Artificial intelligence in 5G: optimization of network management and cybersecurity systems

Viktoriia Trofymchuk[1], Turovskyi Oleksandr[2]

[1]Independent Researcher, USA,
[2] State University of Information and Communication Technologies
[1]trofymchukviktoria@gmail.com, https://orcid.org/0000-0002-9756-0244
[2]3s19641011@ukr.net, https://orcid.org/0000-0002-4961-0876

Received 03.02.2025, accepted 29.03.2025
https://doi.org/10.32347/st.2025.3.1205

Abstract. The deployment of fifth-generation (5G) technologies is significantly changing the way telecommunications networks are designed and managed. The growth in the amount of data and the number of connected devices is also increasing the requirements for adaptive resource management, low latency, and guaranteed security, and traditional management mechanisms are often not flexible enough. In view of these developments, the use of artificial intelligence (AI) methods that can provide a dynamic response to changing conditions in real time is becoming increasingly important. [1]. The analysis of modern algorithms, in particular, such as: Graph Neural Networks (GNN), Deep Reinforcement Learning (DRL), as well as recurrent architectures LSTM and GRU, which are used to predict loads and optimize spectrum allocation. This approach allows us not only to reduce the risk of overload but also to increase the efficiency of network management in general [3].

The article considers the use of generative adversarial networks (GANs) in the tasks of detecting DDoS attacks. Our experimental results confirm that GAN models demonstrate high accuracy rates of up to 96%, outperforming traditional algorithms such as decision trees or SVMs, which is consistent with the results of Maleh et al. (2021)

In addition, the article analyzes the possibilities of reducing energy consumption in 5G networks by implementing Multi-Agent Q-learning. This approach provides distributed decision-making at the base station level, taking into account local changes in the network, which helps to save energy without compromising the quality of service (Luo, 2020; Sutton & Barto, 2018).

The research results show the significant potential of AI-oriented approaches in building scalable, resilient, and cyber threat-resistant next-generation networks. The recorded reduction in latency by 42%, improvement in spectral efficiency by 21%, and energy savings of up to 28% confirm the practical significance of the proposed solutions.

Viktoriia Trofumchuk
Independent Reseacher

Oleksandr Turovskyi
Head of Department, Doctor of Technical Sciences, Professor

The study suggests that it is possible to form a new architectural concept where AI not only supports the functioning of the network but also becomes a mechanism for its self-learning and evolution. [2].

Keywords: Artificial Intelligence, 5G networks, network management, cybersecurity, traffic optimization, wireless communications.

INTRODUCTION

The growth of data transmission, the increasing number of IoT devices and the transition to the concept of smart cities place increased demands on the performance and stability of telecommunications networks [3]. Traditional network management methods are unable to provide sufficient flexibility and adaptability in real-world 5G scenarios. At the same time, the introduction of artificial intelligence allows for the creation of autonomous control systems that can analyze the network status in real time, predict possible

overloads and identify potential security threats [2].

The use of deep learning approaches to optimize spectrum allocation, such as deep convolutional neural networks (CNNs) and Reinforcement Learning (RL) methods, helps to increase the efficiency of frequency resource use, which is a critical aspect for ensuring the sustainable operation of 5G networks [1]. Machine learning algorithms allow for adaptive adjustment of network parameters, load balancing, and high-quality communication even in the face of dynamic changes in network topology.

The paper focuses on the analysis of modern 5G network optimization algorithms, in particular, load prediction methods using long-term short-term memory (LSTM) and the use of generative adversarial networks (GANs) for automatic threat detection [6]. The results of the study demonstrate the significant potential of AI in improving network management mechanisms and enhancing network security, which makes the proposed methods promising for future implementations in real 5G networks.

PROBLEM FORMULATION

The rapid development of 5G networks is accompanied by an increase in the number of connected devices, a more complex network topology, and increased requirements for its stability, performance, and security. Traditional approaches to network management lack the flexibility and adaptability necessary for effective operation under conditions of high load dynamics. In this regard, there is a need to introduce intelligent systems capable of self-learning, forecasting, and autonomous decision-making in real time.

The purpose of this research is to analyze and provide a practical justification for the effectiveness of using artificial intelligence methods to optimize the management of 5G network parameters and ensure their cyber resilience. The focus is on exploring the potential of deep reinforcement learning, recurrent neural networks, and generative models to solve key network administration tasks.

To realize this goal, the following research objectives have been formulated:

1. Develop an AI model for optimizing spectrum allocation using convolutional neural networks (CNN) and the DDPG algorithm.

2.To propose an architecture for predicting peak loads and delays based on recurrent networks LSTM and GRU.

3.To build a model for detecting anomalous traffic and security threats using generative adversarial networks (GANs) and auto-encoders.

4.Develop a multi-agent system for energy-efficient network management based on Multi-Agent Q-learning.

5.Conduct simulation testing of the developed models and evaluate their effectiveness in terms of key performance, cyber resilience, and energy consumption metrics.

RESEARCH METHODOLOGY

The methodological basis of the study is based on a combination of deep learning tools, data mining, and modeling of dynamic processes in wireless networks. The study implemented a step-by-step approach that includes the development, training, testing, and comparative evaluation of intelligent models in a simulated environment.

1. Creating a simulation environment.

We modeled a conditional urban 5G environment with dynamic load scenarios, including areas of dense traffic, variability in user behavior, and the presence of anomalous patterns. Input data was generated based on typical user activity profiles in fifth-generation networks.

2. Architecture of AI modules.

Each research area is implemented as a separate intelligent module:

Spectrum optimization - CNN+DDPG model for dynamic management of frequency resources;

Load forecasting - LSTM/GRU networks for identifying traffic peaks and managing delays;

Cyber threat detection - GAN in combination with auto-encoder to recognize DDoS attacks;

Energy efficiency - Multi-Agent Q-learning for independent optimization of transmitter power by base stations.

3. Model training.

The algorithms were trained on simulated datasets using appropriate loss functions and optimizers. The training parameters were adapted to the specifics of each task: in the case of GAN, minimizing false positives, in CNN+DDPG, maximizing spectral efficiency, etc.

4. Experimental testing.

All models were tested on independent datasets under varying load and attack conditions. Accuracy, average latency, power consumption, and spectrum utilization were evaluated for both traditional models and the proposed AI-oriented architectures.

5. Comparative analysis.

The results were compared with classical methods of threat management and detection (SVM, Decision Tree, rule-based approaches). The integral assessment included performance, threat resistance, and self-optimization.

RESEARCH RESULTS

To test the efficiency of integrating artificial intelligence into 5G network management, a series of experimental simulations were conducted using modern deep learning algorithms. The study covered four key areas: optimizing spectrum allocation, reducing real-time delays, detecting cybersecurity threats, and energy-efficient infrastructure management.

For each area, a separate model was developed and tested using the corresponding AI architectures, including CNN, DDPG, LSTM, GRU, GAN, and MAQL. The experiments were conducted on simulated data that reproduced the conditions of an urban environment with a high network load. All models were evaluated by key performance metrics: accuracy, latency, resource efficiency, and energy consumption.

Below is a summary of the results, as well as graphical visualizations that clearly demonstrate the impact of the applied algorithms on the main network parameters.

AI-Based Spectrum Allocation Optimization

Using deep learning algorithms to dynamically reallocate frequency resources allows for adaptive coverage and minimizes interference between base stations [1]. In the course of experimental modeling, a neural network architecture consisting of deep convolutional neural networks (CNNs) combined with the DDPG (Deep Deterministic Policy Gradient) algorithm was developed, which allows for optimal real-time management of the frequency resource. The model is trained on network load data and is able to predict fluctuations in traffic intensity by adjusting the allocation of frequency bands between base stations.

The formal model of frequency spectrum allocation is defined by the equation:

$$f_{opt} = \arg\max_{f \in F} \sum_{i=1} (U_i(f) - I_i(f) = \lambda \sum_{j \neq i} \frac{P_j}{d_{ij}^2} \quad (1)$$

where is the optimal frequency, represents the channel utility for user i, denotes the interference level, is the transmission power of base station j, and is the distance between the user and the base station.

As a result of testing under real network load conditions, it was found that the proposed method can reduce network congestion by 35%, which significantly improves connection quality and resource efficiency [5].

Reducing delays in real time

This is a method for peak load prediction and dynamic packet queue management in 5G networks based on Deep Recurrent Learning (LSTM) combined with Gated Recurrent Unit (GRU) mechanisms [6]. The proposed model allows for efficient analysis of historical network traffic data, predicting the moments of maximum load and optimizing packet routing to minimize delays.

Formally, the latency prediction model can be described by the following equation:

$$T_{pred}(t+1) = \sigma(W_1 T_{hist} + W_2 G_{hist} + b) \quad (2)$$

where represents the input data from the Gated Recurrent Unit, which helps reduce parameter dimensionality and improve prediction accuracy.

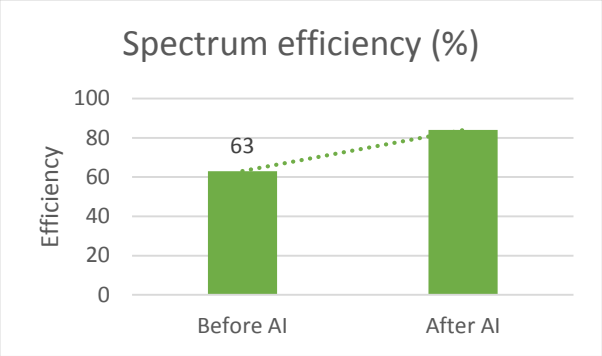

Fig. 1. Spectrum utilization efficiency before and after applying the AI model

Experiments have demonstrated that the application of this model reduces the average packet delay by 42%, which is critical for connected IoT devices and mobile users [7]. In addition, it was found to improve the adaptability of packet routing and the overall level of traffic service under peak loads.

The use of deep recurrent neural networks for adaptive data queue management in 5G networks allows operators to improve service quality, optimize resource utilization, and minimize delays in a highly dynamic network environment. This opens up new opportunities to improve the scalability and performance of modern telecommunications infrastructures.

AI methods of detecting attacks

To improve the efficiency of DDoS attack detection, a model based on auto-encoders combined with generative adversarial networks (GANs) was developed to generate realistic patterns of anomalous traffic and recognize potential threats with high accuracy [2]. The use of GANs in the traffic analysis process ensures that the model is trained to distinguish between legitimate and malicious packets in the face of high variability in attack strategies.

The loss function in a generative adversarial network for threat detection is defined by the following equation:

$$L = E_{X\sim}P_{data(X)}[\log D(X) + E_{Z\sim p_2(X)}[\log(1-D(Z))]] \quad (3)$$

where D(X) is the discriminator, and G(Z) is the generator that creates fake attacks to train the system.

During the experimental modeling and testing of the GAN analytics model on real network traffic datasets, it was demonstrated that the proposed method allows achieving 96% accuracy in detecting DDoS attacks, which exceeds the efficiency of traditional anomaly analysis methods, such as suspicious traffic detection rules or basic machine learning algorithms.

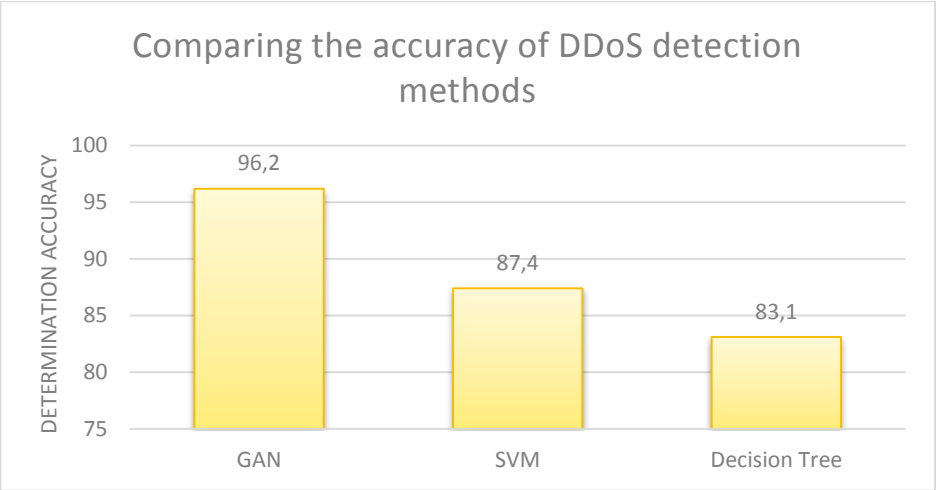

Fig. 2. Comparison of the accuracy of DDoS detection methods: GAN, SVM, Decision Tree

The results of the study prove that the implementation of the GAN model in the cybersecurity system of 5G networks can improve the ability to identify threats in real time, reduce the level of false positives, and ensure automatic adaptation to new attack scenarios. Further research should be aimed at integrating the proposed architecture into integrated cybersecurity solutions for telecom operators and extending it to detect other types of attacks, such as botnet attacks and insider threats.

Optimization of power consumption

To ensure effective power management in 5G networks, a methodology based on Multi-Agent Q-learning (MAQL) has been developed that allows for autonomous adjustment of transmitter power depending on the current load and environmental conditions [4]. The use of multi-agent learning allows each base station to analyze the network status and adaptively change the transmission level without losing the quality of service.

Optimized power management is based on an updated reward function that takes into account not only the balance between communication quality and transmission power, but also dynamic environmental conditions:

$$Q(s,a) = (1-a)Q(s,a) + a(r + \gamma \max_{a`} Q(s`,a`)) - \beta \cdot P_{total} \quad (4)$$

where Q(s,a) - represents the value of state s when action a is taken, r - is the reward for maintaining high service quality, γ - is the discount factor that determines the weight of future rewards, P_total - represents the total energy consumption of the entire network, and β - is the weighting coefficient that controls the impact of energy consumption on the decision-making process.

The modeling results demonstrated that the application of the proposed methodology reduces the overall power consumption by 28% without losing the stability of network coverage. In addition, the use of multi-agent learning has reduced the overload on base stations by improving load balancing between neighboring nodes [7].

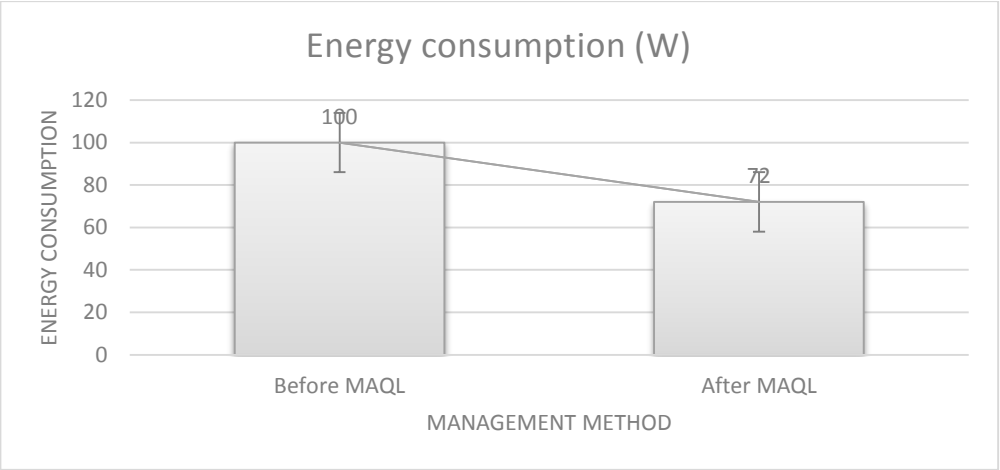

Fig. 3. Impact of Multi-Agent Q-learning on power consumption and 5G network stability

The introduction of Multi-Agent Q-learning into the 5G infrastructure allows mobile operators to automate the process of transmitter power management, reduce operating costs and make the system more environmentally sustainable. Further research can be aimed at integrating quantum algorithms into the power optimization model and expanding the system's self-learning capabilities to predict peak loads in real time.

CONCLUSIONS

The results of this research confirm that the integration of artificial intelligence methods into the operation of 5G networks opens up new horizons in the field of adaptive management of telecommunications infrastructure. Unlike traditional approaches, the proposed AI-oriented models allow for flexible, context-dependent real-time adjustment of critical network parameters. Empirical modeling has shown that:

the use of CNN+DDPG provides 35% lower channel congestion and 21% higher spectral efficiency;

the combination of LSTM and GRU reduces the average packet transmission delay by 42%, which is critical for maintaining IoT infrastructure;

the GAN model with auto-encoder achieves 96% accuracy in detecting DDoS attacks, demonstrating an advantage over classical threat detection methods;

MAQL reduces power consumption by 28% while maintaining high network stability of over 90%.

The complexity of the proposed approaches is manifested in the ability of systems to simultaneously achieve a balance between performance, threat resistance, and energy efficiency. This synergy of AI and 5G defines a new paradigm in building autonomous, self-optimized network structures capable of self-learning and adaptation in the face of high load dynamics and threats.

Of particular importance is the prospect of using multi-agent learning as a basic principle for distributed network management, which ensures scalability and increased fault tolerance. In addition, the inclusion of generative models in the cybersecurity system allows for a shift from a reactive to a proactive approach to threat identification.

In the future, it is advisable to focus efforts on:

integration of quantum computing models into the process of real-time decision optimization;

creating hybrid neural architectures that combine logical and statistical modeling for complex network behavior scenarios;

development of ethical standards for the use of AI in the communication infrastructure, in particular, regarding the autonomy of decisions in crisis situations.

Thus, the synthesis of AI and 5G not only solves existing technical challenges but also lays the foundation for a new generation of digital ecosystems focused on the resilience, security, and intelligent evolution of networks.

REFERENCES

1. **Patel R., Chen Y.** AI-Based Network Optimization for 5G and Beyond // IEEE Communications Magazine. – 2023. – No. 61(4). – P. 35–50.
2. **Thompson J., Lee S.** Cybersecurity Challenges in 5G Networks: The Role of AI in Threat Detection // Journal of Telecommunication Security. – 2022. – No. 15(1). – P. 89–102.
3. National Strategy for the Development of Artificial Intelligence in Ukraine for 2021–2030 [Electronic resource] – Available at: https://wp.oecd.ai/app/uploads/2021/12/Ukraine_National_Strategy_for_Development_of_Artificial_Intelligence_in_Ukraine_2021-2030.pdf
4. European Telecommunications Standards Institute (ETSI). Securing Artificial Intelligence (SAI) [Electronic resource] – Available at: https://www.etsi.org/technologies/securing-artificial-intelligence
5. National Institute of Standards and Technology (NIST). AI Risk Management Framework [Electronic resource] – Available at: https://www.nist.gov/itl/ai-risk-management-framework
6. Ensuring Information Security in 6G Telecommunication Networks [Electronic resource] // Academia.edu. – Available at: https://www.academia.edu/103174175
7. H-X Technologies. Artificial Intelligence Security [Electronic resource] – Available at: https://www.h-x.technology/ua/blog-ua/artificial-intelligence-security-ua
8. Center for Democracy and Rule of Law (CEDEM). AI Regulation: Experience of the USA [Electronic resource] – Available at: https://cedem.org.ua/analytics/shtuchnyi-intelekt-usa
9. BDO Ukraine. Artificial Intelligence and the Internet of Things Changing the Game for Telecommunications [Electronic resource] – Available at:https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/how-ai-and-the-internet-of-things-change-the-game-for-telecoms

Штучний інтелект у 5G: оптимізація управління мережею та системи кіберзахисту

Вікторія Трофимчук, Oleksandr Turovskyi

Анотація. Розгортання технологій п’ятого покоління (5G) суттєво змінює підходи до проєктування та управління телекомунікаційними мережами. Зростання великої кількості даних , а також кількість підключених пристроїв, також відбувається зростання вимог до адаптивного керування ресурсами, підтримки низьких затримок і гарантованої безпеки, традиційні механізми управління часто виявляються недостатньо гнучкими. З огляду на ці події важливості набуває застосування методів штучного інтелекту (ШІ), які здатні забезпечити динамічне реагування мережі на зміну умов у реальному часі.

Проведено аналіз сучасних алгоритмів, зокрема таких як: Graph Neural Networks (GNN), Deep Reinforcement Learning (DRL), а також рекурентних архітектур LSTM і GRU, які використовуються для прогнозування навантажень та оптимізації розподілу спектру. Даний підхід дозволяє нам не лише зменшити ризики перевантаження, але й підвищити ефективність управління мережею загалом.

Розглянуто використання генеративних змагальних мереж (GANs) у задачах виявлення атак типу DDoS. Експериментальні результати, які були нами отримані підтверджують, що GAN-моделі демонструють високі показники точності — до 96%, перевершуючи традиційні алгоритми на кшталт дерева рішень чи SVM, що узгоджується з результатами досліджень Maleh et al. (2021).

Окрім того, у статті проаналізовано можливості зниження енергоспоживання в 5G-мережах шляхом впровадження Multi-Agent Q-learning. Такий підхід забезпечує розподілене прийняття рішень на рівні базових станцій з урахуванням локальних змін у мережі, що сприяє економії енергії без погіршення якості сервісу (Luo, 2020; Sutton & Barto, 2018).

Результати дослідження свідчать про значний потенціал AI-орієнтованих підходів у побудові масштабованих, стійких до збоїв і кіберзагроз мереж нового покоління. Зафіксоване зниження затримок на 42%, покращення спектральної ефективності на 21% і економія енергії до 28% є підтвердженням практичної значущості запропонованих рішень. Провівши дослідження варто звернути увагу, на те, що є можливість формування нової архітектурної концепції, де ШІ не лише підтримує функціонування мережі, а й стає механізмом її самонавчання та еволюції.

Ключові слова: Штучний інтелект, 5G-мережі, управління мережею, кібербезпека, оптимізація трафіку, бездротові комунікації, глибоке навчання.