UDC 004.78:004.89:004.032.6 DOI: 10.20535/2411-2976.22025.27-35

AI-POWERED WI-FI ACCESS CONTROLLERS: A NEW APPROACH TO WIRELESS NETWORK DESIGN

Andrii P. Bondarchuk, Nataliia V. Korshun, Oles A. Dibrivnyi, Svitlana M. Spivak

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

Background. Classical Wi-Fi architectures based on conventional access controllers are unable to provide stable, secure, and efficient wireless connectivity under modern conditions of high connection density and dynamic loads. This leads to frequent connection drops, inefficient use of network resources, and complicates proactive threat detection. As a result, organisations face decreased productivity, increased operational costs, and heightened cybersecurity risks.

Objective. The aim of the article is to present an approach to designing Wi-Fi wireless networks using artificial intelligence and genetic algorithms, and to develop a comprehensive model and algorithm for multi-criteria optimisation of the network infrastructure.

Methods. The research uses theoretical analysis of modern AI-based solutions, mathematical modelling of the access point placement optimisation problem, and the application of a genetic algorithm to find Pareto-optimal configurations. An original optimisation procedure is proposed, including stages of population generation, coverage assessment, fitness function calculation, and application of genetic operators.

Results. An innovative mathematical approach for optimising access point placement is proposed, considering not only technical parameters but also architectural features of premises, quality of service (QoS), energy efficiency, and security. A comparative analysis of modern AI solutions from leading vendors (Juniper Mist AI, HPE Aruba Networking Central, Cisco DNA Center) is conducted. A closed-loop optimisation algorithm is developed, combining genetic algorithms for initial design and AI systems for dynamic network adaptation during operation.

Conclusions. The research confirmed the high efficiency of integrating artificial intelligence and genetic algorithms for creating scalable, intelligent network infrastructures capable of real-time autonomous optimisation. The implementation of the proposed solutions significantly improves wireless communication quality, reduces operational costs, and ensures stable network performance under dynamic load conditions.

Keywords: *wireless networks; artificial intelligence; Wi-Fi; genetic algorithms; coverage optimisation; AI access controllers.*

Introduction

Modern business, education, and daily life are unimaginable without stable and secure wireless access. Wi-Fi has transformed from a convenient option into a critical communication artery that supports the operation of digital ecosystems, ranging from smart offices and IoT sensors to video surveillance systems and virtual reality. This creates unprecedented pressure on network infrastructure, demanding not just functionality but also high performance, reliability, and contextual awareness.

Traditional Wi-Fi architectures, based on classical access controllers, are reaching their limits. Their reactive operational model, relying on predefined rules and threshold values, is unable to effectively counter the dynamic chaos of the radio environment, the rapid increase in client numbers, and sophisticated cyber threats. Administrators are forced to "fight fires" manually, which complicates scaling and leads to unsatisfactory user experiences.

A new generation of network solutions is emerging to replace this approach, leveraging the power of artificial intelligence (AI) and machine learning (ML). At the heart of these systems are intelligent access controllers that transform Wi-Fi from a set of hardware into an intelligent, self-organising, and predictive platform. They do not merely execute commands but analyse, predict, and act autonomously.[1-2]

Main

Network design utilising intelligent controllers is based on several key principles that fundamentally distinguish them from traditional approaches.

Predictive analytics stands as one of the most powerful tools in the AI controller's arsenal. Unlike reactive systems that identify problems only after they occur, intelligent networks continuously analyse vast amounts of historical and real-time data to anticipate future scenarios. This enables a shift from a "fire-fighting" model to preventive management. By analysing signal degradation trends, the system can predict potential connection drops and proactively increase signal strength or prepare for seamless handover between access points. Thus, predictive analytics transforms the network from a passive infrastructure into an active participant that not only responds to changes but prepares for them. This significantly enhances network stability and prevents issues that users might not even notice, ensuring a continuous and high-quality operational experience.

The radio frequency (RF) environment is a dynamic and competitive space where Wi-Fi stability is influenced by numerous factors: neighbouring networks, electronic devices causing interference, physical obstacles, and constant user mobility. Traditional controllers periodically scan the airwaves and make adjustments, but these actions often lag behind real-time changes.

AI controllers implement the principle of continuous autonomous optimisation. They analyse the RF environment in real-time, gathering data from all access points, acting as a distributed radio monitoring system. Machine learning algorithms evaluate noise levels, channel load, and spectrum overlap, and based on this information, dynamically reassign access points to the least noisy and available channels. [3-4]

Furthermore, the system automatically regulates the transmission power of each access point. For instance, if one access point fails, the AI controller can boost the signal of adjacent points to fill the "dead zone," maintaining continuous coverage. It can also reduce power in areas with dense access point deployment to minimise mutual interference and enhance the network's overall throughput capacity.

This self-organising capability makes the network exceptionally adaptable to external conditions. It effectively counters interference that could not be predicted during the design phase and ensures stable and efficient use of the radio frequency spectrum without any human intervention, which is crucial for dense deployment environments such as apartment buildings or office centers.

Traditional network quality of service (QoS) metrics, such as signal level (RSSI), noise, and retransmission count, often do not adequately represent the true service quality perceived by the user. It is unnecessary for the user to be aware of these technical specifications, nor should they be required to understand them; they evaluate the network based on whether video freezes, whether voice calls drop, and how quickly web pages load. AI controllers are precisely oriented towards these subjective yet critically important factors.

The system analyses information by aggregating data from both network elements and the client devices themselves, using specialised agents or standard protocols. It can measure association time, packet loss, and latency/jitter for video conferencing systems or streaming services. The AI controller correlates all failures, identifies the root cause, and either resolves it autonomously (for example, by transferring the client to another access point) or provides the administrator with clear diagnostic information and specific remediation recommendations.

Thus, the focus shifts from device management to ensuring a successful outcome for the end-user, representing a fundamental change in the philosophy of building and maintaining wireless networks.

Behavioural security based on anomaly detection

Cyber threats to wireless networks are constantly evolving, and traditional protection methods like MAC address blocking or signature analysis are no longer effective against targeted attacks or previously unseen malware. AI offers a behavioural approach to security, based on anomaly detection.

In the first stage, the machine learning system builds a baseline profile of normal behaviour for each network, user, and device during a designated "learning period." This profile includes parameters such as typical times and volumes of data transmission, commonly used applications, and the protocols and servers to which connections are made. After the learning phase, the system begins monitoring all network activity for deviations from this established norm. For example, if a printer that normally transmits small amounts of data suddenly starts massively scanning the internal network, this is an anomaly. If a user account becomes active at 3 AM and starts bulk downloading confidential files, this is an anomaly. An attempt to spoof an access point (Evil Twin Attack) will also be detected by analysing behavioural differences compared to legitimate access points.

Upon detecting suspicious activity, the system can automatically take a range of measures: isolate the compromised device in a special segmented network (VLAN), reduce its priority, block its access to critical resources, or immediately alert the administrator with a detailed incident description. This approach enables the detection and neutralisation of zero-day threats and sophisticated APT attacks that evade traditional protection systems.

Simplified management and automation

The complexity of managing large, distributed Wi-Fi networks is one of the main challenges for IT departments. Administrators could spend hours troubleshooting a single complaint, reviewing logs from various devices. AI controllers radically change this paradigm by offering a simplified, intuitive interface and extensive automation of routine operations.

The central point of management becomes a single dashboard that displays high-level analytics instead of raw data: overall network health status, user satisfaction ratings, lists of the most active applications, and priority incidents. [6-7]

The extensive use of automation significantly reduces the time required to resolve typical problems. The system can automatically recover "frozen" access points, reconfigure security settings for new clients, generate compliance reports, and even suggest optimal locations for new equipment based on an analysis of current coverage.

Comparison of existing technologies

Table 1. The market offers several leading solutions implementing the described principles.

Criterion	**Traditional Controllers**	**Smart Controllers (e.g., Juniper Mist, HPE Aruba Networking Central)**
Problem Resolution Approach	Reactive (after complaints)	Proactive and Predictive
RF Optimisation	Based on static rules	Dynamic, autonomous, based on ML data analysis
Security	Signature analysis, Access Control Lists (ACL)	Anomaly detection, behavioural analysis
Management	Complex, requires deep knowledge	Simplified, with intuitive UI and built-in virtual assistant
Scalability	Limited by the complexity of manual management	High, thanks to automation
Analytics and Reporting	Basic network status reports	Deep QoE analytics, root-cause analysis

Juniper Mist AI utilises a virtual assistant that not only collects data but also understands user queries in natural language and provides recommendations. HPE Aruba Networking Central integrates AI to analyse telemetry from millions of devices, offering predictive recommendations. Cisco DNA Center also possesses powerful ML-based analytics capabilities for security and automation.

Let's examine each of these technologies in more detail.

Juniper implements an approach that combines several types of artificial intelligence. The foundation of the system is the Marvis virtual assistant, which uses Natural Language Processing (NLP) to communicate with administrators. For analytics, deep learning is used based on data from radio sensors (Virtual Network Assistant), enabling the detection of the most complex anomalies in the RF environment. Predictive analytics algorithms build models of network behaviour, forecasting congestion and other problems several hours before they occur. [9-10]

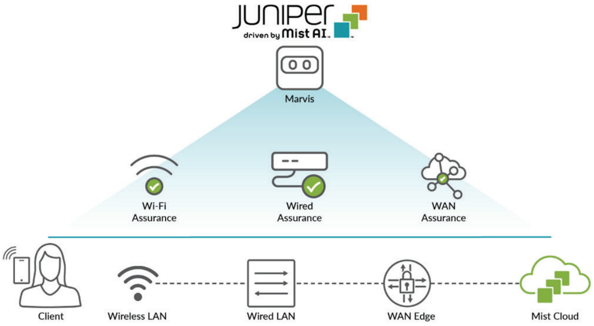

Fig. 1. – Juniper Mist AI architecture

Aruba uses machine learning to analyse telemetry from millions of devices through its cloud platform. A distinctive feature is the use of algorithm ensembles that combine classification, regression analysis, and clustering. The system applies predictive modelling for network upgrade recommendations, leveraging historical data from thousands of similar deployments. For security anomaly detection, unsupervised learning is used, enabling the identification of previously unknown threats without the need for signature updates.

Cisco emphasises supervised learning for classifying network events and semi-supervised learning for analysing user behaviour. The platform utilises Recurrent Neural Networks (RNNs) for time-series analysis of network traffic, which allows for the detection of complex attack patterns. To ensure Quality of Experience (QoE), a combination of classical ML algorithms (decision trees, random forest) is applied to correlate data from various sources—from RF metrics to application performance indicators.

Each vendor employs a unique combination of AI technologies: Juniper focuses on interactive NLP and deep learning for proactive anomaly detection, Aruba utilises scalable ML for predictive analytics based on cloud data, and Cisco integrates diverse ML algorithms for deep event correlation within enterprise networks.

A new approach to wireless network design

Wi-Fi network design has evolved from traditional methods to intelligent systems utilising artificial intelligence. Modern design involves creating adaptive infrastructure capable of self-diagnosis and autonomous optimisation. The integration of AI access controllers, which transform the design process from reactive to predictive, is gaining particular relevance. [11]

For organisations with a large number of users, network design must consider not only technical parameters but also operational specifics, connection density, and quality of service requirements. The use of AI controllers enables the creation of networks capable of adapting to dynamic load changes and ensuring stable connectivity in critically important areas.

The task of designing a Wi-Fi network can be formalised as a multi-criteria optimisation problem with constraints. For the AI approach, this translates to finding the optimal network parameters considering a set of quality criteria:

$$\begin{cases} \vec{x} = (x_1, \dots, x_m) \\ \tau_i(\vec{x}) \geq \sigma_i, i = \overline{1,n} \\ f_j(\vec{x}) \to max, j = \overline{1,k}, \vec{x} \in D \end{cases}$$

where, $\vec{x} = (x_1, \dots, x_m)$ is the vector of network parameters, m – is the number of variables; $\tau_i(\vec{x})$– are the constraint functions of the problem; σ_i– are the maximum permissible values of the constraints; f_j is the j- th optimality criterion, k – is the number of optimality criteria; D – is the set of permissible values for the optimisation variables.

In multi-criteria optimisation, there is an inherent uncertainty of goals, meaning only a compromise solution can be obtained.

Let $\overrightarrow{x_1}, \overrightarrow{x_2} \in D$. If for all criteria $f_1(\vec{x}), \dots, f_k(\vec{x})$ the inequalities $f_i(\overrightarrow{x_2}) \geq f_i(\overrightarrow{x_1}), i = 1, k$, hold, and at least one inequality is strict, then solution $\overrightarrow{x_2}$ is considered preferable to solution $\overrightarrow{x_1}$.

In multi-criteria optimisation, a point $\overrightarrow{x_0} \in D$ s called Pareto optimal if no other points $\vec{x} \in D$, exist that are preferable to $\overrightarrow{x_0}$. Pareto optimal points form a set called the Pareto front**.** The goal of multi-criteria optimisation is to identify this Pareto front from the set of all possible solutions.

Subsequently, the final solution from the set of Pareto-optimal solutions is selected either based on expert evaluation or by applying an additional criterion.

Numerous researchers successfully apply genetic algorithms to optimise Wi-Fi access point placement. These heuristic algorithms, based on the principles of natural selection, offer advantages such as high computation parallelization, parameter stability, and effectiveness for multi-criteria optimisation. However, the method also has limitations, including high computational complexity and the lack of universal stopping criteria.

The primary objective is the optimal placement of access points to ensure comprehensive coverage of educational buildings and seamless roaming. Modern technologies guarantee high-quality service even under high connection density, allowing for a focus on optimising coverage and network energy efficiency.

Contemporary AI systems utilise an enhanced version of this model, where the criteria encompass not only technical parameters but also Quality of Experience (QoE) metrics, security levels, and energy efficiency.

Genetic algorithms, as a component of AI systems, demonstrate high effectiveness for wireless network optimisation tasks. This heuristic approach, based on the principles of natural selection, enables finding optimal solutions under multi-criteria optimisation conditions, which is particularly crucial when designing complex network infrastructures.

Key advantages of genetic algorithms include adaptability to complex spatial configurations, the ability to account for the architectural features of an institution's premises, and effective operation within multidimensional search spaces for optimal solutions. This facilitates finding a balance between conflicting requirements for the network infrastructure. [13]

Modern AI controllers implement intelligent management of the radio frequency environment by utilising dynamic RF environment management based on big data analytics. The optimisation process involves three key components: continuous monitoring with telemetry collection from access points and client devices, predictive analytics for load forecasting, and autonomous adjustment of network parameters.

For organisations with a large number of users, this approach ensures automatic network adaptation to changes in user density throughout the day, the characteristics of different room types, and security requirements. This is achieved through dynamic power adjustment, optimal channel selection, and efficient load balancing.

The premises for wireless communication are modelled as a collection of walls with specified parameters:

$$W_i = \{f_i(x); x_i'; x_i''; h_i; \varepsilon_i^{int};\ \varepsilon_i^{ext}\}, i = 1, M$$

where:

M is the number of walls;

$f_i(x)$ is the equation of the i-th wall with boundaries $x_i'; x_i''$;

h_i is the thickness of the inner layer;

$\varepsilon_i^{int};\ \varepsilon_i^{ext}$ is the dielectric permittivity of the inner and outer wall layers, respectively.

Coverage quality criteria are defined as:

$$U_{ij} = \begin{cases} 1, \text{if at point } i \text{ the signal level from point } j \text{ is sufficient} \\ 0, \text{otherwise} \end{cases}$$

The objective function takes the form:

$$\begin{cases} max\ \Sigma_{i=1}^{R} \Sigma_{j=1}^{N} U_{ij}\ \varphi(\psi(x_i;\ y_i;\ x_j;\ y_j)) \\ \Sigma_{j=1}^{N} U_{ij} \leq 1, \forall_i \in\ [1, R] \end{cases}$$

where:

(x_i, y_i)- coordinates of room points;

(x_j, y_j) - coordinates of access points;

$\varphi(\psi)$- signal requirement satisfaction function.

The initial population generation process takes into account a number of critical factors, including the geometric constraints of the premises, the computational complexity of the algorithm, and technical limitations on the number of non-overlapping channels (specifically, the existence of only 3 such channels in the 2.4 GHz band).

Let us define the following terms*:* N – the initial number of access points to be deployed. The entire area of the premises is divided into a specific number of U^2 squares.

Generation Procedure*:*

1. Divide the area into U^2 squares (based on the condition $(U-1)^2 < N \leq U^2)$).
2. Randomly place access points within the squares.
3. Adjust positions near walls (if H < 0.5 m).
4. Set the initial transmission power (up to 20 dBm).

Fitness function:

$$F\ = \Sigma_i\ [w_i <\ W]\ c_i +\ \Sigma_i[l_i >\ 3]\ h_i$$

where:

$c_i = const + e^{(W-w_i)}$- penalty for weak signal;

$h_i = e^{(l_i-3)}$ - penalty for excessive coverage;

$const \geq N(e^W - 1)$ - normalisation constant dependent on the number of access points.

The mutation operator in the genetic algorithm implements a series of modifications to existing network configurations to maintain population diversity.

Mutation includes:

- Removal of access points (probability α);
- Addition of access points (probability β);
- Displacement of access points (probability γ);
- Power adjustment $\pm$ (probabilities θ_1, θ_2).

Crossover is performed with probabilities:

$$p_1c\ =\ F_1/(F_1\ +\ F_2), p_2c = 1 - p_1c$$

with combination of access point characteristics from parent solutions.

The proposed approach combines the advantages of modern artificial intelligence technologies with advanced optimisation methods. It accounts for complex architectural features of premises and provides multi-criteria optimisation, enabling the simultaneous consideration of various, often conflicting, network requirements.

The system demonstrates high efficiency due to its capability for parallel computing, which significantly accelerates the optimisation process. Furthermore, the algorithm can adapt to real-world operational conditions, ensuring stable network performance even with changing external factors and load.

Table 1.2 Comparative characteristics of network optimisation approaches

Criterion	**Traditional Methods**	**Genetic Algorithms**
Adaptability	Limited by predefined rules	High, with learning capability
Handling Complex Configurations	Partial	Complete, considering architectural features
Criteria Balancing	Prioritization of individual parameters	Multi-criteria optimisation

Scalability	Limited by manual configuration complexity	High, automated scaling
Response to Changes	Reactive	Predictive and proactive

Extended optimisation model for AI systems

The modern optimisation model for AI-driven networks incorporates additional parameters:

- Quality of Experience (QoE) metrics - connection time, streaming video stability, voice call quality;
- security parameters - anomaly detection level, threat isolation effectiveness;
- economic indicators - energy consumption, total cost of ownership, resource utilisation efficiency.

The fitness function takes the form:

$$F = \sum[\mathrm{w_iQoE - metrics}] + \sum[\mathrm{ecurity\ metrics}] + \sum[\mathrm{economic\ factors}]$$

where w_i is a parameter that quantitatively expresses the relative importance of each quality criterion in the multi-criteria network optimisation.

Optimal solutions obtained through genetic algorithms serve as the foundation for training AI access controllers. This integration enables:

- continuous improvement - AI controllers utilise real operational data to correct initial parameters;
- autonomous adaptation - the system can independently adjust network parameters in response to changing conditions;
- predictive maintenance - anticipating configuration change needs based on trend analysis.

Wi-Fi access point placement optimisation algorithm using artificial intelligence

The use of artificial intelligence in designing Wi-Fi networks for a large number of users opens up new possibilities for creating adaptive, efficient, and secure network infrastructures. The combination of genetic algorithms for initial optimisation and AI controllers for dynamic management enables the creation of networks capable of delivering high-quality service under the dynamic load conditions characteristic of modern companies. [7]

Modern wireless network design for organisations with a large number of users requires a fundamentally new approach that combines the precision of mathematical models with the intellectual capabilities of artificial intelligence. The proposed optimisation algorithm flowchart presents an innovative methodology that transforms the traditional design process into a dynamic, self-improving system. [13]

The algorithm implements a holistic approach to creating Wi-Fi infrastructure, where the initial design is organically combined with subsequent network operation and adaptation. The methodology is based on a hybrid model that integrates genetic algorithms for finding optimal topological solutions and machine learning for continuous real-time optimisation of network parameters. [5, 13]

A key feature of the proposed approach is the iterative "design-implementation-adaptation" cycle, which enables the creation of networks capable of operating effectively under conditions of high load dynamics, characteristic of organisations with a large number of users. The algorithm considers not only the technical parameters of radio coverage but also comprehensive requirements for service quality, security, and energy efficiency.

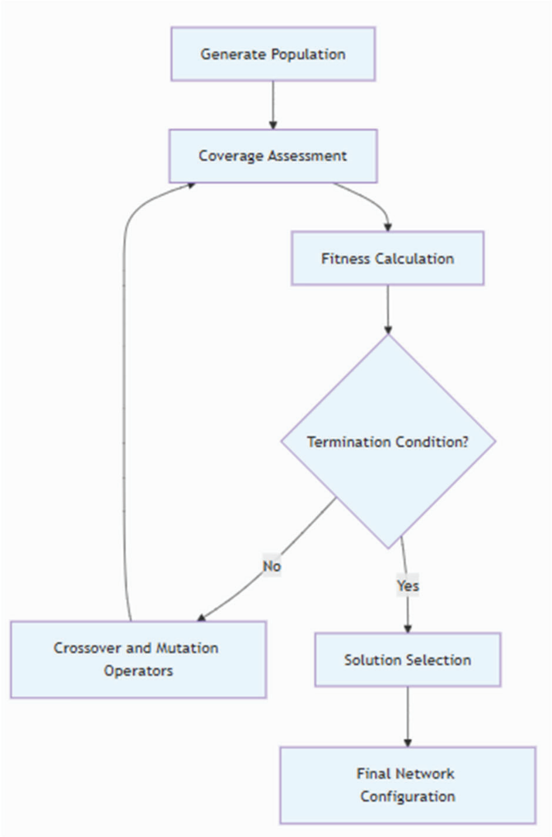

Fig. 2. Description of the Wi-Fi network optimisation algorithm flowchart

The presented flowchart describes the iterative process of optimising Wi-Fi access point placement using genetic algorithms.

Algorithm execution steps:

1. Generate Population - Generation of an initial population of solutions, where each individual represents a potential access point placement configuration.
2. Coverage Assessment - Evaluation of the wireless coverage quality for each configuration using RF modelling.
3. Fitness Calculation - Calculation of the fitness function, which considers:
   - Coverage Quality (QoE)
   - Energy Efficiency
   - Security Requirements
   - Implementation Cost
4. Termination Condition - Checking the algorithm's termination criteria:
   - Reaching the maximum number of iterations
   - Finding a satisfactory solution
   - Absence of significant improvement
5. Crossover and Mutation Operators - Application of genetic operators to create a new population:
   - Crossover of the best solutions
   - Random parameter mutations
6. Solution Selection - Selection of the optimal configuration from the Pareto front based on:
   - Cost Minimisation
   - Coverage Maximisation
   - Expert Evaluation
7. Final Network Configuration - Final network configuration, ready for deployment.

The proposed flowchart visualises the multi-stage process of wireless network optimisation, which begins with the analysis of input data regarding the architectural features of the premises and specific operational requirements. During the initialisation phase, the AI model is configured based on historical data, followed by a comprehensive assessment of the radio frequency environment using machine learning predictive models and an analysis of the user experience quality.[14]

This approach opens new possibilities for creating intelligent network infrastructures capable of providing stable, high-quality communication. The closed optimisation loop allows not only for generating effective initial solutions but also ensures their continuous improvement during operation, which is critically important for implementing modern digital services in educational institutions and corporate environments.

Conclusion

The study confirmed the high efficiency of integrating artificial intelligence and genetic algorithms for the design and optimisation of modern Wi-Fi wireless networks. The proposed approach enables a transition from traditional static methods to a dynamic, adaptive model capable of autonomously optimising network coverage, energy efficiency, and security in real-time.

The developed model and optimisation algorithm demonstrated the ability to effectively solve complex multi-criteria problems, considering technical parameters, Quality of Experience (QoE), architectural features of premises, and economic factors. The combination of genetic algorithms for finding optimal topological solutions with AI systems for subsequent dynamic adaptation ensures stable and reliable network operation even under conditions of high connection density, characteristic of modern educational and corporate environments.

A key advantage of the proposed approach is the implementation of a closed optimisation loop that combines the stages of design, implementation, and operation, ensuring continuous improvement of the network infrastructure. This not only significantly improves the quality of user service but also reduces operational costs through management automation and proactive problem resolution.

Prospects for further research include the improvement of machine learning models for more accurate load forecasting, the expansion of security system functionalities based on behavioural analysis, and integration with IoT ecosystems.

References

1. Zia, Kamran, Alessandro Chiumento, and Paul JM Havinga. "AI-enabled reliable QoS in multi-RAT wireless IoT networks: Prospects, challenges, and future directions." IEEE Open Journal of the Communications Society 3 (2022): 1906-1929. Retrieved from: DOI: 10.1109/OJCOMS.2022.3215731

2. ATAWIA, Ramy; GACANIN, Haris. Self-deployment of future indoor Wi-Fi networks: An artificial intelligence approach. In: GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017. pp. 1-6. Retrieved from: DOI: 10.1109/GLOCOM.2017.8254611

3. Jianjun, H. Wireless Access Point Configuration by Genetic Programming / H. Jianjun, E. Goodman // Evolutionary Computation. – 2001. – Vol. 1. – pp. 1178–1184. Retrieved from: DOI: 10.1109/CEC.2004.1330995

4. Mykyta Moshenchenko, Bohdan Zhurakovskyi, & Nataliia Korshun (2021). Optimization Algorithms of

Smart City Wireless Sensor Network Control. Cybersecurity Providing in Information and Telecommunication Systems II 2021, (3188), pp. 32-42. Retrieved from: http://ceur-ws.org/Vol-3188/

5. Vanhatupa, T. Genetic Algorithm to Optimize Node Placement and Configuration for WLAN Planning / T. Vanhatupa, M. Hannikainen, T. Hamalainen//Wireless Communication Systems. ISWCS 2007. 4th International Symposium, Trondheim 17–19 Oct. 2007. – Trondheim, 2007. – pp. 612–616. Retrieved from: DOI: 10.1109/ISWCS.2007.4392413

6. Sawaragi, Y. Theory of Multiobjective Optimization / Y. Sawaragi, H. Nakayama, T. Tanino. – Orlando: Academic Press, 1985. – 296 p.

7. Zhang, W., Yu, K., Wang, W., & Li, X. (2020). A self-adaptive AP selection algorithm based on multiobjective optimization for indoor WiFi positioning. IEEE Internet of Things Journal, 8(3), pp. 1406-1416. Retrieved from: DOI: 10.1109/JIOT.2020.3011402

8. Jaffres-Runser, K., Gorce, J. M., & Ubeda, S. (2007). QoS constrained wireless LAN optimization within a multiobjective framework. IEEE Wireless Communications, 13(6), pp. 26-33. Retrieved from: DOI: 10.1109/MWC.2006.275195

9. Juniper Mist WAN Assurance Configuration Guide/Overview of Juniper Mist WAN Assurance. Retrieved from: https://www.juniper.net/documentation/us/en/software/mist/mist-wan/topics/concept/mist-wan-overview.html

10. Julenius, J. (2025). Juniper Mist and Mist AI–an artificial intelligence-assisted network management environment. 35 p.

11. Maksuriwong, K. Wireless LAN access point placement using a multi-objective genetic algorithm / K. Maksuriwong, V. Varavithya, N. Chaiyaratana // Systems, Man and Cybernetics, 2003. IEEE International Conference, Washington, 5–8 Oct. 2003. – Washington, 2003. – Vol.2 – pp. 1944–1949. Retrieved from: DOI: 10.1109/ICSMC.2003.1244696

12. Kamenetsky, M. Coverage planning for outdoor wireless LAN systems / M. Kamenetsky, M. Unbehaun // Broadband Communications, 2002. Access, Transmission, Networking 2002. International Zurich Seminar, Zurich, 19-21 Feb. 2002. – Zurich, 2002. – pp. 491–496. Retrieved from: DOI: 10.1109/IZSBC.2002.991793

13. Yun, Z. An Integrated Method of Ray Tracing and Genetic Algorithm for Optimizing Coverage in Indoor Wireless Networks / Z.Yun, S.Lim, M. Iskander // Antennas and Wireless Propagation Letters. – 2008. – Vol.7. – pp. 145–148. Retrieved from: DOI: 10.1109/LAWP.2008.919358

14. B. Zhurakovskyi, et al., Smart house management system, in: Emerging Networking in the Digital Transformation Age, TCSET 2022, Lecture Notes in Electrical Engineering, vol 965, 2023, pp. 268–283. Retrieved from: doi:10.1007/978-3-031-24963-1_15

Бондарчук А.П., Коршун Н.В., Дібрівний О.А., Співак С.М.

Штучний інтелект у контролерах доступу WI-FI: новий підхід до проектування безпроводових мереж

Київський столичний університет ім. Бориса Грінченка, м. Київ, Україна

Проблематика. Класичні архітектури Wi-Fi, що базуються на звичайних контролерах доступу, не справляються із забезпеченням стабільного, безпечного та ефективного безпроводового зв'язку в сучасних умовах високої щільності підключень та динамічних навантажень. Це призводить до частих втрат зв'язку, неефективного використання мережевих ресурсів та ускладнює проактивне виявлення загроз безпеки. Як наслідок, організації стикаються зі зниженням продуктивності, зростанням експлуатаційних витрат і підвищеними ризиками кібербезпеки.

Мета досліджень. Метою статті є представлення підходу до проектування безпроводових мереж Wi-Fi з використанням штучного інтелекту та генетичних алгоритмів, а також розробка комплексної моделі та алгоритму багатокритеріальної оптимізації мережевої інфраструктури.

Методика реалізації. У дослідженні використано теоретичний аналіз сучасних рішень на основі ШІ, математичне моделювання задачі оптимізації розміщення точок доступу та застосування генетичного алгоритму для пошуку Парето-оптимальних конфігурацій. Запропоновано оригінальну процедуру оптимізації, що включає етапи генерації популяції, оцінки покриття, розрахунку функції придатності та застосування генетичних операторів.

Результати досліджень. Запропоновано інноваційний математичний підхід для оптимізації розміщення точок доступу, який враховує не лише технічні параметри, а й архітектурні особливості приміщень, якість обслуговування (QoS), енергоефективність та безпеку. Проведено порівняльний аналіз сучасних ШІ-рішень від провідних вендорів (Juniper Mist AI, HPE Aruba Networking Central, Cisco DNA Center). Розроблено алгоритм оптимізації із замкненим циклом, що поєднує генетичні алгоритми для початкового проектування та системи ШІ для динамічної адаптації мережі під час експлуатації.

Висновки. Дослідження підтвердило високу ефективність інтеграції штучного інтелекту та генетичних алгоритмів для створення масштабованих, інтелектуальних мережевих інфраструктур, здатних до автономної оптимізації в реальному часі. Впровадження запропонованих рішень значно покращує якість безпроводового зв'язку, знижує експлуатаційні витрати та забезпечує стабільну роботу мережі в умовах динамічного навантаження.

Ключові слова: *безпроводові мережі; штучний інтелект; Wi-Fi; генетичні алгоритми; оптимізація покриття; контролери доступу з ШІ.*

Received by the Editorial Office
October 30, 2025

Accepted for publication
December 1, 2025