UDC 681.3 DOI: 10.18372/2073-4751.73.17640

Kulakov Y.O., Doctor of Technical Sciences,
orcid.org/0000-0002-8981-5649,
Korenko D.V.,
orcid.org/0000-0003-0463-189X

METHODS OF APPLYING ARTIFICIAL INTELLIGENCE IN SOFTWARE-DEFINED NETWORKS

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

ya.kulakov@gmail.com

Introduction

Rapid and high-quality decision-making in modern business has become critically important for the successful operation of enterprises in a competitive market. Ensuring productive and uninterrupted operation of the company's IT infrastructure is a key factor that enables achieving this goal.

The foundation of building a company's IT infrastructure lies in enterprise networks. The main objective of these networks is to ensure the guaranteed faultless operation of the enterprise's IT infrastructure. In this case, it involves not only the automation of business processes but also the secure storage of data and guaranteed continuous access to them, enabling effective communication and data exchange within the organization, as well as ensuring the security of these processes [1-3].

The application of Software-Defined Networking (SDN) in the construction of enterprise networks helps to ensure more efficient utilization of network resources and reduce network management costs. Software control enables quick and easy configuration changes, remote management of network devices, and network monitoring. Software-defined networks significantly reduce management costs and enhance network security levels.

In addition, software-configured networks allow for a higher level of security, as they allow you to block access to certain resources and applications in case of potential threats and establish access and authorization rules for network users.

In turn, the application of artificial intelligence (AI) in the field of information technology is one of the most relevant and rapidly growing areas of development. AI makes it possible to solve complex tasks faster and more efficiently, reduce the number of errors and increase the quality of work. Software-configured networks, in turn, are an important component of modern infrastructure.

Improving the quality of service (QoS) of traffic and reducing its design time can be achieved using multipath routing in SDN for centralized formation of multiple paths [4], unlike known methods that have high time complexity. Therefore, it was proposed to consider the possibility of using artificial intelligence to build traffic transfer routes and dynamic rerouting. This will significantly improve the performance and efficiency of SDN networks.

There are many methods of applying artificial intelligence in software-configured networks. It allows you to optimize various processes, for example, load distribution between network nodes or predict network load in the future. Also, AI helps to identify and eliminate problems in the network with the help of diagnostic and monitoring systems.

Certainly, artificial intelligence allows for the automation of SDN network management, reducing human intervention and increasing the accuracy and efficiency of management processes. For example, the use of AI methods in control systems to automatically determine the optimal network configuration or to automatically adjust network parameters.

It should also be noted that artificial intelligence can improve the security of enterprise networks. It allows you to detect and block malicious attacks on the network, as

well as detect suspicious behavior on the network.

Main part

Artificial intelligence (AI) is a branch of computer science that deals with the development of programs and systems that allow computers to make intelligent decisions based on data analysis and the use of various algorithms. The ideas that formed the basis of AI appeared in the middle of the 20th century, and since then AI has gone through many stages of development.

AI features key aspects such as machine learning, pattern recognition, natural language processing, autonomy, and expert systems.

In the modern world, artificial intelligence is widely used in transport networks (autonomous cars), as well as, especially recently, in UAV networks and voice recognition systems [3,4].

One of the promising fields is its implementation in smart networks (Smart Grids). Smart grids are electricity supply networks that use artificial intelligence to improve efficiency and energy efficiency. AI makes it possible to maximize the use of available resources, reduce energy costs and ensure uninterrupted operation of the network. The use of artificial intelligence in smart networks makes it possible to reduce electricity costs, ensure more accurate and efficient transmission and reduce the load on the network.

Another promising direction of using AI is its implementation in the Internet of Things (IoT) network. IoT is a network of Internet-connected devices that collect and process data. Artificial intelligence makes it possible to improve the functionality of the Internet of Things network, ensure the safety and protection of devices from malicious attacks, and also optimize the operation of the system as a whole.

Another direction is the construction of intelligent networks. Intelligent networks are networks that have the ability to self-organize and self-manage, as well as the ability to learn and adapt to changes in the environment. They allow you to perform many complex tasks, such as data routing, traffic management, detection and prevention of malicious attacks, and many others [5,6].

One of the most relevant areas of AI development is its application in software-configured networks. This is due to the need to increase the efficiency and productivity of SDN networks, which is a key component of modern infrastructure. AI allows you to create intelligent systems that are capable of data analysis, automatic control and management of processes in networks.

The use of artificial intelligence in software-configured networks allows you to automatically allocate resources, control network flows, detect and prevent cyber attacks, manage network devices, power consumption, and much more. For example, an intelligent network flow control system allows analyzing the level of network load and determining the optimal data transmission path, which will improve the network's efficiency [5-7].

Also, AI ensures network security and prevents cyber attacks. An intelligent network security monitoring system analyzes network traffic and detects potential threats such as viruses, malware and data interception attacks. In addition, AI is used to develop prognostic models that allow predicting possible network failures and taking timely measures to prevent them [9-11].

The use of AI in software-configured networks allows optimizing the operation of network devices. For example, intelligent systems are used to predict the volume of traffic and optimally distribute it between different network nodes. This makes it possible to increase the efficiency of using network resources and ensure stable and fast network operation. Also, AI allows analyzing user behavior, selecting personalized content and improving the work of technical support services [12].

Artificial intelligence allows solving the problem of a large amount of data collected in the network. Intelligent systems are used for automatic analysis and processing of this data, which allows to increase its usefulness.

The application of artificial intelligence in different types of networks contains

different aspects. For leading networks, for example, AI allows improving data routing, detecting abnormal situations in the network, warning about possible accidents and their elimination. For wireless networks, artificial intelligence allows to improve the quality of data transmission, manage network resources, warn about possible obstacles and eliminate them.

However, it should be noted that using AI in SDN networks requires a large amount of data for training algorithms. This means that it is necessary to provide access to a sufficient amount of data from various sources to ensure the high quality of the algorithms.

However, as already mentioned, the use of AI also brings its own challenges and issues, particularly with regard to privacy and data security. While artificial intelligence improves network efficiency and performance, it also creates new opportunities for cyberattacks that are difficult to detect and defend against.

One such challenge is the use of AI to breach network security. For example, phishing attacks will become more effective when using artificial intelligence, which increases the probability of an attacker successfully entering the network and obtaining the necessary information. In addition, AI can be used to create malicious programs that can harm the system, steal information, or demand a ransom [8,9].

Another problem is the issue of confidentiality and privacy of data. Artificial intelligence makes it possible to collect and analyze large volumes of data, which may contain personal information about network users. This violates the privacy of users and causes problems with compliance with the legislation on the protection of personal data [10,11].

Therefore, the use of artificial intelligence in software-configured networks has many advantages and opportunities, but also introduces certain challenges that must be considered when designing and implementing such systems.

On the one hand, the use of AI facilitates and accelerates data processing in SDN networks, provides more accurate and faster results and more effective management of network processes and resources. Artificial intelligence can reduce the response time to requests, ensuring speed and efficiency of user service, which is important in today's world, where speed and quality of service are key competitive advantages for businesses.

On the other hand, AI causes certain problems in SDN networks. For example, inadequate security of AI will lead to data theft, hacking of network infrastructure and other cybercrimes. In addition, an improperly designed AI system will lead to insufficient accuracy and reliability of results, which, in turn, will cause errors and erroneous decisions.

In the case of using AI in a networked environment, there are also problems with the use of different network standards and protocols, which will make it difficult to integrate AI with existing network systems and devices.

One of the solutions to these problems is the development and use of standards and protocols that support the integration of AI with existing network systems and ensure the security and reliability of network processes. In addition, it is important to develop effective algorithms to optimize the operation of networks using AI, as well as to ensure the appropriate level of training and support for specialists who work with software-configured networks and AI.

Therefore, the use of AI in SDN networks has significant advantages for increasing the efficiency and reliability of network processes. However, it also creates new challenges that require careful development and implementation of standards and protocols, as well as training and support of specialists who will be engaged in the development, management and support of enterprise SDN networks.

Conclusions

The application of artificial intelligence (AI) in enterprise SDN networks has the potential to improve network quality and efficiency, reduce costs, and improve security. However, its implementation also causes

certain problems. This includes issues of data security and privacy, as well as ethics and accountability for the actions of AI-based systems. It should be noted that the use of artificial intelligence should not replace the human factor, but should be an auxiliary tool to improve the efficiency and accuracy of the network.

In summary, we can conclude that the use of AI in enterprise SDN networks is an important stage in the development of technologies that improves the efficiency, security and accuracy of networks. The implementation of artificial intelligence in information systems is already happening, and large companies are actively using it in their products and investing in research and development in this field. Therefore, this direction of research is relevant and promising.

Literature

1. *Kulakov Y., Korenko D.* Modified Method of Traffic Engineering in DCN with a Ramified Topology. International Journal of Advanced Computer Science and Applications. – Vol. 12. – No. 12. – 2021. – P. 439-446.

2. *Korenko D., et al.* Creation of the method of multipath routing using known paths in software-defined networks. Technology audit and production reserves. – Vol. 4. – No. 2(66). – 2022. – P. 19-24.

3. *Teslyuk V., et al.* Optimal artificial neural network type selection method for usage in smart house systems. Sensors. – Vol. 21. – 2020. – 47 p.

4. *Muthukrishnan N., et al.* Brief history of artificial intelligence. Neuroimaging Clinics. – Vol. 30(4). – 2020. – P. 393-399.

5. *Alonso R.S., et al.* Deep reinforcement learning for the management of software-defined networks and network function virtualization in an edge-IoT architecture. Sustainability. – Vol. 12(14). – 2020. – P. 1-23.

6. *Shah H.A., Zhao L.* Multiagent deep-reinforcement-learning-based virtual resource allocation through network function virtualization in Internet of Things. IEEE Internet of Things Journal. – Vol. 8. – 2020. – P. 3410-3421.

7. *Huang X., et al.* Deep reinforcement learning for multimedia traffic control in software defined networking. IEEE Network. – Vol. 32. – 2018. – P. 35-41.

8. *Wang W., et al.* Anomaly detection of industrial control systems based on transfer learning. Tsinghua Science and Technology. – Vol. 26. – 2021. – P. 821-832.

9. *Xin Y., et al.* Machine learning and deep learning methods for cybersecurity. IEEE Access. – Vol. 6. – 2018. – P. 35365-35381.

10. *Li X., Zhang T.* An exploration on artificial intelligence application: From security, privacy and ethic perspective. 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). IEEE, 2017. – P. 416-420.

11. *Taddeo M.* Three ethical challenges of applications of artificial intelligence in cybersecurity. Minds and machines. – Vol. 29. – 2019. – P. 187-191.

12. *Yu C., et al.* DROM: Optimizing the routing in software-defined networks with deep reinforcement learning. IEEE Access. – Vol. 6. – 2018. – P. 64533-64539.

Kulakov Y.O., Korenko D.V.

METHODS OF APPLYING ARTIFICIAL INTELLIGENCE IN SOFTWARE-DEFINED NETWORKS

This work is devoted to the review of artificial intelligence application methods in enterprise networks using SDN technology. The paper examines the features and methods of using AI in these networks, as well as identifies potential problems that may arise.

The paper provides an overview of the main features of AI in enterprise SDN networks. AI has been found to automate many processes in the network, such as routing, monitoring, bandwidth management, and more. Using AI helps improve network efficiency, reduce costs, and improve security.

Potential problems that may arise when using AI were also highlighted. In particular, questions arise regarding data security and privacy, as well as ethics and responsibility for the actions of AI-based systems.

In general, the work puts forward the idea of using artificial intelligence in enterprise networks using SDN technology to improve network efficiency and ensure security. The methods of applying AI in these networks are reviewed, potential problems are identified, and prospective directions of research are outlined.

This work provides an overview of the features and capabilities of AI in enterprise SDN networks, and also lays the foundation for further research in this area. The implementation of artificial intelligence in enterprise networks is an urgent task, as it helps to improve the efficiency and security of networks and opens up new opportunities for their development.

***Keywords**: artificial intelligence, enterprise networks, SDN, Smart Grids, transport networks, UAV networks.*

Кулаков Ю.О., Коренко Д.В.

МЕТОДИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ

Ця робота присвячена огляду методів застосування штучного інтелекту у корпоративних мережах з використанням технології SDN. У роботі розглянуті особливості та методи використання ШІ у цих мережах, а також виявлені потенційні проблеми, які можуть виникнути.

У роботі проведено огляд основних особливостей ШІ у корпоративних SDN мережах. Виявлено, що ШІ дозволяє автоматизувати багато процесів у мережі, таких як маршрутизація, моніторинг, управління пропускною здатністю тощо. Використання ШІ сприяє покращенню ефективності мережі, зменшенню витрат і поліпшенню безпеки.

Також були висвітлені потенційні проблеми, які можуть виникнути при використанні ШІ. Зокрема, виникають питання стосовно безпеки та конфіденційності даних, а також етичність і відповідальність за дії систем, що базуються на ШІ.

Загалом, робота висуває ідею використання штучного інтелекту у корпоративних мережах з використанням технології SDN для підвищення ефективності роботи мережі та забезпечення безпеки. Оглянуті методи застосування ШІ в цих мережах, виявлені потенційні проблеми та намічені перспективні напрямки досліджень.

Ця робота дає загальний огляд особливостей та можливостей ШІ у корпоративних SDN мережах, а також ставить основу для подальших досліджень у цій області. Впровадження штучного інтелекту в корпоративні мережі є актуальним завданням, оскільки воно сприяє покращенню ефективності та безпеки мереж та відкриває нові можливості для їх розвитку.

***Ключові слова:** штучний інтелект, корпоративні мережі, SDN, Smart Grids, транспортні мережі, БПЛА мережі.*