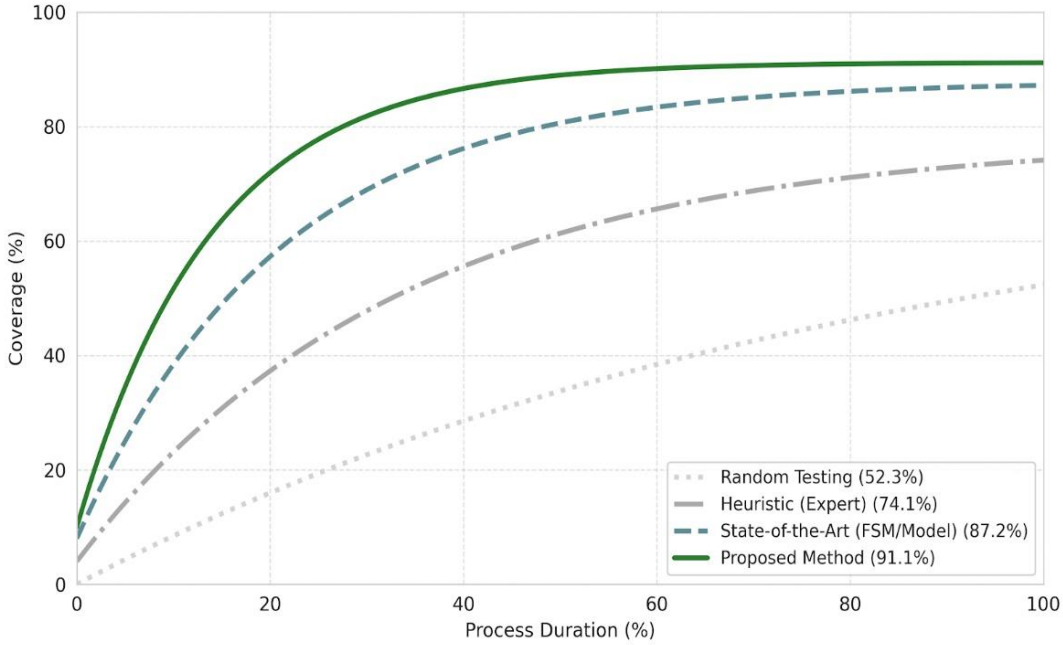

Fig. 3. Generalized dynamics of gateway component coverage

Thus, experiments confirm that algebraic formalization of the test synthesis process provides a significant increase in code coverage and defect detection compared to random search and static analysis methods.

Conclusions and prospects for further development

1. A theoretical algebraic model for synthesizing tests for intelligent IoT gateways has been developed and substantiated, based on the use of a pair of universal algebras (scenario generation and population evolution). This made it possible to formalize the process of testing complex heterogeneous systems and prove the mathematical correctness of transferring evolutionary computing methods to the field of technical diagnostics.

2. An extended classification of concepts (gene-parameter, chromosome-scenario, phenotype-behavior) has been proposed, which, unlike classical approaches, takes into account the specifics of IoT: multi-protocol, energy dependence, real-time operation, and variable data formats.

3. The effectiveness of using a combination of heuristics and combined crossover to overcome local extrema when searching for vulnerabilities has been proven. It has been shown that the introduction of structural constraints (control genes) and chromosome length correction mechanisms significantly increases the percentage of valid tests in the population, allowing computational resources to be focused on verifying the deep logic of the gateway.

4. The practical implementation of the proposed methods on parallel computing structures solves the problem of critical time constraints when testing high-density networks, ensuring the scalability of the diagnostic process and the possibility of integration into modern development pipelines.

The theoretical and algebraic solutions obtained in this work and the proven effectiveness of evolutionary test synthesis create a fundamental basis for the transition from disparate testing tasks to the creation of a comprehensive methodology. The priority direction for further scientific research is the development of methods for component and integral diagnostics of the intelligent gateway of the peripheral layer of a multi-density IoT. The implementation of this direction involves solving two interrelated classes of problems:

1. At the level of individual gateway subsystems (components), further work will focus on deepening the specialization of evolutionary operators to take into account hardware specifics (development of methods for generating stress tests for the gateway's neural processing units (NPUs), creation of adaptive scenarios for testing the physical level in conditions of high signal interference characteristic of dense LoRaWAN, ZigBee, Wi-Fi 6, etc. networks).

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

2. Development of integral diagnostics methods (detection of defects that arise exclusively during the interaction of correctly functioning separate components (taking into account resource collisions, inter-level tracking of error propagation).

Thus, the proposed algebraic approach creates a reliable foundation for the implementation of new directions, since its abstract nature allows expanding the signature of operations without changing the overall architecture of the method.

Conflict of interest

The authors declare that they have no conflict of interest with respect to this research, including financial, personal, authorship, or other conflicts that could influence the research and its results presented in this article.

Funding

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technology in the creation of this work.

References

1. Beniwal, G., Singhrova, A. (2022), "A systematic literature review on IoT gateways", *Journal of King Saud University – Computer and Information Sciences*, No. 34(10), P. 9541–9563. DOI: https://doi.org/10.1016/j.jksuci.2021.11.007

2. Minani, J. B., Sabir, F., Moha, N., Guéhéneuc, Y.-G. (2024), "A Systematic Review of IoT Systems Testing: Objectives, Approaches, Tools, and Challenges", *IEEE Transactions on Software Engineering*, No. 50(4), P. 785–815. DOI: https://doi.org/10.1109/TSE.2024.3363611

3. Trimananda, R., Aqajari, S.A.H., Chuang, J., Demsky, B., Xu, G. H., Lu, S. (2020), "Understanding and automatically detecting conflicting interactions between smart home IoT applications", *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, P. 1215–1227. DOI: https://doi.org/10.1145/3368089.3409682

4. Shu, Z., Yan, G. (2022), "IoTInfer: Automated Blackbox Fuzz Testing of IoT Network Protocols Guided by Finite State Machine Inference", *IEEE Internet of Things Journal*, No. 9(22), P. 22737–22751. DOI: https://doi.org/10.1109/JIOT.2022.3182589

5. Hakiki, R.I., Azerine, A., Tlemsani, R., Golabi, M., Idoumghar, L. (2025), "Enhancing IoT intrusion detection with genetic algorithm-optimized convolutional neural networks", *The Journal* DOI: https://doi.org/10.1007/s11227-025-07626-8

6. Jain, V., Agrawal, M. (2020), "Applying Genetic Algorithm in Intrusion Detection System of IoT Applications", *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184)*, P. 284–287. DOI: https://doi.org/10.1109/ICOEI48184.2020.9143019

7. Dong, J., Li, Z., Zheng, Y., Luo, J., Zhang, M., Yang, X. (2024), "Real-time fault detection for IIoT facilities using GA-Att-LSTM based on edge-cloud collaboration", *Frontiers in Neurorobotics*, No. 18, P. 1499703. DOI: https://doi.org/10.3389/fnbot.2024.1499703

8. Katsura, Y., Endo, A., Arai, I., Fujikawa, K. (2025), "Efficient IDS for IoT Networks Using Host-Based Data Aggregation and Multi-Entropy Analysis", *IEEE Access*, No. 13, P. 125406–125419. DOI: https://doi.org/10.1109/ACCESS.2025.3589057

9. Sampathkumar, B., Das, R., Martin, B., Enescu, F., Kalla, P. (2025), "An Algebraic Approach to Partial Synthesis of Arithmetic Circuits", *Proceedings of the 30th Asia and South Pacific Design Automation Conference*, P. 1097–1103. DOI: https://doi.org/10.1145/3658617.3697724

10. Humenberger, A., Amrollahi, D., Bjørner, N., Kovács, L. (2022), "Algebra-Based Reasoning for Loop Synthesis", *Formal Aspects of Computing*, No. 34(1), P. 1–31. DOI: https://doi.org/10.1145/3527458

11. Vidalie, J., Batteux, M., Mhenni, F., Choley, J.-Y. (2022), "Category Theory Framework for System Engineering and Safety Assessment Model Synchronization Methodologies", *Applied Sciences*, No. 12(12), P. 5880. DOI: https://doi.org/10.3390/app12125880

12. Molina Araque, S., Martinez, I., Papadopoulos, G.Z., Montavont, N., Toutain, L. (2023), "Yet Another Compact Time Series Data Representation Using CBOR Templates (YACTS)", *Sensors*, No. 23(11), P. 5124. DOI: https://doi.org/10.3390/s23115124

13. Tao, T. (2024), *A pilot project in universal algebra to explore new ways to collaborate and use machine assistance?* URL: https://terrytao.wordpress.com/2024/09/25/a-pilot-project-in-universal-algebra-to-explore-new-ways-to-collaborate-and-use-machine-assistance/ (дата звернення: 21.01.2026).

14. Mabrok, M.A., Ryan, M J. (2017), "Category Theory as a Formal Mathematical Foundation for Model-Based Systems Engineering", *Applied Mathematics & Information Sciences*, No. 11(1), P. 43–51. DOI: https://doi.org/10.18576/amis/110106

15. Breiner, S., Subrahmanian, E., Sriram, R.D. (2023), "Category Theory". In A. M. Madni, N. Augustine, & M. Sievers (Eds.), *Handbook of Model-Based Systems Engineering*, P. 1259–1299. DOI: https://doi.org/10.1007/978-3-030-93582-5_85

16. Jamil, M.A. (2025), "Evolutionary Algorithm Behavior to Optimize the IoT Scheduling Problem", *2025 IEEE International Conference on E-Business Engineering (ICEBE)*, P. 288–291. DOI: https://doi.org/10.1109/ICEBE68123.2025.00052

17. Surayya, A., Muzakkir Hussain, M., Reddy, V.D., Abdul, A., Gazi, F. (2025), "Evolutionary Algorithms for Edge Server Placement in Vehicular Edge Computing", *IEEE Access*, No. 13, P. 79030–79052. DOI: https://doi.org/10.1109/ACCESS.2025.3566172

18. De Benedictis, A., Flammini, F., Mazzocca, N., Somma, A., Vitale, F. (2023), "Digital Twins for Anomaly Detection in the Industrial Internet of Things: Conceptual Architecture and Proof-of-Concept", *IEEE Transactions on Industrial Informatics*, No. 19(12), P. 11553–11563. DOI: https://doi.org/10.1109/TII.2023.3246983

19. Muench, M., Stijohann, J., Kargl, F., Francillon, A., Balzarotti, D. (2018), "What You Corrupt Is Not What You Crash: Challenges in Fuzzing Embedded Devices", *Proceedings 2018 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. DOI: https://doi.org/10.14722/ndss.2018.23166

20. Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I., Guizani, M. (2020), "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security", *IEEE Communications Surveys & Tutorials*, No. 22(3), P. 1646–1685. DOI: https://doi.org/10.1109/COMST.2020.2988293

21. Aldysty, A.R., Moustafa, N., Lakshika, E. (2025), "A Holistic Review of Fuzzing for Vulnerability Assessment in Industrial Network Protocols". *IEEE Open Journal of the Communications Society*, No. 6, P. 4437–4461. DOI: https://doi.org/10.1109/OJCOMS.2025.3569291

22. Qureshi, A.-H., Larijani, H., Ahmad, J., Mtetwa, N. (2019), "A Heuristic Intrusion Detection System for Internet-of-Things (IoT)". *Intelligent Computing*, Vol. 997, P. 86–98. DOI: https://doi.org/10.1007/978-3-030-22871-2_7

23. Latha, R., Thangaraj, J.J. (2025), "IoT security using heuristic aided symmetric convolution-based deep temporal convolution network for intrusion detection by extracting multi-cascaded deep attention features", *Expert Systems with Applications*, No. 269, P. 126363. DOI: https://doi.org/10.1016/j.eswa.2024.126363

24. Németh, G.Á. (2025), "Model-based mutation testing for Finite State Machine specifications with MTR", *Infocommunications Journal*, No. 17(3), P. 84–91. DOI: https://doi.org/10.36244/ICJ.2025.3.10

25. Pan, Z., Zhang, L., Hu, Z., Li, Y., Chen, Y. (2022), "SATFuzz: A Stateful Network Protocol Fuzzing Framework from a Novel Perspective", *Applied Sciences*, No. 12(15), P. 7459. DOI: https://doi.org/10.3390/app12157459

Received (Надійшла) 22.01.2026
Accepted for publication (Прийнята до друку) 29.01.2026
Publication date (Дата публікації) 12.03.2026

Відомості про авторів / About the Authors

Панченко Володимир Іванович – Національний технічний університет "Харківський політехнічний інститут", старший викладач кафедри комп'ютерної інженерії та програмування; Харків, Україна;
Volodymyr Panchenko – National Technical University "Kharkiv Polytechnic Institute", Senior Lecturer at the Computer Engineering and Programming Department; Kharkiv, Ukraine;
e-mail: Volodymyr.Panchenko@khpi.edu.ua
ORCID ID: https://orcid.org/0000-0003-3364-3398

Кучук Георгій Анатолійович – доктор технічних наук, професор, Національний технічний університет "Харківський політехнічний інститут", професор кафедри комп'ютерної інженерії та програмування; Харків, Україна;
Heorhii Kuchuk – Doctor of Technical Sciences, Professor, National Technical University "Kharkiv Polytechnic Institute", Professor at the Computer Engineering and Programming Department; Kharkiv, Ukraine;
e-mail: mkuchuk56@ukr.net
ORCID ID: http://orcid.org/0000-0002-2862-438X

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

ТЕОРЕТИКО-АЛГЕБРАЇЧНІ ОСНОВИ ЕВОЛЮЦІЙНОГО СИНТЕЗУ ТЕСТІВ КОМПОНЕНТІВ ІНТЕЛЕКТУАЛЬНИХ ШЛЮЗІВ ВИСОКОЩІЛЬНИХ IOT-СИСТЕМ

Актуальність. *Сучасна парадигма Інтернету речей (IoT) переживає фундаментальну трансформацію, переходячи від простих мереж збору телеметрії до складних, високощільних екосистем, де ключову роль відіграють інтелектуальні шлюзи. Архітектурна гетерогенність шлюзів породжує проблему "комбінаторного вибуху станів", коли простір можливих конфігурацій та сценаріїв відмов перевищує можливості традиційних детермінованих методів тестування, не здатних ефективно виявляти глибоко приховані вразливості.* ***Об'єктом дослідження*** *є процеси автоматизованого синтезу діагностичних тестів і верифікації надійності для багатошарових гетерогенних компонентів інтелектуальних IoT-шлюзів.* ***Мета статті –*** *розроблення теоретичних засад і математичної моделі еволюційного синтезу тестів для інтелектуальних шлюзів IoT.* ***Завдання дослідження****: формалізація адаптації генетичних алгоритмів до особливостей архітектури IoT; підвищення ефективності виявлення критичних дефектів.* ***Застосовані методи****: апарат теорії універсальних алгебр і теорії категорій.* ***Результати дослідження.*** *У роботі запропоновано й математично обґрунтовано модель синтезу тестів, яка базується на використанні пари універсальних алгебр, що описують простір тестових сценаріїв та еволюційні оператори. Упроваджено й систематизовано розширений понятійний апарат, що відтворює впровадження термінології популяційної генетики у сферу технічної діагностики кіберфізичних систем. Доведено наявність гомоморфізму між алгебраїчними моделями класичних генетичних алгоритмів і процесами пошуку вразливостей у IoT-шлюзах. Розроблено метод синтезу тестів на основі математичного апарату сучасної алгебри. Обґрунтовано застосування теорії категорій для опису морфізмів між просторами станів шлюзу й еволюційними операторами, що дає змогу гарантувати коректність перетворень тестових наборів.* ***Висновки.*** *Запропонований підхід сприяє створенню універсального підходу до тестування, що забезпечує суттєве підвищення покриття коду й виявлення дефектів. Сфера використання досягнутих результатів: системи автоматизованого проєктування й діагностики для IoT, платформи тестування кіберфізичних систем, розроблення інструментарію для QA-інженерів у сфері Embedded Systems та Edge AI.*

Ключові слова: *Інтернет речей; інтелектуальний шлюз; генетичні алгоритми; універсальна алгебра; теорія категорій; синтез тестів.*

Бібліографічні описи / Bibliographic descriptions

Панченко В. І., Кучук Г. А. Теоретико-алгебраїчні основи еволюційного синтезу тестів компонентів інтелектуальних шлюзів високощільних IoT-систем. *Автоматизовані системи управління та прилади автоматики*. 2026. № 1 (188). С. 44–53. DOI: https://doi.org/10.30837/0135-1710.2026.188.044

Panchenko, V., Kuchuk, H. (2026), "Theoretical-algebraic basics of evolutionary test synthesis for gateways components of high-density IoT systems", *Management Information System and Devices*, No. 1 (188), P. 44–53. DOI: https://doi.org/10.30837/0135-1710.2026.188.044