Вісник Тернопільського національного технічного університету
https://doi.org/10.33108/visnyk_tntu
Scientific Journal of the Ternopil National Technical University
2025, № 3 (119) https://doi.org/10.33108/visnyk_tntu2025.03
ISSN 2522-4433. Web: ***visnyk.tntu.edu.ua***

UDC 004.7:004.8:621.3

ADAPTIVE MULTI-PROTOCOL COMMUNICATION FOR ENERGY SYSTEMS

Andrii Voloshchuk; Halyna Osukhivska

Ternopil Ivan Puluj National Technical University,
Ternopil, Ukraine

Abstract. *This paper examines approaches to implementing adaptive multi-protocol communication in energy systems undergoing transformation in the context of distributed generation growth and Smart Grid concept development. An architecture is proposed that integrates OpenID Connect (a unified authentication provider) with a machine learning module for dynamic selection of optimal data transmission protocols among MQTT, CoAP, HTTPS protocols and legacy systems. The solution is based on employing widely-used algorithms (Random Forest, neural networks, logistic regression) for real-time communication efficiency prediction. The system ensures flexible, secure, and scalable management of heterogeneous devices through a unified control center. The obtained results demonstrate potential for communication cost reduction, reliability enhancement, and foundation establishment for implementing intelligent communication systems in the energy sector with automatic protocol switching.*

Key words: *energy networks, energy efficiency, communication protocols, machine learning methods, adaptive protocol selection.*

https://doi.org/10.33108/visnyk_tntu2025.03.097 *Received 25.08.2025*

1. INTRODUCTION

Today's energy infrastructure is undergoing radical changes under the influence of intensive deployment of renewable energy sources, expansion of distributed generation, and implementation of the smart grid concept. Forecast studies by the International Energy Agency indicate rapid growth in the share of distributed energy resources, which will reach 30% of the global energy system by 2030 [1]. The increasing complexity of energy networks is accompanied by a significant increase in the number of connected devices, according to forecasts by IoT Analytics (Fig. 1). The global number of connected IoT devices demonstrates exponential growth from 15.9 billion in 2023 to 41.1 billion by 2030, representing a compound annual growth rate (CAGR) of 14% [2]. This dynamic emphasizes the critical importance of selecting scalable and efficient data transmission protocols for energy systems. Therefore, this trend requires high-tech solutions for efficient data transmission between network components.

Studies of statistical characteristics of electricity consumption reveal distinct cyclical and periodic patterns of loads, which creates prerequisites for taking such patterns into account in order to optimize data transmission protocols according to predicted operating modes. In this context, mathematical modeling of electricity consumption characteristics becomes a fundamental basis for creating predictive systems and control algorithms. The methodological toolkit for statistical evaluation of energy consumption characteristics relies on the mathematical apparatus of probability theory and mathematical statistics for building stochastic models.

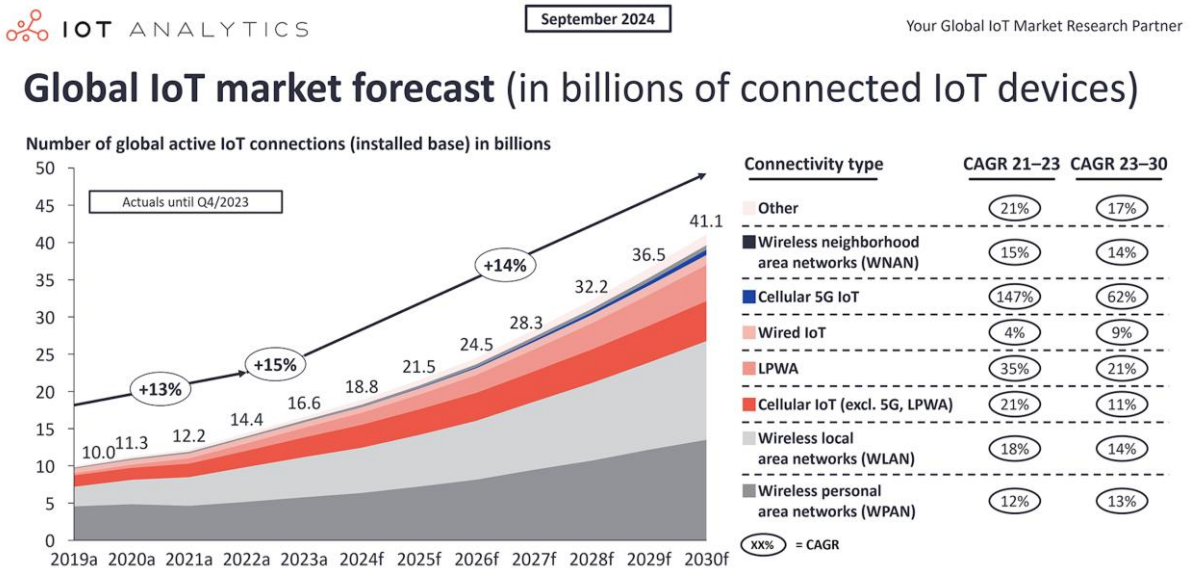

Figure 1. Dynamics of growth in the number of connected IoT devices until 2030 [2]

Therefore, the selection of optimal network protocols in the context of modern Smart Grid networks and SCADA systems becomes particularly relevant, taking into account energy loads at a specific point in time, when ensuring stable functioning is of critical importance [3, 4].

Analysis of publication activity in key areas of «energy efficiency» and «energy networks» demonstrates rapid growth of scientific interest in this topic. According to data from Scopus and Web of Science bibliometric databases, the number of publications on energy efficiency has almost doubled in the last three years, and research on energy networks shows an even more pronounced growth dynamic (Fig. 2).

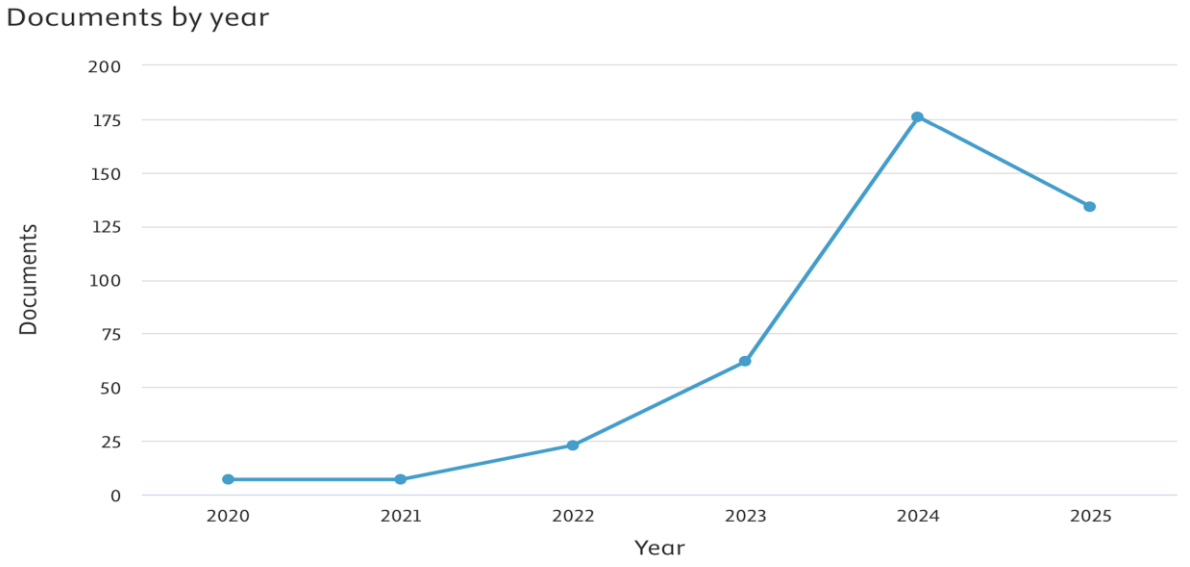

Figure 2. Dynamics of publication growth in the fields of «energy efficiency» and «energy networks» during 2020–2025, based on data from Scopus and Web of Science bibliometric databases

This indicates increased attention from the global scientific community to issues of energy system optimization, especially in terms of data transmission protocols and communication technologies. In particular, there is a significant increase in the number of

publications devoted to the application of machine learning methods for optimizing the selection of data transmission protocols in intelligent energy networks

Based on bibliometric data from Scopus and Web of Science, the distribution of scientific publications across subject areas highlights the prominent role of Computer Science (Fig. 3) and substantiates the relevance of research in this domain.

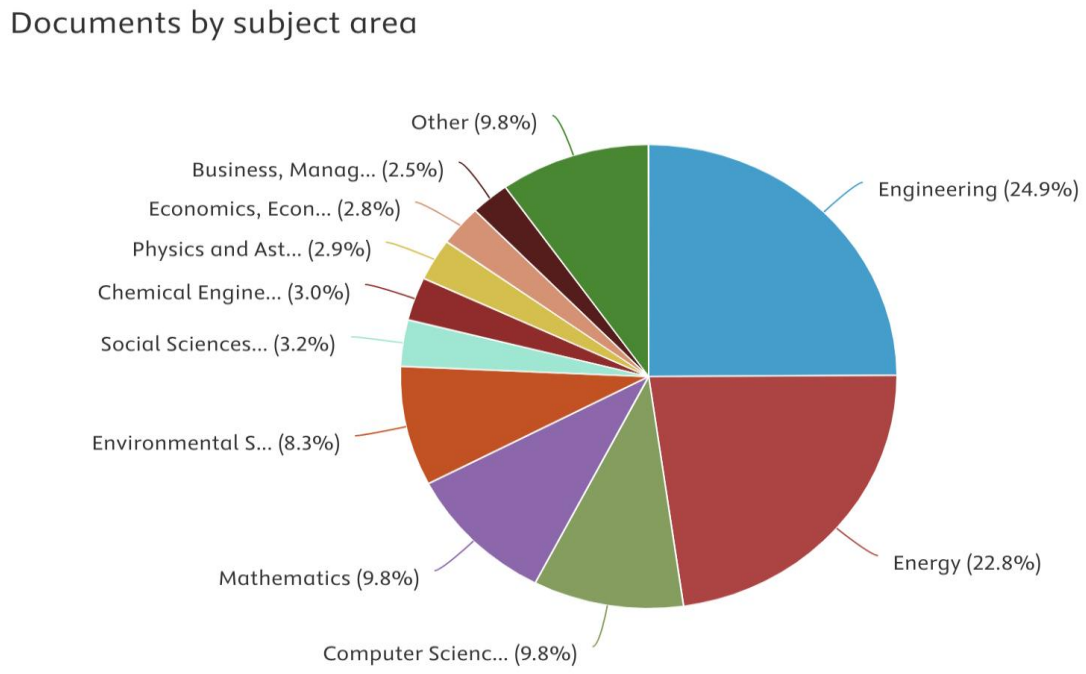

Figure 3. Analysis of publication activity distribution by main subject areas

The synergy of energy consumption modeling results with advanced network technologies creates powerful potential for achieving optimal balance between energy efficiency, reliability, and speed of data transmission systems in energy systems. The evolutionary transition from centralized models to decentralized Smart Grid architectures necessitates a fundamental rethinking of approaches to information exchange organization. Optimizing the balance between data processing speed and transmission reliability represents a key challenge in designing modern energy systems [5, 6, 7].

2. MULTI-PROTOCOL COMMUNICATION IN ENERGY SYSTEMS

An effective solution for optimizing the balance between data processing speed and transmission reliability is the use of an OIDC identity provider. Traffic optimization in networks at the level of software architecture and data representation is critically important for energy systems [8]. Such a task requires the development of comprehensive solutions capable of flexible interaction with various data transmission protocols and ensuring system scalability with the growth in the number of connected devices. It is important to note that the implementation of technologies for flexible management of communication protocols in real time using centralized authentication and data transmission efficiency prediction algorithms is accompanied by a number of challenges related to the need for rapid processing and secure transmission of significant data arrays from peripheral devices to centralized analytics and decision-making servers. In this context, automated selection of data transmission protocols in energy systems is important.

Figure 4 presents a generalized architecture for connecting a unified OIDC provider for an energy system, which includes various types of devices (MQTT sensors, CoAP controllers, HTTPS clients, Legacy systems) with their protocols, an OIDC provider with internal components (authentication, authorization, ML module), and target services (analytics, management, data storage).

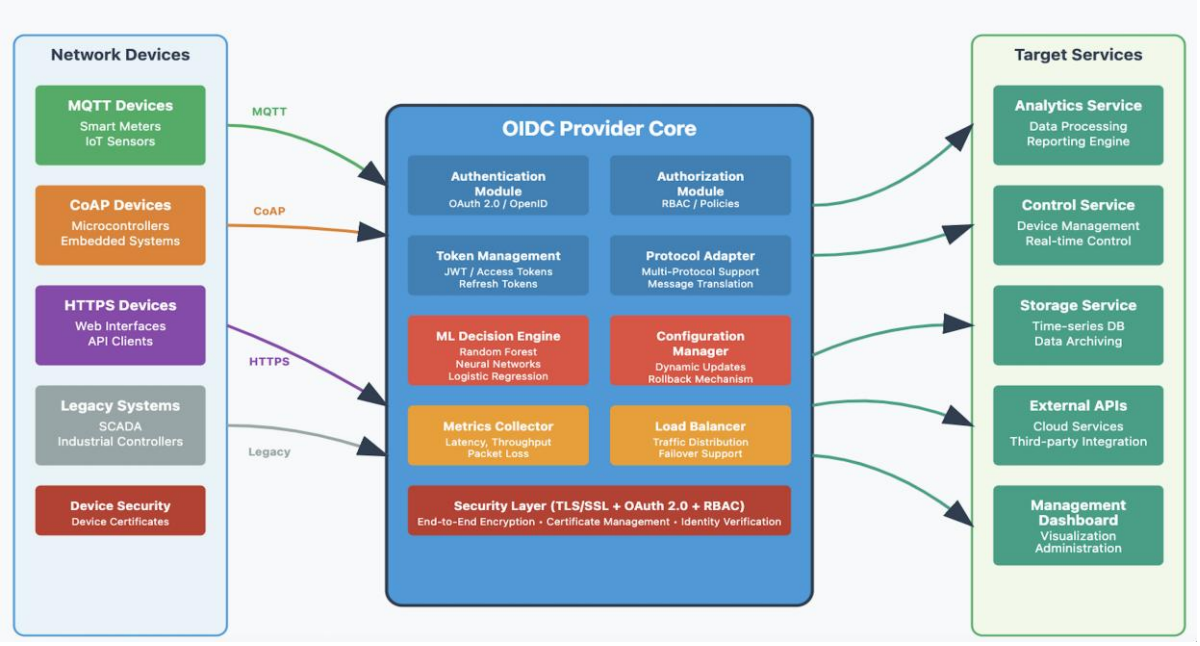

Figure 4. OIDC provider architecture with multi-protocol communication support

The presented architectural scheme demonstrates a comprehensive OIDC provider system with multi-protocol communication support, specifically designed for intelligent energy networks. The architecture is built on the principle of centralized management, where the OIDC provider acts as a key orchestration component that ensures unified data flow between heterogeneous network devices and target services.

The network component of the scheme represents various categories of network devices, each characterized by specific communication protocols and functional purposes. MQTT devices, including smart meters and IoT sensors, provide telemetric data collection with minimal energy consumption thanks to the efficient "publisher-subscriber" architecture. CoAP devices, represented by microcontrollers and embedded systems, are optimized for operation under strict resource constraints and ensure reliable data transmission through UDP-based transport. HTTPS devices, including web interfaces and API clients, guarantee a high level of security through TLS/SSL encryption, although this is accompanied by increased computational resource requirements. Legacy systems, such as SCADA and industrial controllers, are integrated through specialized protocol adapters, ensuring compatibility with existing energy infrastructure.

The central component of the scheme represents the OIDC provider as a multifunctional system consisting of several interconnected modules. Verification of digital identifiers of devices and users is implemented through the use of the OAuth 2.0 Authorization Framework [14] and the OpenID Connect standards [15]. The authorization module applies RBAC policies to ensure granular access control to system resources. The token management system provides generation, validation, and rotation of JWT tokens with corresponding metadata and permissions. The protocol adapter performs translation and standardization functions for messages between different communication protocols, ensuring seamless integration of heterogeneous devices.

The ML protocol selection module deserves special attention, as it uses three complementary machine learning algorithms. Random Forest provides analysis of complex interactions between network parameters and optimal protocol selection. Neural Networks model nonlinear dependencies between device characteristics, network conditions, and protocol performance. Logistic Regression provides interpretable baseline solutions and serves as a fallback mechanism when there is insufficient data for more complex models.

The metrics collection module continuously monitors key network performance indicators, including transmission delay, packet loss rate, and throughput. These metrics serve as input data for ML algorithms and provide real-time optimization of protocol solutions. The Load Balancer ensures intelligent traffic distribution between different services and implements failover mechanisms to maintain high system availability.

The target services scheme demonstrates the architecture of target services, each specializing in specific aspects of energy data processing. Analytics Service implements advanced big data processing algorithms for generating insights and predictive analytics in the energy domain. Control Service provides real-time device management and automation of technological processes with minimal response delay. Storage Service implements time-series databases for efficient storage and archiving of telemetric data with optimized compression and indexing.

The External APIs Module ensures integration with cloud services and third-party systems through standardized REST and GraphQL interfaces. The Management Dashboard provides comprehensive visualization of system status, performance metrics, and administrative functionality for energy network operators.

The architecture enables a multi-level security model that includes device-level authentication through digital certificates, transport-level encryption through TLS/SSL protocols, and application-level authorization through OAuth 2.0 tokens. End-to-end encryption ensures data integrity and confidentiality throughout the entire lifecycle from source to target service. This allows ensuring a unified level of security and digital identity management for all types of devices regardless of the underlying protocol (MQTT, CoAP, HTTPS, Legacy).

The use of multi-protocol communication in energy systems allows selecting the most optimal data transmission protocol at a specific moment, taking into account various influences on the energy system. Comparative analysis of the functional capabilities of main communication protocols in energy systems reveals their specific characteristics and limitations. The MQTT protocol, based on the "publisher-subscriber" principle, demonstrates high efficiency for IoT devices with limited energy resources due to minimal 2-byte packet headers, low delays, and stable operation under unstable connection conditions [9, 10]. However, the basic version of MQTT has limited built-in encryption capabilities and "request-response" pattern implementation.

The CoAP protocol, designed for resource-constrained networks, uses efficient binary encoding with caching support and follows REST architectural principles [11]. Its functioning based on the UDP transport protocol significantly reduces communication overhead costs, but does not guarantee reliable message delivery. Additional limitations are related to scaling for large networks and difficulties passing through NAT and firewalls.

The HTTPS protocol is distinguished by a high level of security due to TLS/SSL encryption, which prevents data interception or modification during transmission [12, 13]. However, the high level of security is accompanied by increased energy consumption due to cryptographic calculations, significant hardware resource requirements, and a lengthy connection establishment process.

Unlike using specialized solutions from individual suppliers (such as AWS IoT Core), our developed system implements an OpenID Connect (OIDC) provider as a universal authentication and data collection mechanism for all protocols regardless of their features. This standardized approach ensures seamless integration regardless of the underlying protocol, increasing system interoperability while maintaining information security requirements. The

OIDC provider unifies authentication processes and implements a unified security model that functions effectively in MQTT, CoAP, and HTTPS environments without additional modifications.

The dynamic system update process is implemented through a multi-level automatic reconfiguration mechanism. First, the metrics collection system continuously monitors key network performance indicators (delay, packet loss, throughput) at 30-second intervals and transmits data to the centralized analytics module. The machine learning module processes the obtained metrics using three trained models (Random Forest, Neural Networks, Logistic Regression) and generates recommendations for the optimal protocol for current conditions. In case of recommendation changes, the system initiates gradual protocol switching through the OIDC provider: first, access tokens for all devices are updated with new protocol parameters, then new connections are gradually activated (starting with 10% of devices for testing), and only after confirming stable operation does complete switching of the entire network occur. The rollback mechanism allows automatic return to the previous protocol in case critical errors are detected during a 5-minute observation window after switching.

The proposed approach significantly simplifies management of heterogeneous devices in energy networks, optimizes data transmission processes, ensures flexible scaling, and increases overall operational efficiency of all components, while implementing a protocol-agnostic security model and centralized digital identity management.

3. RESEARCH METHODS AND RESULTS

Efficient data exchange between energy network nodes requires the use of modern communication protocols that ensure reliability, minimal delays, and energy efficiency. The selection of optimal data transmission protocols depends on the specifics of the operating environment and requirements for connection speed and stability, and for this purpose, the use of machine learning methods is proposed. This study employed Random Forest, Neural Networks, and Logistic Regression. These three main models were chosen for their ability to identify different types of patterns: Random Forest - for detecting complex interactions between features, Neural Networks (with two hidden layers of 64 and 32 neurons) – for modeling complex nonlinear dependencies between protocol characteristics for modeling nonlinear dependencies [16], and Logistic Regression for ensuring interpretability of results. Together, they provide powerful and complementary tools for deep analysis of network data.

Protocol comparison and selection is implemented through a multi-stage algorithm where all machine learning models processed the same set of input data. The effectiveness of each model was evaluated using the F1-score metric, which takes into account both precision and recall:

$$F1 = 2 \times \frac{(precision \times recall)}{(precision + recall)} \quad (1)$$

This metric has particular value for evaluating classification quality under unbalanced class conditions, as it takes into account both false positive and false negative results. Specifically, in the context of our study, the F1-score allows for correct assessment of the models' ability to differentiate protocols based on their characteristics even under complex conditions of uneven class distribution in the training data.

To ensure research representativeness, the data collection process took place directly during system operation, which allowed obtaining relevant results under real operating conditions. For quantitative analysis, an evaluation of MQTT, CoAP, and HTTPS protocols was conducted based on three key indicators: transmission delay (latency), packet loss rate (packet loss), and throughput. Data collection was performed using specialized network

analysis tools, including Wireshark for deep packet inspection, tcpdump for monitoring network traffic at the TCP/IP level, JMeter for load testing, and iperf for throughput measurement. For each protocol, 20,000 data messages were transmitted, ensuring statistical significance of the results.

For this study, real data obtained from smart meters installed in a private enterprise were used. These meters provide information to specialized equipment for data collection and processing. The dataset consisted of structured records containing transmission delay, throughput, and packet loss indicators. These parameters were continuously monitored and recorded in real time, forming the basis for further analysis. The collected metrics were subsequently used as input for the machine learning models, enabling the system to make protocol selection decisions in real time depending on the observed communication environment.

The data processing methodology involved dividing the obtained energy load data array into training and test samples in an 80:20 ratio. To ensure reliable assessment of the stability of the created models, a 5-fold cross-validation methodology (Stratified K-Fold) was applied [17], in which each model was tested on five different subsets of training data [18]. Data preprocessing included normalization using StandardScaler to bring all indicators to a unified measurement scale, which eliminated the dominance of individual features with large absolute values and improved training accuracy.

The final protocol selection was based on a comprehensive approach that combined quantitative indicators (average F1-score value of all machine learning models) with qualitative verification of compliance with industry technical requirements for energy systems. Specifically, such critical parameters were considered as maximum allowable delay, acceptable packet loss level, and minimum required throughput to ensure uninterrupted system operation, particularly during emergency conditions such as power outages or external disruptions [19, 20, 21].

The obtained results of data transmission in energy systems using multi-protocol communication during different time periods presented in Table 1 demonstrate the system's ability to adapt to changing conditions.

Table 1

Results of data transmission in energy system using multi-protocol communication during different time periods with Logistic Regression, Random Forest, Neural Network methods

Model	Accuracy	Protocol	F1-score
27.01.2025, 10:00 am			
Logistic Regression	0.68	CoAP	0.70
Random Forest	0.62	CoAP	0.71
Neural Network	0.63	MQTT	0.67
02.02.2025, 10:00 am			
Logistic Regression	0.60	MQTT	0.67
Random Forest	0.58	MQTT	0.66
Neural Network	0.60	HTTPS	0.69

Analysis of Table 1 data indicates variability of results across different time periods. Based on the obtained results, we can observe that in most cases the Random Forest model recommended using the MQTT protocol, while the Neural Network in two cases preferred the HTTPS protocol, and Logistic Regression demonstrated a more conservative approach, evenly distributing recommendations between MQTT and CoAP depending on specific network conditions.

This divergence is explained by different model sensitivity to various aspects of network performance. Random Forest proved to be more sensitive to delay and packet loss indicators, the Neural Network better accounted for security aspects and connection stability, while Logistic Regression focused on linear dependencies between main performance metrics and demonstrated the highest interpretability of results. Consensus among the three models was achieved through a weighted algorithm that considered both individual F1-scores of each model and the degree of consistency of their recommendations.

The system automatically updates device configurations through the OIDC provider after determining the optimal protocol based on the generalized decision. Such implementation creates a protocol-agnostic layer that guarantees compliance with security standards while simultaneously ensuring flexible switching between protocols.

A key advantage of the proposed multi-model approach lies in its ability to significantly simplify the administration and management of heterogeneous devices within energy networks. In contrast to traditional methods, which require specific configurations for each device type and communication protocol, the unified OIDC-based system integrated with three complementary machine learning algorithms enables centralized management from a single control point, thereby reducing operational costs and enhancing overall system reliability.

4. CONCLUSIONS

The presented study demonstrates the effectiveness of a comprehensive approach to dynamic data transmission protocol selection in energy systems with multi-protocol communication, leveraging machine learning methods. The proposed methodology successfully addresses the challenges of adaptive protocol selection through the integration of three complementary models: Random Forest, Neural Networks, and Logistic Regression, each providing optimal recommendations for different network conditions and performance requirements.

Comparative analysis of the models revealed distinct sensitivities to network parameters: Random Forest exhibited the highest stability for delay and packet loss metrics, Neural Networks better accounted for security aspects and connection stability, and Logistic Regression offered the greatest interpretability of results. A consensus algorithm based on weighted F1-scores ensures reliable decision-making even when model recommendations diverge.

The methodology establishes a robust foundation for next-generation energy systems with intelligent protocol management capable of adapting to changing operating conditions and optimizing resource utilization. The use of multi-protocol communication simplifies the integration of heterogeneous devices, ensures system scalability, and reduces operational costs through centralized management.

The practical implementation of the proposed approach is expected to enhance the efficiency, stability, and security of modern Smart Grid systems, which is particularly important in the context of exponential growth in IoT devices and the increasing integration of distributed energy resources. It should be emphasized that, in scenarios where devices support only a limited set of communication protocols, the methodology can be adapted to perform protocol

selection within the available subset. This ensures that the decision-making process remains relevant under constrained conditions, while still leveraging the benefits of machine learning–based optimization.

Overall, the study confirms that combining multi-model machine learning with centralized authentication and protocol-agnostic management can significantly improve performance, reliability, and security of contemporary energy networks, providing a scalable and flexible solution for future Smart Grid implementations.

References

1. International Energy Agency. (2023). World Energy Outlook 2023. IEA Publications. Available at: https: //www.iea.org/reports/world-energy-outlook-2023. https://doi.org/10.1787/827374a6-en
2. IoT Analytics. (2024). State of IoT Summer 2024. Available at: https://iot-analytics.com/number-connected -iot-devices/.
3. Ahmad T., Chen H., Guo Y., & Wang J. (2018). A comprehensive overview on the data driven and large scale based approaches for forecasting of building energy demand. Energy and Buildings, 165, 301–320. https://doi.org/10.1016/j.enbuild.2018.01.017
4. Zhang Y., Wang J., & Wang X. (2020). Review on probabilistic forecasting of wind power generation with machine learning. Renewable and Sustainable Energy Reviews, 125, 109827. https://doi.org/10.1016/ j.rser.2020.109827.
5. Dileep G. (2020). A survey on smart grid technologies and applications. Renewable Energy, 146, 2589–2625. https://doi.org/10.1016/j.renene.2019.08.092
6. Kabalci Y. (2016). A survey on smart metering and smart grid communication. Renewable and Sustainable Energy Reviews, 57, 302–318. https://doi.org/10.1016/j.rser.2015.12.114
7. Chen X., McElroy M. B., Wu Q., Shu Y., & Xue Y. (2019). Transition towards higher penetration of renewables: an overview of interlinked technical, environmental and socio-economic challenges. Journal of Modern Power Systems and Clean Energy, 7(1), 1–18. https://doi.org/10.1007/s40565-018-0438-9
8. Starchenko V. (2021) Traffic optimization in wifi networks for the internet of things. Scientific Journal of the Ternopil National Technical University, 104 (4), 131–142. https://doi.org/10.33108/visnyk_tntu2021.04.131
9. Naik N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In 2017 IEEE International Systems Engineering Symposium (ISSE) (pp. 1–7). IEEE. https://doi.org/10.1109/SysEng.2017.8088251
10. Al-Masri, E., et al. (2020). Investigating messaging protocols for the Internet of Things (IoT). IEEE Access, 8, 94880-94911. https://doi.org/10.1109/ACCESS.2020.2993363
11. Thangavel D., Ma X., Valera A., Tan H.-X., & Tan C. K.-Y. (2014). Performance evaluation of MQTT and CoAP via a common middleware. In 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). IEEE. https://doi.org/10.1109/ISSNIP.2014.6827678
12. Rescorla E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Internet Engineering Task Force. https://doi.org/10.17487/RFC8446
13. Kumar S., & Patel D. R. (2019) A survey on Internet of Things: Security and privacy issues. International Journal of Computer Applications, 90 (11), 20–26. https://doi.org/10.5120/15764-4454
14. Hardt D. (2020). The OAuth 2.0 Authorization Framework. RFC 6749 (Updated). Internet Engineering Task Force. https://doi.org/10.17487/RFC6749.
15. Jones M., et al. (2019). OpenID Connect Core 1.0 incorporating errata set 1. OpenID Foundation. https://openid.net/specs/openid-connect-core-1_0.html.
16. Martsenyuk V., & Kit N. (2024) A multivariate method of forecasting the nonlinear dynamics of production network based on multilayer neural models. Scientific Journal of the Ternopil National Technical University, 114 (2), 39–50. https://doi.org/10.33108/visnyk_tntu2024.02.039
17. Combs G., et al. (2023). Wireshark User's Guide for Wireshark 4.0. Wireshark Foundation. https://www. wireshark.org/docs/wsug_html/.
18. Raschka S. (2018). Model Evaluation, Model Selection, and Algorithm Selection in Machine Learning (Version 3). arXiv. https://doi.org/10.48550/ARXIV.1811.12808.
19. International Electrotechnical Commission. (2018). IEC 61850-5-2018: Communication requirements for functions and device models. IEC Publications.
20. IEEE Standards Association. (2018). IEEE Standard 1613-2018: Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations. IEEE.
21. A. Voloshchuk, D. Velychko, H. Osukhivska, A. Palamar, (2024). Computer system for energy distribution in conditions of electricity shortage using artificial intelligence, in: Proceedings of the 2nd International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2024), Volume 3742, Ternopil, Ukraine, June 12–14, pp. 66–75. Available at: https://ceur-ws.org/Vol-3742/paper5.pdf.

УДК 004.7:004.8:621.3

АДАПТИВНА БАГАТОПРОТОКОЛЬНА КОМУНІКАЦІЯ ДЛЯ ЕНЕРГЕТИЧНИХ СИСТЕМ

Андрій Волощук; Галина Осухівська

Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

Резюме. *Розглянуто підходи до впровадження адаптивної багатопротокольної комунікації в енергетичних системах, що трансформуються в умовах зростання розподіленої генерації та розвитку концепції Smart Grid. Запропоновано архітектуру, яка поєднує OpenID Connect (уніфікований провайдер автентифікації) з модулем машинного навчання, з метою динамічного вибору оптимальних протоколів передавання даних між MQTT, CoAP, HTTPS протоколами та застарілими системами. Рішення базується на використанні найпоширеніших алгоритмів (Random Forest, нейронні мережі, логістична регресія) для прогнозування ефективності комунікації в режимі реального часу. Система забезпечує гнучке, безпечне та масштабоване управління різними пристроями через єдиний центр контролю. Отримані результати демонструють потенціал щодо зменшення витрат на комунікацію, забезпечують підвищення надійності та створюють основи для реалізації інтелектуальних комунікаційних систем в енергетичному секторі з автоматичним перемиканням протоколів.*

Ключові слова: *енергетичні мережі, енергоефективність, комунікаційні протоколи, методи машинного навчання, адаптивний вибір протоколу.*

https://doi.org/10.33108/visnyk_tntu2025.03.097 *Отримано 25.08.2025*