DESIGN OF WIRELESS SENSOR NETWORKS BASED ON 5G AND IOT TECHNOLOGIES IN HIGHER EDUCATION INSTITUTIONS AND IMPROVEMENT OF DATA CYBERSECURITY ASSURANCE MECHANISMS

Saparov Umidjon Ali o'g'li
Student of group SI 25-13 Samarkand Branch of
Tashkent University of Information Technologies
Yorqinbek Ergashov Abduazizovich
Student of group KI 25-01 Samarkand Branch of
Tashkent University of Information Technologies
Email: ergashovyorqinbek630@gmail.com
Phone: +998 88 385 35 06

ABSTRACT

This article examines the issues of developing wireless sensor networks based on 5G and IoT technologies in higher education institutions and ensuring their efficient operation. In addition, the requirements for creating a digital smart campus environment necessary for managing data processes and network infrastructure are identified in order to establish a 5G/IoT network for scientific research purposes. The assessment of these requirements was carried out based on an existing campus network.Furthermore, the mechanisms for ensuring the cybersecurity of data transmitted through wireless sensor networks are analyzed.

The study explores modern methods of designing sensor networks, network architecture, as well as cryptographic and authentication techniques for data protection.The obtained results contribute to the development of smart campus systems in higher education institutions, ensuring secure data transmission, and improving network stability. The most promising innovative solutions can later be implemented at both national and international levels. In addition, the locally managed experimental 5G/IoT network infrastructure established within the campus can serve as a basis for developing new regulatory approaches and business models in response to expected changes in the future telecommunications market.

Keywords:5G technology, IoT, wireless sensor networks, smart campus, cybersecurity, data management, infrastructure, cryptographic methods, authentication, digital education.

INTRODUCTION

In recent years, the rapid development of information and communication technologies has led to significant changes in the education system. In particular, the advancement of 5G communication technologies and IoT (Internet of Things) systems

is creating new opportunities in various fields, including higher education institutions. 5G technology differs fundamentally from traditional wireless networks (Wi-Fi, 4G) due to its high bandwidth, minimal latency in data transmission, and the ability to connect millions of devices simultaneously. These technologies enable fast transmission of large volumes of data, establishment of communication between devices, and automation of various processes.In the process of creating modern digital infrastructure in higher education institutions, wireless sensor networks play an important role. Such networks allow monitoring of the educational process, control of laboratory equipment, management of energy consumption, and efficient organization of various information systems within the campus. At the same time, the widespread use of IoT devices makes ensuring data security one of the most pressing issues.

The relevance of this research lies in the fact that, under the rapid development of 5G and IoT technologies, the creation of modern wireless sensor networks in higher education institutions and ensuring data security within them are becoming increasingly important. Therefore, developing smart campus infrastructure based on these technologies and improving its efficiency is one of the key directions of modern scientific research.

According to the Presidential Decree of the Republic of Uzbekistan PF-60 (January 28, 2022) “On the Development Strategy of New Uzbekistan for 2022–2026,” the development of digital technologies, artificial intelligence, 5G, IoT, and information security has been identified as a priority area.Currently, many higher education institutions are striving to implement the Smart Campus concept. A smart campus is an integrated system aimed at managing and optimizing all infrastructure and services of a higher education institution based on modern digital technologies. Through these technologies, various devices, information systems, and infrastructure elements located within the campus are interconnected, exchange data in real time, and are efficiently managed. This requires the formation of a modern infrastructure based on 5G networks, IoT devices, and sensor systems.

However, in such systems, ensuring data reliability, transmission security, and network stability remains one of the key challenges. Therefore, it is necessary to conduct scientific research on the effective design of wireless sensor networks based on 5G and IoT technologies, improving their performance, and ensuring the cybersecurity of transmitted data.

This article analyzes the issues of organizing wireless sensor networks for higher education institutions, developing their architecture, and improving data protection mechanisms.The objective of the study is to identify the requirements for creating a 5G/IoT infrastructure based on an existing campus network, design sensor network architecture, and propose effective solutions for ensuring data security. Additionally, the article examines the role of locally managed experimental networks in shaping new

business models and regulatory approaches in the future telecommunications market.

MAIN PART

Design of a "smart campus" infrastructure based on 5g and iot in higher education institutions. In the process of creating modern digital infrastructure in higher education institutions, the concept of a smart campus based on 5G and IoT (Internet of Things) technologies plays an important role. A smart campus is an integrated system that connects all information systems, devices, and infrastructure elements within a campus through modern digital technologies, enabling real-time management and monitoring.

The high-speed data transmission capability of 5G technology, minimal latency, and the ability to connect a large number of devices simultaneously create a favorable environment for working with IoT devices. IoT devices, in turn, collect data from the campus environment through various sensors and transmit it to central servers via the network. As a result, it becomes possible to automate various processes within the campus infrastructure and manage them efficiently.A smart campus infrastructure based on 5G and IoT technologies is organized according to a multi-layered architecture. This architecture consists of three main layers: the perception layer, the communication layer, and the application layer. Each layer performs specific functions and ensures the efficient operation of the system.

The first layer is the **perception layer (IoT sensor networks)**. In this layer, data is collected from the campus environment using various sensor devices and IoT technologies. For example, smart classroom sensors monitor temperature, lighting levels, and student attendance. In addition, video surveillance is carried out using security cameras. Energy consumption sensors enable monitoring of electricity usage. Furthermore, RFID or ID card systems are used to identify students. The data collected from these devices is transmitted to special gateway devices.

The second layer is the **communication layer (5G network infrastructure)**, which ensures high-speed transmission of data collected from sensors. This layer includes 5G base stations (gNodeB), the 5G core network, and edge computing technologies. 5G technology is characterized by high data transmission speeds (10–20 Gbit/s) and minimal latency (1–5 milliseconds). Additionally, network slicing technology is used in 5G networks to create separate virtual channels for different services. For example, separate network segments are created for educational processes, security systems, and IoT devices.The third layer is the **application layer (data processing center)**. In this layer, data collected through sensor networks is stored and processed on central servers and cloud platforms. The application layer includes a smart university portal, artificial intelligence systems, and databases, through which data is analyzed and management decisions are made. With the help of artificial intelligence technologies, the efficiency of campus infrastructure is improved,

energy resources are optimized, and security systems are enhanced.

Thus, a smart campus infrastructure based on 5G and IoT technologies includes the processes of collecting data through sensor devices, transmitting it via 5G networks, and processing it in central systems. Such an integrated system enables efficient management of the educational process, rational use of energy resources, and обеспечение campus security in higher education institutions.

Data security and cyber protection mechanisms in wireless sensor networks. Wireless Sensor Networks (WSNs) are an important component of IoT technologies. These networks enable the collection, transmission, and processing of data from the environment through various sensor devices. In higher education institutions, such networks are widely used in the development of smart campus infrastructure. However, data transmitted through wireless networks may be exposed to various cybersecurity threats. Therefore, ensuring data security in wireless sensor networks is one of the key issues.

The main security threats in wireless sensor networks include unauthorized data access, modification of network traffic, denial-of-service (DoS) attacks, and node compromise. Such threats can negatively affect the stable operation of sensor networks. Therefore, it is necessary to use modern cyber protection mechanisms to ensure network security.

One of the main methods of ensuring data security is **cryptographic protection**. Through cryptography, transmitted data is encrypted and can only be accessed by authorized users. The encryption process is expressed by the following mathematical model:

$$C=E(K,M)$$

where:

- **M** – original data
- **K** – encryption key
- **E** – encryption function
- **C** – encrypted data

The process of recovering the data is carried out using the following formula:

$$M=D(K,C)$$

where:

- **D** – decryption function

Authentication mechanisms are also important for ensuring security in wireless sensor networks. Authentication systems allow only authorized devices and users to connect to the network, thereby protecting network nodes from unauthorized access.

In addition, modern IoT networks increasingly employ network monitoring and artificial intelligence-based security systems. These systems analyze network traffic,

detect abnormal activities, and help prevent cyberattacks.Thus, ensuring data security in wireless sensor networks requires the integrated use of cryptographic protection, authentication systems, network monitoring, and AI-based security technologies. This approach ensures the stable operation of smart campus infrastructure and preserves data integrity.

Ensuring data security in wireless sensor networks requires the integrated use of cryptographic encryption, authentication mechanisms, network monitoring, and artificial intelligence-based security technologies. These mechanisms ensure the stable and secure operation of smart campus infrastructure based on IoT and 5G technologies.

Economic and legal prospects of local 5g/iot network infrastructure and new business models. The development of 5G and IoT technologies is creating new economic opportunities in the telecommunications sector. In particular, the deployment of local 5G/IoT networks plays an important role in areas such as smart campuses, smart cities, and industrial automation. These local networks enable fast data transmission, efficient communication between devices, and automation of various services.

The economic prospects of local 5G/IoT network infrastructure are primarily associated with the formation of new services and business models. Based on such networks, it is possible to introduce various innovative services in sectors such as education, transportation, energy, security, and healthcare. For example, in a smart campus infrastructure, economic efficiency can be improved through services such as energy management, security systems, transport monitoring, and digital management of the educational process.The development of local 5G networks also leads to the emergence of new business models. In particular, service models such as Network-as-a-Service (NaaS), Platform-as-a-Service (PaaS), and IoT-as-a-Service (IoTaaS) become feasible. Through these models, network infrastructure is provided as a service, offering flexible and efficient solutions for users.

At the same time, legal regulation issues are of great importance in the implementation of local 5G/IoT networks. It is necessary to improve the regulatory framework related to licensing in telecommunications, ensuring data security, and protecting user data. In addition, the development of new infrastructure based on cooperation between the public and private sectors is also essential.

Local 5G/IoT networks are expected to intensify competition in the telecommunications market and create new economic opportunities in the future. These networks will improve the quality of digital services and accelerate the adoption of innovative technologies. As a result, local networks will play a significant role in economic development, digital transformation, and the formation of an innovative ecosystem.

DISCUSSION AND RESULTS

The widespread implementation of digital technologies in higher education institutions is one of the key factors in improving the efficiency of the education system. In particular, the development of 5G communication technologies and IoT systems is creating new opportunities for building smart campus infrastructure. These technologies make it possible to monitor campus processes in real time using various sensor devices, rapidly transmit data, and analyze it within centralized systems. Such infrastructure contributes to more efficient organization of the educational process, rational use of energy resources, and ensuring campus security.

During the research, the architecture of wireless sensor networks based on 5G and IoT technologies was analyzed. Data collected through sensor nodes is transmitted to the 5G network via gateway devices and then processed on central servers or cloud platforms. This process enables high-speed transmission and analysis of large volumes of data.As a result, various campus systems—including security systems, energy management, laboratory equipment, and educational monitoring systems—can be managed through a unified digital platform.

Ensuring data security in wireless sensor networks is also of great importance. The increasing number of IoT devices amplifies network security threats. Therefore, it is necessary to use cryptographic encryption methods, authentication mechanisms, and network monitoring systems to protect transmitted data. These mechanisms ensure the confidentiality, integrity, and reliability of data. In addition, the use of artificial intelligence and data analytics technologies makes it possible to detect abnormal activities in the network and prevent cyberattacks.

The development of local 5G/IoT networks also has significant economic prospects. Such networks create a foundation for the emergence of new services and business models. For example, smart campus services, IoT platforms, and digital services based on network infrastructure can optimize the operations of educational institutions. At the same time, improving the regulatory framework in telecommunications, ensuring data security, and developing the digital services market are important tasks.

The research results show that the integration of 5G and IoT technologies provides an effective technological foundation for forming smart campus infrastructure in higher education institutions. These technologies enable real-time monitoring of various processes through sensor devices, fast data transmission, and efficient data analysis. As a result, the management of the educational process, control of infrastructure systems, and efficient use of resources are significantly improved.The development of an optimal architecture for wireless sensor networks ensures the stable and efficient operation of campus infrastructure. The integration of sensor nodes, gateway devices, 5G networks, and cloud computing platforms enables rapid processing of large volumes of data. This serves as an important technological basis for implementing

modern digital management systems in educational institutions.

Ensuring data security plays a crucial role in the reliable operation of wireless sensor networks. By using cryptographic encryption, authentication systems, and network monitoring mechanisms, it is possible to ensure the confidentiality and integrity of data. This contributes to enhancing cybersecurity in networks based on IoT devices.Furthermore, the implementation of local 5G/IoT networks creates new economic opportunities in the telecommunications market. Based on such networks, it is possible to develop various digital services, IoT platforms, and smart infrastructure systems. As a result, the process of digital transformation accelerates, and an ecosystem of innovative services is formed. This process not only ensures the digital development of higher education institutions but also contributes significantly to the future development of smart cities and the digital economy.

CONCLUSION

This study comprehensively analyzed the issues of organizing wireless sensor networks based on 5G and IoT technologies in higher education institutions, developing smart campus infrastructure, and ensuring data cybersecurity. In the context of the rapid development of information and communication technologies, the creation of modern digital infrastructure in the education system is becoming increasingly important. In particular, the integration of 5G communication technologies and IoT devices enables high-speed transmission of large volumes of data, effective interaction between various devices, and automation of the educational process.

The research results show that wireless sensor networks organized based on the integration of 5G and IoT technologies significantly improve the efficiency of campus infrastructure. With the help of sensor devices, it becomes possible to monitor various processes on campus in real time, control energy consumption, manage security systems, and efficiently organize the educational process. At the same time, developing an optimal network architecture ensures the stable operation of data transmission and processing processes.

The study also revealed that ensuring data security in wireless sensor networks is one of the key factors. The widespread use of IoT devices introduces new security threats. Therefore, the use of cryptographic encryption methods, authentication mechanisms, and network monitoring systems plays an important role in ensuring data confidentiality and integrity. The application of these mechanisms makes it possible to ensure the stable operation of wireless sensor networks and enhance the level of cybersecurity.

In addition, the research findings indicate that the implementation of local 5G/IoT network infrastructure contributes to the emergence of new economic opportunities and innovative business models in the telecommunications sector. Based on smart campus infrastructure, it becomes possible to introduce various digital services,

manage data through IoT platforms, and utilize network infrastructure as a service. This not only increases the efficiency of the education system but also contributes significantly to the development of the digital economy.

In conclusion, wireless sensor networks based on 5G and IoT technologies are one of the key technological foundations for creating smart campus infrastructure in higher education institutions. The implementation of these technologies enables the acceleration of digital transformation, efficient management of infrastructure systems, and обеспечение data security in educational institutions. In the future, further development of 5G and IoT technologies, along with their integration with artificial intelligence and big data technologies, will make it possible to further improve smart campus systems and form an ecosystem of innovative services.

REFERENCES

1. Decree of the President of the Republic of Uzbekistan No. PF–60 dated January 28, 2022. “On the Development Strategy of New Uzbekistan for 2022–2026.”
2. Resolution of the President of the Republic of Uzbekistan No. PQ–200 dated July 4, 2023. “On Measures to Effectively Organize Public Administration in the Field of Higher Education, Science and Innovation within the Framework of Administrative Reforms.”
3. Andrew S. Tanenbaum, David J. Wetherall. Computer Networks. – New Jersey: Pearson Education, 2011.
4. William Stallings. Cryptography and Network Security: Principles and Practice. – New York: Pearson, 2017.
5. Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci. Wireless Sensor Networks: A Survey. – Computer Networks Journal, 2002.
6. Yonggang Zhang, Min Chen. 5G Wireless Networks: Key Technology and Applications. – Springer, 2019.
7. Ala Al-Fuqaha, Mehdi Guizani, Mohsen Mohammadi, Mona Aledhari, Mohammed Ayyash. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. – IEEE Communications Surveys & Tutorials, 2015.
8. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. – Future Generation Computer Systems, 2013.
9. Sabrina Sicari, Alessandro Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini. Security, Privacy and Trust in Internet of Things: The Road Ahead. – Computer Networks, 2015.
10. Daniel Minoli, Kazem Sohraby, Benedetto Occhiogrosso. IoT Considerations, Requirements and Architectures for Smart Buildings and Smart Cities. – IEEE Internet of Things Journal, 2017.