Security of Infocommunication Systems and Internet of Things

2026 Vol 4, No 1

https://doi.org/10.31861/sisiot2026.1.01002

Received 30 December 2025; revised 23 March 2026; accepted 02 June 2026; published 30 June 2026

Methods for Selecting Data Transmission Network Protocols in Energy Systems

Andrii Voloshchuk[1,*], Halyna Osukhivska[2], Maksym Drogobytskyi[2], Illia Fedorovych[1] and Ivan Borodii[1]

[1]Department of Computer Science, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
[2]Department of Computer Systems and Networks, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

*Corresponding author (E-mail: andriy.voloschuk30@gmail.com)

ABSTRACT This paper presents a comprehensive study aimed at enhancing data transmission stability and efficiency in modern energy systems, specifically Smart Grids. The research addresses the critical challenge of optimizing communication protocols within the context of evolving infrastructure and the increasing integration of Distributed Energy Resources. The primary focus of this work is the development of an intelligent communication control system featuring a decision-making mechanism that, based on the analysis of a set of input parameters including network latency, packet loss, and throughput, determines the feasibility of switching between data transmission protocols such as MQTT, CoAP, and HTTPS in real-time. The study employs an ensemble of machine learning classifiers to analyze real-time network telemetry to develop a mechanism for adaptive protocol switching. The proposed methodology integrates the analysis of network traffic dynamics with real-time performance metrics to facilitate dynamic protocol selection. An approach is proposed wherein an ensemble of machine learning models processes a vector of input metrics and classifies the current network state, initiating a protocol switch only when critical threshold values are reached. Experimental validation demonstrates that the adaptive protocol switching system provides improved network traffic scheduling efficiency compared to static implementations. The results indicate significant potential for reducing communication overhead while maintaining high standards of reliability and security in energy system operations. Specifically, the approach prevents data transmission over degraded channels by automatically switching to lightweight protocols like CoAP when connection parameters deteriorate, thereby ensuring compliance with timing requirements. The developed methodology establishes a foundation for the implementation of intelligent communication systems in Smart Grids, contributing to enhanced energy efficiency and grid stability. The findings hold practical value for energy utilities seeking to modernize their infrastructure and optimize data transmission within increasingly complex energy networks.

KEYWORDS communication protocols, data transmission, energy systems, methods, data analysis.

I. INTRODUCTION

The global paradigm shift from centralized power generation to decentralized Smart Grid architectures imposes unprecedented challenges on data transmission reliability and network scalability. As highlighted in the Annual Energy Outlook 2025 by the United States Energy Information Administration, the reliance on distributed generation technologies continues to increase, necessitating advanced grid management solutions [1].

A fundamental basis for developing such systems is the intelligent analysis of network traffic patterns correlated with power system behavior [2].

The global proliferation of connected devices is expected to grow substantially in the coming decade, with the number of Internet of Things (IoT) devices forecast to nearly triple from around 8.7 billion in 2020 to over 25 billion by 2030 [3]. The development of the IoT significantly influences various industrial sectors, including the energy sector [4-6]. Studies on the statistical characteristics of electricity consumption demonstrate pronounced cyclic and periodic loads, enabling the optimization of data transmission protocols aligned with predicted operational modes.

The selection of optimal network protocols becomes particularly relevant in the context of modern distributed Smart Grids and Supervisory Control and Data Acquisition (SCADA) systems, where ensuring stable operation is critical.

The application of modern Machine Learning algorithms enables the detection of complex non-linear dependencies in network traffic patterns caused by fluctuating energy demand. Research indicates that identifying network traffic signatures corresponding to different electricity consumption modes improves network traffic scheduling efficiency.

The evolution from traditional centralized fundamental rethinking of data transmission approaches. Integrating electricity consumption modeling results with modern network technologies creates a synergistic effect, facilitating an optimal balance between energy efficiency, reliability, and speed in data transmission systems [7]. Renewable energy sources are utilized to ensure the requisite power quality and reliable supply while simultaneously mitigating environmental pollution from energy operations [8].

Furthermore, recent studies indicate that precise adjustment of solar panel orientation and configuration can significantly enhance the performance of local energy systems, particularly by minimizing power outages during periods of high demand, as well as in extreme or force majeure situations [9].

II. ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

The contemporary advancement of energy systems necessitates the implementation of secure intelligent monitoring networks.

Reference [10] examines the development of secure smart systems for the hybrid energy sector utilizing IoT and artificial intelligence, thereby establishing a foundation for the subsequent optimization of data transmission. The proliferation of Smart City technologies further underscores the imperative to optimize energy grids. Study [11] demonstrates that the integration of Edge Computing with artificial intelligence significantly alleviates the load on central servers and reduces latency, a critical factor for real-time systems.

Communication adaptability constitutes a key determinant of the efficiency of such systems. Reference [12] proposes a framework for adaptive protocol selection that dynamically optimizes the energy efficiency of IoT communications through context-aware decision-making, which is directly relevant to the challenges associated with switching between MQTT and CoAP. A related approach is presented in, where an architecture combining an OpenID Connect authentication provider with an ensemble of machine learning algorithms (Random Forest, neural networks, logistic regression) is proposed for dynamic selection among MQTT, CoAP, HTTPS, and legacy protocols in distributed energy systems, demonstrating the potential for reducing communication overhead while ensuring scalable and secure device management.

To ensure solution scalability, hybrid architectures are increasingly being adopted. The authors of [13] substantiate the efficacy of a hybrid "Edge-Cloud" approach for managing renewable energy sources, employing deep learning for predictive analytics. This approach facilitates a balance between security and energy routing efficiency, as detailed in [14] within the context of innovations in electricity transmission and distribution.

A crucial aspect of implementing such systems is the control architecture. Comparative research [15] confirms the advantages of utilizing AI-enabled cloud SDN controllers, which provide the necessary scalability and security for modern distributed energy networks.

III. DATA ACQUISITION METHODOLOGY

An important goal of data transmission and processing in energy systems is to establish an optimal balance between processing speed and stability. Recent research indicates that AI-based computer systems can significantly enhance energy distribution efficiency, particularly under power deficit conditions, through adaptive control methods and the integration of diverse data transmission protocols [16]. By continuously analyzing network conditions, energy demand, and device performance, AI algorithms can dynamically optimize communication strategies, reduce transmission delays, and improve the reliability of data exchange across smart grid infrastructures.

This necessitates the development and implementation of integrated solutions capable of effectively interacting with heterogeneous data transmission protocols and ensuring system scalability. Simultaneously, these technologies introduce a series of challenges regarding the efficient processing and transmission of substantial data volumes from edge devices to servers responsible for analysis and decision-making

A fundamental driver for the development of such systems is the optimization of data acquisition and processing from numerous devices integrated into the energy grid. Given the resource constraints of edge devices and the requirements for real-time responsiveness, it becomes important to develop mechanisms capable of functioning effectively with various protocols, such as MQTT, CoAP, and HTTPS. Each of these protocols possesses specific characteristics and distinct limitations.

The general system architecture (Fig. 1) illustrates the complete protocol lifecycle, ranging from data acquisition by devices via MQTT, CoAP, and HTTPS to load balancing through ALB/NLB and storage in the Data Collector & Storage module. The CI/CD system executes ML models for data analysis, the Protocol Decision module determines the optimal protocol, and AWS IoT Core automatically updates device configurations.

Considering the specific characteristics of each protocol, a need arises for an intelligent selection system adaptable to current conditions; let us examine the primary data transmission technologies employed in energy systems [17]. Its advantages include a compact 2-byte packet header, minimal latency, and stable operation in unreliable networks.

However, the basic version of MQTT lacks built-in encryption mechanisms, and limited support for the "request-response" pattern complicates its use in complex interaction scenarios. CoAP was designed for constrained networks and utilizes efficient binary encoding with caching support. Although it follows the REST architecture, it operates over UDP, significantly reducing overhead. However, UDP transport does not guarantee message delivery, and scaling to large networks remains problematic. Difficulties with NAT traversal and firewalls further restrict the scope of CoAP application.

HTTPS is distinguished by a high level of security due to TLS/SSL encryption, preventing data interception or modification during transmission [18]. The trade-off for security is increased energy consumption due to cryptographic computations, significant hardware resource requirements, larger packet headers, and a lengthy connection establishment process. These characteristics render HTTPS a suboptimal choice for energy-efficient devices and unstable network environments.

The utilization of load balancers for these protocols ensures load distribution when routing traffic from various devices, significantly reducing the probability of system overload and guaranteeing stability even under conditions of simultaneous high-volume data influx [19]. This approach not only improves system efficiency but also simplifies scaling as the number of connected devices increases. A crucial aspect of energy systems is their capability for continuous and automatic data processing and optimal decision-making based on analysis results [20]. Implementing CI/CD systems allows for the automation of this process, specifically the execution of

Python scripts for data analysis, protocol testing, and, if necessary, system configuration updates based on test results. This facilitates the optimization of the decision-making process.

Thus, the need to implement such a system (Fig. 1) is driven by the requirement for effective management of a large number of data acquisition devices in energy grids when transmitting data via various communication protocols. Implementing an appropriate system allows for data transmission optimization, ensuring scalability and the overall operational efficiency of all components.

Data from devices are transmitted using various protocols (MQTT, CoAP, HTTPS) to load balancers (ALB and NLB), which ensure efficient traffic distribution. Subsequently, this data reaches the server, where it is aggregated and processed for further analysis [21]. The collected data is transferred to the CI/CD system, which automatically triggers scripts for analysis and protocol testing. Based on the analysis results, the system decides on device configuration changes via AWS IoT Core, or this is performed by a duty engineer monitoring network connection status in real-time, allowing for protocol selection optimization for each device according to specific requirements and the connection status of remote devices.

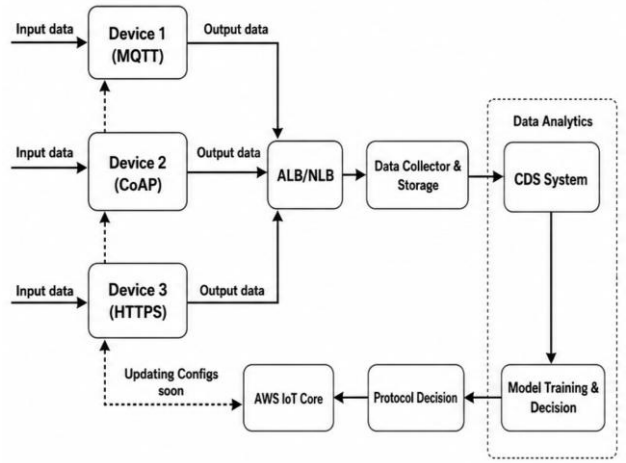

FIG. 1. Diagram of the data acquisition and analysis process within the energy infrastructure.

To guarantee the resilience of the proposed architecture, a comprehensive 'Defense in Depth' strategy is implemented, spanning five hierarchical protection tiers. The foundational layer secures physical assets through Hardware Security Modules (HSM) and Secure Boot capabilities. Access control and network integrity are enforced via AWS IoT Core authentication using X.509 certificates, complemented by AWS WAF/Shield and load balancers at the perimeter. Crucially, data transmission is protected through encrypted channels managed by the ML-adaptive protocol selector, while the final layer ensures continuous oversight via centralized monitoring systems such as CloudWatch and SIEM for real-time incident response.

Ensuring a comprehensive approach to cybersecurity in energy systems is of paramount importance, where the traditional pillars Confidentiality, Integrity, and Availability assume a specific significance. In energy grids, Availability often takes precedence over Confidentiality, as even a momentary loss of connectivity with critical devices can precipitate cascading failures within the power system.

The integration of ML algorithms not only optimizes network performance but also serves as a supplementary defense mechanism capable of detecting anomalous traffic patterns and automatically initiating countermeasures. This is particularly pertinent to Smart Grid infrastructure, where the timely detection and neutralization of cyber threats are for ensuring national energy security. The diagram (Fig. 2) illustrates the real-time dynamic protocol selection process.

Input data (device metrics, network conditions) are processed via an ensemble of four ML models, each specializing in distinct classification aspects. Logistic Regression provides baseline linear classification, Gradient Boosting demonstrates the highest accuracy, Random Forest minimizes overfitting, and the Neural Network detects complex non-linear dependencies.

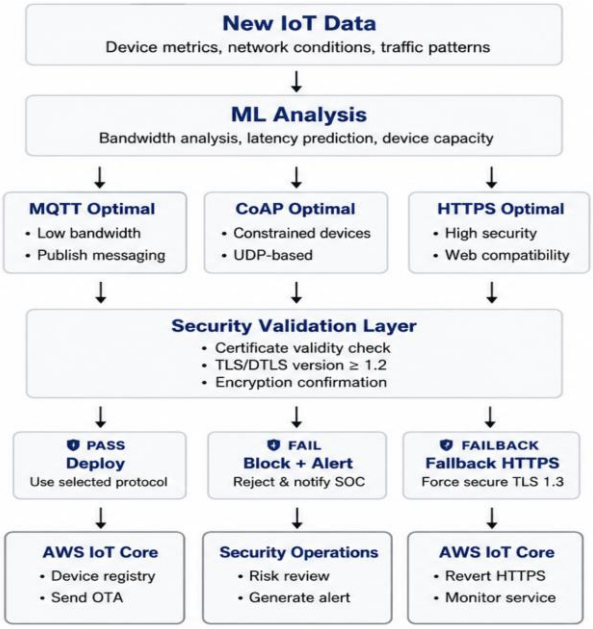

FIG. 2. Diagram of the ML-based protocol selector with multi-level security validation.

The security validation system verifies certificates, TLS/DTLS versions, and encryption standards prior to making the final decision. Upon successful validation, the selected protocol is utilized (Deploy); in case of rejection, a blocking mechanism with an alert is activated (Fail) or a secure HTTPS mode is triggered (Fallback), ensuring operational continuity in compliance with requirements.

The described data acquisition methodology establishes a foundation for the practical implementation of ML algorithms. The subsequent section will examine the research methods and experimental validation of the proposed approach.

IV. ANALYSIS OF RESEARCH RESULTS

Efficient and rapid data exchange between energy network nodes necessitates the implementation of modern communication protocols that ensure reliability, latency minimization, and energy efficiency. In the context of distributed energy management systems, the substantiated

selection of an optimal data transmission protocol depends on the specifics of the operational environment and specific requirements for connection speed and stability. Recent studies demonstrate that artificial intelligence plays a key role in modern energy systems by enabling adaptive optimization, intelligent decision-making, and efficient handling of complex, heterogeneous data streams [22].

Artificial intelligence technologies are the most effective for data analysis [23]. To evaluate and classify protocols according to their characteristics, four primary machine learning algorithms were utilized. Logistic Regression was selected as a baseline linear classifier, enabling the derivation of a simple and interpretable model for the primary analysis of correlations between protocol parameters. Its advantage lies in the ability to estimate the probability of belonging to a specific class through a linear combination of input parameters.

Gradient Boosting proved particularly effective for structured datasets, demonstrating high classification accuracy and strong generalization capability. Random Forest, as an ensemble learning method, significantly reduces the risk of overfitting and enhances robustness to variations in the input data. A Multilayer Perceptron (MLP) with two fully connected hidden layers comprising 64 and 32 neurons, respectively, was employed to capture non-linear dependencies in network telemetry data, consistent with recent applications of deep learning in Smart Grid systems [24]. The MLP was implemented using the MLPClassifier class from the sklearn.neural_network module with the following hyperparameters: ReLU activation function, Adam optimizer, an initial learning rate of 0.001, an L2 regularization coefficient (alpha) of 0.0001, and a maximum of 500 training epochs. The selection of this compact architecture over deeper neural network models (e.g., CNNs, Transformers, and residual networks) is justified by the low dimensionality of the input feature space, which consists of only three network metrics (latency, packet loss, and throughput). Under these conditions, more complex architectures do not provide a statistically significant improvement in classification performance while increasing computational complexity, training time, and the risk of overfitting [24]. Its ability to detect latent correlations between protocol characteristics makes this model a powerful tool for deep analysis of network data.

The process of comparing and selecting the optimal data transmission protocol is implemented in the Data Analysis block of this system using a multi-stage comparator algorithm. In the first stage, all machine learning models process an identical input dataset. Their results are stored in appropriate data structures (specifically tables and variables), ensuring consistency and comparability of the obtained metrics. Subsequently, the efficiency of each model is evaluated, and scores are assigned for the objective determination of the most suitable protocol. Each of the four machine learning models independently determines the most effective protocol.

The software implementation of the processing, analysis, and model testing logic was executed in Python using the scikit-learn library. Traditional security approaches often focus on Confidentiality, leading to the use of "heavyweight" protocols such as HTTPS. However, in cyber-physical energy systems, Availability often becomes the priority. A control command transmission delay exceeding 100 ms can lead to emergency situations, which is equivalent to a successful DoS attack on the system [25]. The corresponding logic is implemented in the identify_optimal_protocol function (Fig. 3), which performs an analysis of the classification results.

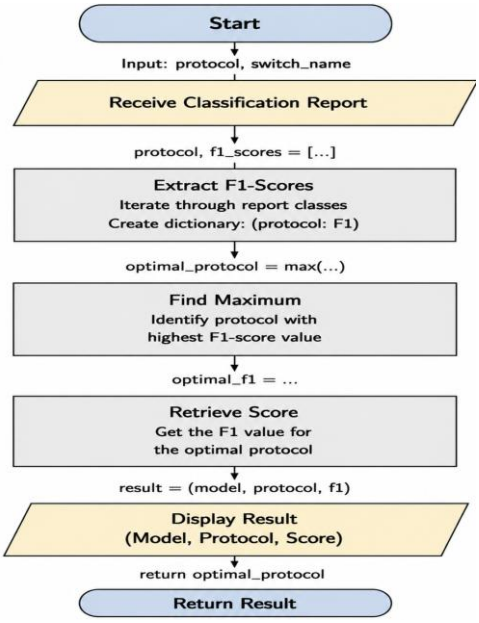

FIG. 3. Implementation of the algorithm for determining the optimal protocol based on F1-score.

The developed model addresses the security challenge of availability. When the system detects network degradation (e.g., due to a link-layer DDoS attack or congestion), it automatically switches the channel from TCP-oriented HTTPS (which is vulnerable to TCP retransmission storms) to UDP-oriented CoAP/DTLS. This facilitates the reduction of the attack surface by lowering handshake overhead in DTLS, enabling the system to remain controllable even under low bandwidth conditions. Furthermore, this mechanism prevents cascading failures, as rapid protocol switching offloads network gateways, thereby preserving the functionality of the network segment.

Thus, the protocol change is viewed not as a reduction in security level, but as an adaptive mechanism for countering service degradation, complying with NIST SP 800-82 recommendations regarding Industrial Control Systems (ICS) security.

During the execution of the function, a dictionary named protocol_f1_scores is generated, recording the F1 metric value for each protocol as derived by a specific model. Using the standard max function, the protocol with the maximum F1 score is identified and considered optimal for the respective model.

For the quantitative evaluation of protocol classification performance, the F1 score was utilized, which incorporates both the precision and recall of predictions. The F1 score is calculated as the harmonic mean of these two metrics according to Formula (1):

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

This metric is valuable given that classes may be imbalanced, necessitating the consideration of not only the number of correct predictions but also the rate of missed detection. Within the context of this study, the F1-score enables an accurate assessment of the model's ability to differentiate between various protocols while accounting for their specific characteristics.

At the concluding stage, the system executes the final decision regarding the selection of the optimal protocol. The definitive selection of the model for deployment is based on a comparative analysis of F1-scores derived from the experimental results. The model demonstrating the highest stability and precision across all simulated scenarios is integrated into the decision module. Consequently, the system ensures a rigorous approach to selection, relying on absolute classification performance metrics.

Within the scope of this research, a comprehensive performance analysis of various network protocols, specifically MQTT, CoAP, and HTTPS, was conducted in the context of their application in systems. To ensure study representativeness, network traffic patterns were simulated to replicate characteristics typically observed via analyzers such as Wireshark and tcpdump. This approach allowed for the generation of controlled stress-test scenarios (storms, heavy loads) that are difficult to reproduce consistently in a physical testbed.

The experimental evaluation methodology was designed in accordance with established practices in smart meter data analytics and energy consumption analysis [26].

To ensure study representativeness, data acquisition was conducted during simulated system operation under realistic conditions, yielding relevant and reproducible results [27]. Each protocol was evaluated based on latency, packet loss, and throughput, fostering a comprehensive understanding of their performance under real-world operating conditions and large-scale data processing requirements. For each protocol, a total of 10,000 data messages were transmitted.

The acquired data were partitioned into training and testing sets at an 80:20 ratio, resulting in 24,000 messages for the training set and 6,000 messages for the test set. To ensure evaluation objectivity, protocol classes within the samples were balanced to prevent bias in model training results.

To assess the stability of the developed models, a 5-fold Stratified K-Fold cross-validation methodology was applied, wherein each model was tested on five distinct subsets of the training data. Subsequently, the models were evaluated on an independent test set (6,000 messages). Consequently, six tests were conducted for each model (five cross-validation stages and one final test). Prior to training, data normalization was performed using StandardScaler to ensure a unified measurement scale for metrics.

For each investigated metric, the mean value and standard deviation were calculated based on the simulation of diverse operational scenarios (stable grid, storm, heavy load). For instance, the latency result of 0.11 ± 0.16 s for MQTT indicates its high speed but susceptibility to jitter under load.

TABLE 1. Consolidated results of protocol performance analysis.

Metric	MQTT	CoAP	HTTPS
Latency, s	0.11 ± 0.16	0.07 ± 0.06	0.31 ± 0.35
Packet Loss, %	2.53 ± 2.38	2.53 ± 2.38	2.53 ± 2.38
Throughput, Mbps	1.01 ± 1.29	1.33 ± 1.46	0.59 ± 0.95

The definitive selection of the optimal protocol framework is predicated on a synthesis of quantitative metrics derived from the machine learning models. The primary criterion for model selection is the F1-score, as it balances precision and recall in unevenly distributed scenarios (e.g., rare network storms). Initially, the candidate protocol is predicted by the best-performing model (Gradient Boosting). Subsequently, it undergoes validation against industry standards. Should the candidate fail to meet these constraints, the system triggers a fallback mechanism. This ensures the objectivity, reproducibility, and adaptability of the solution within environments.

Initially, the candidate protocol is identified based on superior machine learning metrics. Subsequently, it undergoes validation against industry standards. Should the candidate fail to meet these constraints (e.g., HTTPS rejected due to excessive latency), the system automatically reverts to the next-highest-ranked alternative. This mechanism ensures the objectivity, reproducibility, and adaptability of the solution within Smart Grid environments. The data presented in the subsequent tables illustrate the results of the protocol performance analysis across distinct temporal intervals.

This analysis accounts for variations in operational states induced by factors such as increased latency, network unavailability for a specific protocol, or fluctuations in other parameters influencing data transmission. It is observed that the system selects distinct protocols in accordance with the acquired data and analysis results, thereby demonstrating dynamic adaptability and the absence of bias toward a single protocol.

The testing results of the machine learning models across various time periods (April 3, 2025, April 10, 2025, April 17, 2025) are summarized in Table 2.

While the aggregate accuracy metrics presented in Table 2 demonstrate the general effectiveness of the models, they do not reveal the specific nature of classification errors. To provide a deeper insight into the decision-making process and verify the robustness of the proposed algorithms against conflicting input parameters (such as high security requirements versus critical network latency), Confusion Matrices were generated. The visualization of these matrices is presented in Fig. 4.

To verify the robustness of the proposed models, Confusion Matrices were generated (Fig. 4). These matrices reveal significant differences in how algorithms handle non-linear decision boundaries introduced by conflicting parameters, particularly the trade-off between high security requirements and critical network latency constraints. Gradient Boosting and Neural Network demonstrated the highest stability (Accuracy ~83% – 84%), effectively distinguishing between MQTT and HTTPS despite their similar TCP-based characteristics

under stable conditions. Conversely, Logistic Regression showed a slightly higher misclassification rate, indicated by a lower diagonal density, which confirms that optimal protocol selection is a non-linear problem requiring complex decision trees or neural connections to resolve effectively. Additionally, CoAP was correctly identified in the majority of 'Network Storm' scenarios, validating the system's ability to switch to a lightweight protocol during critical packet loss events to maintain connectivity.

While the confusion matrices visually demonstrate the classification behavior and error distribution, a precise quantitative comparison is required to select the optimal model for deployment. The aggregate performance metrics across all simulated scenarios including accuracy, precision, recall, and F1-score are summarized in Table 3. These indicators provide a definitive assessment of each algorithm's reliability in handling the stochastic nature of network traffic.

Based on the highest F1-score and Precision, the Neural Network and Gradient Boosting models are identified as the most suitable candidates for integration into the intelligent protocol selection module.

The obtained results are consistent with recent studies investigating the application of machine learning methods in Smart Grid communication systems. Similar to previous research, ensemble learning algorithms demonstrated high robustness and reliable classification performance when applied to structured network telemetry data. The proposed approach achieved competitive performance while maintaining relatively low computational complexity,

TABLE 2. Results of machine learning model testing at different time periods.

Model	Accuracy	Protocol	F1-Score
03.04.2025, 10:00 am			
Logistic Regression	0.8067	CoAP	0.7885
Gradient Boosting	0.8010	CoAP	0.7861
Random Forest	0.7901	MQTT	0.7752
Neural Network	0.8033	CoAP	0.7854
10.04.2025, 10:00 am			
Logistic Regression	0.8333	MQTT	0.8073
Gradient Boosting	0.835	MQTT	0.69
Random Forest	0.8167	MQTT	0.7898
Neural Network	0.8417	MQTT	0.8156
17.04.2025, 10:00 am			
Logistic Regression	0.7953	HTTPS	0.7947
Gradient Boosting	0.8353	HTTPS	0.8332
Random Forest	0.8286	HTTPS	0.8267
Neural Network	0.8403	HTTPS	0.8381

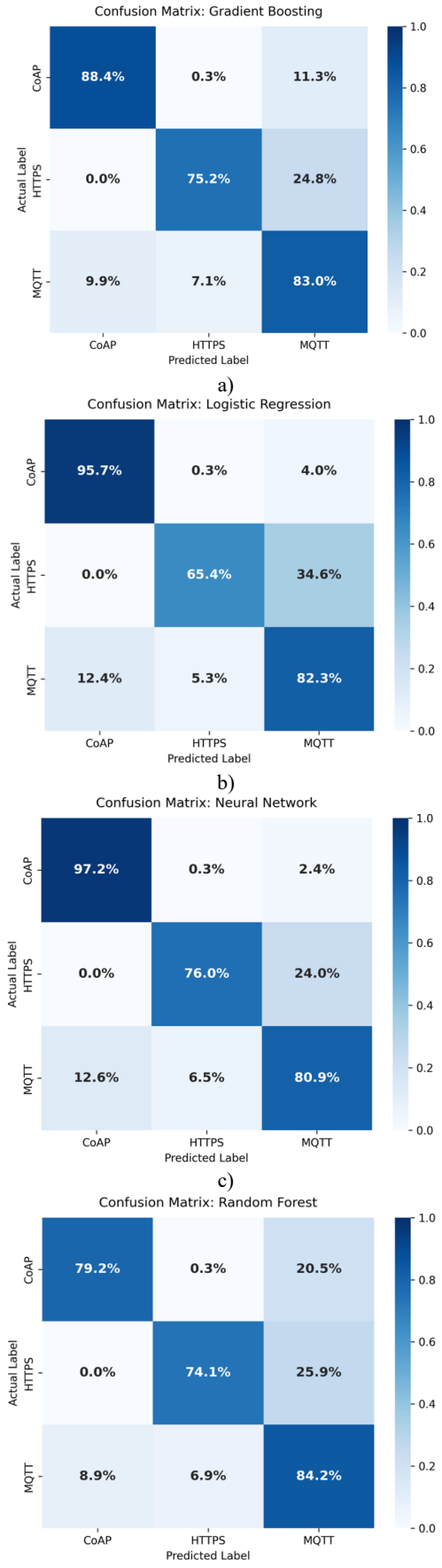

FIG. 4. Confusion Matrices evaluating the classification performance: (a) Logistic Regression; (b) Gradient Boosting; (c) Random Forest; (d) Neural Network.

TABLE 3. Final aggregated metrics.

Model	Accuracy	F1-Score	Recall
Logistic Regression	0.8118	0.8106	0.8118
Gradient Boosting	0.8234	0.8241	0.8234
Random Forest	0.8118	0.8120	0.8118
Neural Network	0.8284	0.8295	0.8284

making it suitable for real-time protocol selection in resource-constrained energy infrastructures. These findings indicate that lightweight machine learning models remain an effective solution for adaptive communication management in Smart Grid environments. Across various temporal intervals, each experimental run was predicated on distinct input datasets, resulting in variability in the values of key metrics. As observed, the system exhibits a dynamic response to any fluctuations, with results shifting accordingly. The testing results of the machine learning models demonstrate accuracy variability contingent upon input data characteristics. During each iteration, the models yielded different performance indicators, enabling conclusions to be drawn regarding their generalizability and adaptability.

Upon the conclusion of testing and the determination of the most effective data transmission protocol, the system automatically updates the device configuration and AWS infrastructure, ensuring optimal connection performance and stability. Immediately following the selection of a new protocol (e.g., MQTT), devices receive updated settings via the AWS IoT Core service. The utilization of AWS IoT Jobs or AWS IoT Device Management facilitates centralized configuration modification and connection parameter management. A new configuration file modifying connection parameters is dispatched to the device, and, if necessary, a firmware update is initiated using the Over-the-Air (OTA) mechanism. Concurrently, AWS IoT Policies are updated to ensure correct device access to resources via the selected protocol.

To ensure seamless network operation, corresponding adjustments are also implemented at the load balancer level. When utilizing an Application Load Balancer (ALB), routing rules are updated to direct traffic via MQTT. In the case of a Network Load Balancer (NLB), target group adjustments are performed to minimize latency. If traffic routing is managed via DNS, appropriate modifications are applied to Amazon Route 53 rules, ensuring request routing via the optimal path.

The update automation process is fully integrated into the CI/CD pipeline. Following the identification of the optimal protocol, a device update is initiated using the AWS CLI or SDK. An AWS IoT Job is launched to modify connection configurations, with parallel verification of the correctness of implemented changes.

This approach secures system flexibility and adaptability, guaranteeing stable data transmission even under variable operational parameters. The integration of AWS IoT Core with load balancers and CI/CD technologies allows not only for the determination of optimal communication protocols but also for the rapid implementation of corresponding changes across the entire infrastructure scale.

V. CONCLUSION

In this study, a method for dynamic protocol selection has been proposed, predicated on the continuous monitoring and analysis of a complex set of input parameters, including latency, packet loss, and throughput. The scientific novelty lies in the utilization of machine learning models to detect complex non-linear dependencies among these network parameters and to autonomously decide on the necessity of switching the current protocol to maintain connection resilience.

A decision-making algorithm has been implemented operating on a feedback principle, where the system not only detects connection degradation but performs an active countermeasure by switching protocols. This allows latency parameters to be optimized and maintained within acceptable operational limits even under unstable network conditions caused by grid load fluctuations or conflicting constraints such as high security requirements versus critical battery levels.It has been experimentally confirmed that analyzing input parameters using non-linear methods, particularly Gradient Boosting and Neural Networks, ensures high classification stability (F1-score = 0.82%) in determining the optimal moment for switching.

This approach significantly minimizes the issue of false positives compared to linear classifiers, which struggle to resolve conflict scenarios. Furthermore, a "Defense in Depth" security architecture is proposed, integrating the protocol switching mechanism as an active defense against DDoS attacks. By minimizing handshake overhead using UDP-based protocols such as DTLS during critical loads, the system effectively reduces the attack surface. Future research will focus on implementing Federated Learning to enable model training directly on edge gateways without transmitting sensitive data to the cloud, as well as optimizing the energy efficiency of cryptographic algorithms for autonomous sensors.

AUTHOR CONTRIBUTIONS

A.V. – conceptualization, software, validation, formal analysis, resources, data curation, writing – original draft preparation, visualization; H.O. – methodology, investigation, writing – review and editing, supervision; M.D. – methodology, software, investigation, validation, writing – review and editing; I.F. – software, formal analysis, validation, writing – review and editing; I.B. – investigation, data curation, validation, visualization, writing – review and editing.

COMPETING INTERESTS

The authors declare no competing interests.

REFERENCES

[1] U.S. Energy Information Administration, "Annual Energy Outlook 2025," Washington, DC, USA, 2025. [Online]. Available: https://www.eia.gov/outlooks/aeo/

[2] V. Gotovych, O. Nazarevych, and L. Shcherbak, "Mathematical modeling of the regular-mode electric power supply and electric power consumption processes of the organization," *Scientific Journal of the Ternopil National Technical University*, vol. 91, no. 3, pp. 134–142, 2018, doi: 10.33108/visnyk_tntu2018.03.134.

[3] G. Paolone, D. Iachetti, R. Paesani, F. Pilotti, M. Marinelli, and P. Di Felice, "A Holistic Overview of the Internet of Things Ecosystem," *IoT*, vol. 3, no. 4, pp. 398–434, Oct. 2022, doi: 10.3390/iot3040022.

[4] N. M. Kiasari, M. Ghaffari, and H. H. Aly, "A comprehensive review of the current status of smart grid technologies for renewable energies integration and future trends: The role of machine learning and energy storage systems," *Energies*, vol. 17, no. 16, p. 4128, 2024, doi: 10.3390/en17164128.

[5] Q. N. Minh, V.-H. Nguyen, V. K. Quy, L. A. Ngoc, A. Chehri, and G. Jeon, "Edge computing for IoT-enabled smart grid: The future of energy," *Energies*, vol. 15, no. 17, p. 6140, 2022, doi: 10.3390/en15176140.

[6] T. Salman and R. Jain, "A survey of protocols and standards for Internet of Things," *arXiv preprint arXiv:1903.11549*, 2019, doi: 10.48550/arXiv.1903.11549.

[7] L. Tightiz and H. Yang, "A comprehensive review on IoT protocols' features in smart grid communication," *Energies*, vol. 13, no. 11, p. 2762, 2020, doi: 10.3390/en13112762.

[8] M. Bilal, A. A. Algethami, Imdadullah, and S. Hameed, "Review of computational intelligence approaches for microgrid energy management," *IEEE Access*, vol. 12, pp. 123294–123321, 2024, doi: 10.1109/ACCESS.2024.3440885.

[9] L. H. Hussienat *et al.*, "Analysis of the parameters of local power system devices with solar power plants and energy storage facilities and determination of operating modes during various periods of power outages," *Advances in Science and Technology Research Journal*, vol. 19, no. 4, pp. 229–240, 2025, doi: 10.12913/22998624/200329.

[10] Shruti, S. Rani, M. Shabaz, A. K. Dutta, and E. A. Ahmed, "Enhancing privacy and security in IoT-based smart grid system using encryption-based fog computing," *Alexandria Engineering Journal*, vol. 102, pp. 66–74, 2024, doi: 10.1016/j.aej.2024.05.085.

[11] Y. Herman, H. Lastivka, and A. Samila, "Embedded operating systems in IoT edge computing," *Security of Infocommunication Systems and Internet of Things*, vol. 2, no. 2, p. 02001, 2024, doi: 10.31861/sisiot2024.2.02001.

[12] A. Voloshchuk and H. Osukhivska, "Adaptive multi-protocol communication for energy systems," *Visnyk TNTU*, vol. 119, no. 3, pp. 97–106, 2025, doi: 10.33108/visnyk_tntu2025.03.097.

[13] V. Rekha *et al.*, "Hybrid edge-cloud approach for renewable energy management using deep learning with predictive analytics," in *Proc. 2024 Int. Conf. on Recent Advances in Science and Engineering Technology (ICRASET)*, Bengaluru, India, 2024, pp. 1–7, doi: 10.1109/icraset63057.2024.10895726.

[14] M. A. Mahmoud *et al.*, "A review on smart energy grid technology: features and specifications," *Journal of Engineering and Applied Sciences*, vol. 15, no. 2, pp. 535–547, 2020, doi: 10.36478/jeasci.2020.535.547.

[15] N. O. Aljehane, "Software-defined networking for smart grid: A review," *IEEE Access*, vol. 11, pp. 23541–23560, 2023, doi: 10.1109/ACCESS.2023.3253874.

[16] A. Voloshchuk, D. Velychko, H. Osukhivska, and A. Palamar, "Computer system for energy distribution in conditions of electricity shortage using artificial intelligence," in *Proc. 2nd Int. Workshop Comput. Inf. Technol. Ind. 4.0 (CITI 2024)*, Ternopil, Ukraine, 2024, vol. 3742, pp. 66–75.

[17] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/comst.2015.2444095.

[18] M. A. Al-Garadi *et al.*, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.

[19] M. K. Ahmed, S. A. Salman, and O. Y. Abdulhammed, "Load balancing techniques in cloud computing: A review," *Samarra Journal of Pure and Applied Science*, vol. 6, no. 1, pp. 223–250, 2024, doi: 10.54153/sjpas.2024.v6i1.526.

[20] S. Lavirotte, G. Rocher, J.-Y. Tigli, and T. Gonnin, "IoT-based systems actuation conflicts management towards DevOps: A systematic mapping study," in *Proc. 5th Int. Conf. on Internet of Things, Big Data and Security (IoTBDS)*, Prague, Czech Republic, 2020, pp. 227–234, doi: 10.5220/0009355102270234.

[21] M. Niraula, P. R. Ojha, S. Simkhada, and Y. Layalu, "Review on the application of machine learning algorithms on smart grid optimization," *Kathford J. Eng. Manag.*, vol. 3, no. 1, pp. 62–71, 2023, doi: 10.3126/kjem.v3i1.62877.

[22] T. Ahmad *et al.*, "Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities," *J. Clean. Prod.*, vol. 289, p. 125834, 2021, doi: 10.1016/j.jclepro.2021.125834.

[23] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3125–3148, 2019, doi: 10.1109/tsg.2018.2818167.

[24] D. Zhang, X. Han, and C. Deng, "Review on the research and practice of deep learning and reinforcement learning in smart grids," *CSEE J. Power Energy Syst.*, vol. 4, no. 3, pp. 362–370, 2018, doi: 10.17775/cseejpes.2018.00520.

[25] S. Williams and M. Short, "Electricity demand forecasting for decentralised energy management," *Energy Built Environ.*, vol. 1, no. 2, pp. 178–186, 2020, doi: 10.1016/j.enbenv.2020.01.001.

[26] A. V. Voloshchuk, H. M. Osukhivska, Yu. B. Palianytsia, A. M. Lutskiv, and V. B. Valiashek, "Determination of balance in electric power systems using machine learning methods based on informative features obtained by the component method," *Bulletin of NUWEE. Technical Sciences*, vol. 4, no. 112, pp. 148–161, Dec. 2025, doi: 10.31713/vt4202514.

[27] Y. Zhang, T. Huang, and E. F. Bompard, "Big data analytics in smart grids: A review," *Energy Inform.*, vol. 1, no. 1, 2018, doi: 10.1186/s42162-018-0007-5.

Andrii Voloshchuk

In 2021, he received a Master's degree in Computer Systems and Networks from Ternopil Ivan Puluj National Technical University. PhD student at the Department of Computer Science at Ternopil Ivan Puluj National Technical University. His research interests include cloud computing, computer networks, programming, and artificial intelligence.

ORCID: 0009-0007-1478-1601

Halyna Osukhivska

PhD, Associate Professor, Head of the Department of Computer Systems and Networks, Ternopil Ivan Puluj National Technical University. 56 Ruska Str., Building 1, Room 604, Ternopil, Ukraine, 46001.
Research interest stochastic analysis, machine learning, mathematical modeling.

ORCID: 0000-0003-0132-1378

Illia Fedorovych

PhD student at the Department of Computer Science at Ternopil Ivan Puluj National Technical University, working on GPU computing. Master of Software Engineering from Igor Sikorsky Kyiv Polytechnic Institute with 10 years of practical experience in the field.

ORCID: 0009-0003-7739-9689

Maksym Drogobytskyi

PhD student at the Department of Computer Systems and Networks, Ternopil Ivan Puluj National Technical University. Practicing Software Engineer. His research interests include MicroGrid integration, dynamic load balancing of electrical networks, embedded computer systems, edge computing, IoT, and computer networks.

ORCID: 0009-0009-6865-6034

Ivan Borodii

PhD student at the Department of Computer Science at Ternopil Ivan Puluj National Technical University. Practicing Software Engineer with over 8 years of experience. Master of Computer Engineering.

ORCID: 0009-0005-4986-4429

Методи вибору мережевих протоколів передачі даних в енергетичних системах

Андрій Волощук[1,*], Галина Осухівська[2], Максим Дрогобицький[2], Ілля Федорович[1], Іван Бородій[1]

[1]Кафедра комп'ютерних наук, Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна
[2]Кафедра комп'ютерних систем та мереж, Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

*Автор-кореспондент (Електронна адреса: andriy.voloschuk30@gmail.com)

АНОТАЦІЯ У статті представлено результати комплексного дослідження, спрямованого на підвищення стабільності та операційної ефективності процесів передачі даних у сучасних енергетичних системах, зокрема в інтелектуальних мережах (Smart Grids). Робота присвячена вирішенню актуальної науково-технічної проблеми оптимізації комунікаційних протоколів в умовах динамічного розвитку інфраструктури та зростаючої інтеграції розподілених енергетичних ресурсів. Основну увагу в роботі зосереджено на розробці інтелектуальної системи керування комунікаціями, яка включає адаптивний механізм прийняття рішень. Цей механізм, базуючись на безперервному аналізі набору вхідних параметрів (таких як затримка в мережі, втрата пакетів та пропускна здатність), визначає доцільність перемикання між різнорідними протоколами передачі даних (зокрема MQTT, CoAP та HTTPS) у режимі реального часу. У дослідженні використовується ансамбль класифікаторів машинного навчання для аналізу мережевої телеметрії в реальному часі з метою розробки механізму адаптивного перемикання протоколів. Запропонована методологія поєднує аналіз динаміки мережевого трафіку з метриками продуктивності в реальному часі, що дозволяє реалізувати динамічний вибір протоколу. Авторами запропоновано підхід, у якому ансамбль моделей машинного навчання обробляє вектор вхідних метрик та класифікує поточний стан мережі, ініціюючи зміну протоколу лише у випадках досягнення критичних порогових значень. Експериментальна валідація демонструє, що система адаптивного перемикання протоколів забезпечує підвищення ефективності планування мережевого трафіку порівняно зі статичними реалізаціями. Отримані результати свідчать про значний потенціал запропонованого підходу щодо зменшення комунікаційних накладних витрат при одночасному збереженні високих стандартів надійності та безпеки. Зокрема, підхід дозволяє запобігти передачі даних через деградовані канали шляхом автоматичного перемикання на легковагові протоколи у разі погіршення параметрів з'єднання. Розроблена методологія створює фундамент для впровадження інтелектуальних комунікаційних систем, сприяючи підвищенню енергоефективності та стабільності мережі.

КЛЮЧОВІ СЛОВА комунікаційні протоколи, передача даних, енергетичні системи, методи, аналіз даних.