5G Energy Internet Network Security Load Forecasting System Based on Quantum Reinforcement Learning and Dynamic Topology Perception

Wangdong Wu, Yongdong Dai, Shenyu Wang, Maofei Wang, Weijian Xiao, Yi Zhou
State Grid Jiangsu Electric Power Co., Ltd, Taizhou Power Supply Branch, Taizhou 225300, Jiangsu, China
Corresponding author: Wangdong Wu (e-mail: wuwangdong2022@163.com)

ABSTRACT In 5G energy internet environments, load forecasting is challenged by frequent topology reconstruction and diversified security threats, which affect real-time power stability and operational reliability. To overcome the limitations of traditional methods, this paper proposes a collaborative optimization model integrating Quantum Proximal Policy Optimization and dynamic topology perception. The closed-loop system integrates power-load, communication, and security information into a unified state tensor. For dynamic topology modeling, a GraphSAGE-TGAT graph neural network with event-driven updates enables millisecond-level reconstruction and adapts to highly dynamic 5G network structures. At the policy optimization level, a quantum-classical hybrid framework is constructed using multimodal features, compound action spaces, and a multi-objective reward system to improve search efficiency and convergence. Real-time response is further enhanced through offline pre-training, online fine-tuning, and adaptive learning-rate adjustment. For security defense, a risk-scoring module is combined with quantum-resistant encryption switching and network path reconstruction to support dynamic threat response. Experiments on 10 typical nodes show that the system achieves MAPE of 2.2%, MSE of 0.84, average inference delay of 28.5 ms, and MAPE fluctuation controlled within 2.5%–3.2% in robustness tests.

INDEX TERMS quantum reinforcement learning, dynamic topology perception, 5g energy internet, network security, wireless communication environments

I. INTRODUCTION

WITH the widespread deployment of 5G communication technology and the rapid development of the energy internet, their integration is becoming a key pathway for building next-generation intelligent power system. Such systems rely on this digital infrastructure to ensure real-time power quality and operational reliability in industrial and grid-edge applications [1,2]. The low latency, high reliability, and large connection capabilities of 5G provide strong support for distributed energy scheduling, intelligent power management, and edge load forecasting in the energy internet [3–5]. However, this integration also brings unprecedented challenges: the energy network structure is becoming increasingly complex [6], the network topology changes frequently [7], and the system faces a variety of security threats, such as data tampering, communication interruption, and malicious load injection [8]. In addition, these systems often decouple load forecasting from network structure and ignore the potential impact of system topology on load evolution, thereby reducing the robustness and adaptability of the model, making it more prone to failure under abnormal conditions [9,10].

To address the above issues, this study proposes a network security load forecasting system for the 5G energy internet that integrates quantum proximal policy with a dynamic topology perception mechanism. The system applies graph neural network modeling topology dynamics, perceives network structure evolution in real time, and enhances the structural cognition ability of the model. At the same time, combined with the high-dimensional search and fast convergence characteristics of quantum strategy optimization, it realizes the joint prediction of load value and security risk score in a high-uncertainty environment.

II. RELATED WORK

With the deep integration of 5G and energy internet, load forecasting technology is gradually evolving from traditional static modeling to dynamic perception of complex environments [11,12]. Early studies mostly used classical statistical models, such as Autoregressive Integrated Moving Average

(ARIMA) [13] and Kalman filtering [14], to construct time series models of power loads. Such systems have a certain degree of accuracy in scenarios with strong data regularity and low volatility, but their prediction performance is significantly reduced when faced with nonlinear and sudden load patterns that frequently occur in energy systems. To further improve the model's perception and modeling capabilities of the evolution of complex system structures, network topology perception and graph embedding technology have been widely applied to load forecasting tasks [15,16]. Li Z et al. proposed a hybrid modeling system that combines a Temporal Convolutional Network (TCN) with GraphSAGE, which significantly improved the prediction accuracy and response timeliness of power network equipment load forecasting [17]. Existing studies have attempted to embed intrusion detection and encryption mechanisms into the load forecasting framework. Majeed A et al. proposed a 5G network threat classification method based on deep learning, which uses virtual network function modules to dynamically identify suspicious traffic, achieve early warning and optimize network slice resources, and improve network security and attack detection capabilities [18]. Noor K et al. reviewed the application of machine learning and transfer learning in 5G intrusion detection and explored the potential of deep learning and deep transfer learning models in enhancing DDoS (Distributed Denial of Service) attack detection [19]. However, despite the continuous advancement of QRL theoretical research, its practical application in complex systems such as energy and communications remains relatively limited, especially in combining dynamic structure modeling with safety decision-making tasks; there is still a lack of systematic exploration.

III. CONSTRUCTION AND IMPLEMENTATION OF NETWORK SECURITY LOAD FORECASTING SYSTEM FOR 5G ENERGY INTERNET

A. SYSTEM ARCHITECTURE AND DATA MODELING

1) System Overall Architecture

To achieve real-time power load prediction and risk response control with network security perception capability in the 5G energy internet environment, this paper designs a system architecture that integrates quantum reinforcement learning and dynamic topology modeling. The overall architecture follows the three-layer design concept of "data collection–intelligent decision-making–cooperative execution" to form a closed-loop control system with perception drive and prediction orientation as the core. Its structure is shown in Figure 1:

At the data collection layer, the system deploys multi-source edge sensing nodes at substations, distributed power sources, terminal power equipment, and 5G base stations to collect multi-dimensional communication and power status data, including power load curves, power grid operation status parameters, link delays, packet loss rates, channel occupancy rates, etc. in real time. In addition, it also accesses the real-time alarm event log output by the network security monitoring module. The data collection layer has a built-in data cleaning and preprocessing module that can clean and preprocess the received data, and the processed data is uploaded to the core intelligent decision-making layer through a secure channel.

At the intelligent decision-making layer, the system first uses GraphSAGE and TGAT to model the topology of the 5G communication network, represents the communication nodes, link status, and slice resources as structured graph vectors, and dynamically captures the evolution characteristics of the network topology [20,21]. This topological information, together with historical load sequences and security event records, constitutes the input for the QPPO-based reinforcement learning agent to perform policy reasoning. The intelligent agent structure adopts a hybrid model of quantum variational circuits and classical value networks to learn the strategy distribution and state value function, respectively. In each time step, the intelligent agent predicts the power load value and its corresponding safety risk score of the next cycle based on the current environmental state and updates the strategy based on the difference with the actual feedback. At the execution linkage layer, the prediction results are analyzed and responded to in real time. If the load prediction value is significantly abnormal or the risk score exceeds the set threshold, the system sends a response instruction to the energy dispatch center and the network security protection system through the southbound interface, triggering measures including load migration, backup power activation, communication path reconstruction, or priority allocation of security resources to suppress potential service interruptions and attack spread risks. At the same time, the feedback of the execution results also flows back to the data acquisition layer as input for subsequent strategy training and adaptive adjustment, realizing iterative optimization and closed-loop evolution of the entire system.

2) Multi-Source Data Modeling

In order to achieve joint modeling and decision optimization of load forecasting and network security risks in 5G energy internet, building a unified multi-source heterogeneous data modeling mechanism is the key foundation. This paper proposes a time series fusion modeling framework that embeds multi-modal data such as power, communication, network topology, and security events into a high-dimensional semantic space to provide structured environmental observation input for reinforcement learning agents. In terms of power load and state data modeling, the system uses a sliding time window mechanism to reconstruct the historical data sequence. For any time step t, the input subsequence with a window length of Δt is expressed as:

$$X_t^{load} = \left\{ x_{t-\Delta t+1}^{load}, \ldots, x_t^{load} \right\} \tag{1}$$

$x_t^{load} \in \mathbb{R}^d$ represents the load and power state vector at time t. To improve the model's ability to perceive non-stationary behavior, the first-order difference term is applied:

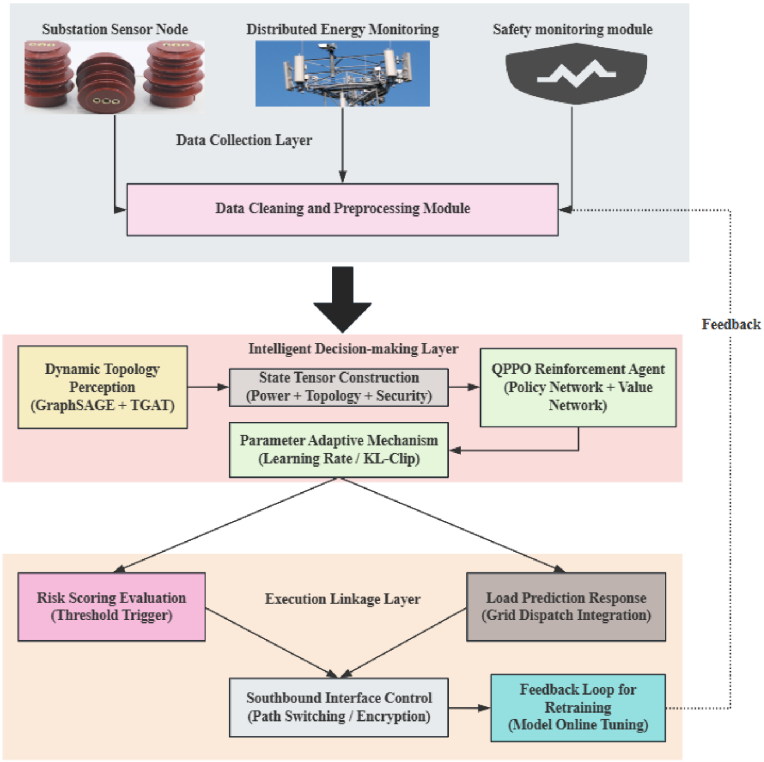

FIGURE 1. System overall architecture

$$\Delta x_t = x_t - x_{t-1} \tag{2}$$

This first-order difference term explicitly models abrupt load variations, thereby increasing the model's sensitivity to anomalous operational states.

In the communication link dimension, a link state tensor $X_t^{comm} \in \mathbb{R}^{N\times N\times f}$ is constructed, where N is the number of nodes and f is the link feature dimension. Each channel $x_t^{comm}(i,j)$ in the tensor represents the quality of the communication link between node i and node j at time t, which is used to characterize the impact of link stability in the prediction path on the overall performance of the system.

To dynamically describe the evolution of the 5G network structure, the system applies a dynamic graph sequence modeling system to represent the network topology state, which is defined as:

$$\mathcal{G} = \{G_1, G_2, \ldots, G_T\}, \quad G_T = (V_t, E_t) \tag{3}$$

V_t and E_t represent the node set and edge set at time t, respectively. The original graph structure is mapped into a low-dimensional vector representation by the graph embedding function:

$$\phi : G_t \mapsto G_t^{topo} \in \mathbb{R}^{N\times d_g} \tag{4}$$

This representation is used to capture the connection relationships, path weight change, and topology reconstruction pattern in the network structure and provide microstructure features for reinforcement learning.

In terms of network security event modeling, the system constructs a discrete event sequence:

$$A_t^{sec} = \{a_{t,1}, a_{t,2}, \ldots\}, \quad a_{t,k} = (l_k, c_k, s_k) \tag{5}$$

l_k, c_k, and s_k represent the location, category, and severity of the event, respectively. Through the time alignment function $\psi(t_k) \mapsto t$, the asynchronous security events are mapped to the unified time scale, and the sparse event embedding vector is further constructed.

B. DESIGN OF DYNAMIC TOPOLOGY PERCEPTION MODULE

1) Network Event Monitoring and Topology Change Detection Mechanism

In order to achieve real-time perception and dynamic modeling of the communication topology of 5G energy internet, this study builds a network event monitoring and topology change detection mechanism that integrates link state perception, anomaly detection, and topology evolution analysis. The system deploys link quality monitoring modules in the core network and edge nodes to continuously collect key performance indicators such as round-trip delay, packet loss rate, and link bandwidth utilization. These data are input into the topology perception module as a direct representation of the network operation status.

For the rapid identification of structural mutations, the system applies an event triggering model based on statistical deviations. When link indicators fluctuate dramatically in

a short period of time, the system classifies such abrupt fluctuations as candidate topological disturbance events and triggers an incremental update of the topology embedding. On this basis, to capture the structural evolution trend of nodes and links, the system adopts a differential detection strategy within a sliding time window and defines the difference between the topological structure G_t at any moment and G_{t-1} at the previous moment as the topological change matrix:

$$\Delta G_t = G_t - G_{t-1} \tag{6}$$

This matrix is used to record the information of newly added or disconnected nodes and edges as the basis for triggering the graph neural network to update node embedding, ensuring that the topology perception module can maintain high sensitivity and rapid response capabilities to changes in network structure in complex dynamic environments.

2) Topological Vector Generation Strategy Based on Graph Neural Network

In the dynamic topology perception module, to extract high-level semantic features from the time-varying graph structure, the system applies the GNN embedding mechanism. Recent studies have demonstrated the strong capability of GNNs in capturing complex spatiotemporal dependencies in energy systems and dynamic evolutionary patterns in communication links [22,23]. Inspired by these advances, this system combines GraphSAGE and TGAT to achieve structural and temporal modeling of the network topology. GraphSAGE, as a static graph encoder, learns the local structural representation of the node at the current moment G_t based on the neighbor sampling and aggregation mechanism. Its core idea is to generate a node vector representation with structural perception ability by aggregating information from multi-order neighbors:

$$h_i^t = \sigma\left(W \cdot AGG\left(\{v_i^t\} \cup \{v_j^t : j \in \mathcal{N}(i)\}\right)\right) \tag{7}$$

$AGG(\cdot)$ represents the aggregation function; σ is the activation function and W is the training learnable weight matrix.

The GraphSAGE output is then processed by TGAT, which jointly models temporal evolution and inter-node dependencies through time-aware graph attention. TGAT combines the time encoding mechanism with the graph attention mechanism to perform temporal modeling of node embedding in asynchronous event-driven scenarios and finally forms a node representation matrix $H_t \in \mathbb{R}^{N \times d_h}$ with time dependency. Then, the system uses the Global Average Pooling operation to integrate all node embeddings into a unified topological representation vector:

$$G_t^{topo} = \frac{1}{N} \sum_{i=1}^{N} h_i^t \in \mathbb{R}^{d_g} \tag{8}$$

This topological vector serves as a compact semantic encoding of the current network structure. The millisecond-level reconstruction claim is validated under the following experimental conditions: network size of 10-50 nodes with average degree 3.2, event-driven updates triggered by topology changes, and execution on an NVIDIA A100 GPU. Under this setup, the GraphSAGE-TGAT pipeline completes embedding updates in an average of 8.7 ms per event, satisfying the sub-10 ms requirement for 5G network slicing control loops. Together with other modal inputs such as load, communication links, and security events, it constitutes the state space input of the intelligent agent, which is used to support the prediction and decision-making process of quantum reinforcement learning in complex dynamic environments.

3) Topology Embedding Update Mechanism

To ensure that the reinforcement learning agent can continuously obtain graph representation information with timeliness and structural discrimination in a dynamic network environment, this paper designs and implements a topology embedding update mechanism that integrates event-driven and periodic scheduling. The execution process of this mechanism is shown in Figure 2:

This mechanism can dynamically adjust the update frequency and calculation granularity of the topology representation according to different types of network status changes so as to improve the accuracy of system status perception and the timeliness of policy response.

C. QPPO REINFORCEMENT LEARNING AGENT CONSTRUCTION

1) State Space Design

In this study, the construction of the state space S_t aims to provide the reinforcement learning agent with multi-modal observation input with timeliness, structure, and security perception. The system extracts the load of recent power load through the sliding window mechanism to reflect the power historical sequence X_t^{load} consumption trend and fluctuation pattern before the current moment. In order to characterize the dynamic characteristics of the power grid topology, this paper adopts a heterogeneous graph neural network model composed of GraphSAGE and TGAT to model and embed the current topology graph G_t and generate a topology representation vector G_t^{topo} to capture the network connection relationship and its evolution trajectory. At the communication level, the system collects key operating indicators of the link in real time, including latency, utilization, and packet loss rate, to form a communication state vector X_t^{comm} used to reflect the quality and stability of network transmission. At the same time, the alarm information extracted through security logs and attack detection mechanisms is encoded as A_t^{sec} to represent the potential risks and threat scenarios faced by each node and link at any time.

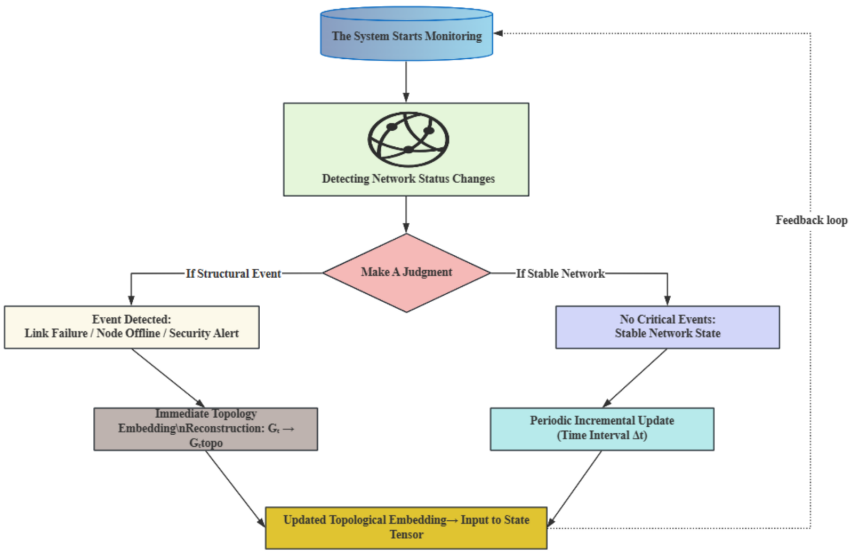

FIGURE 2. Execution process of topology embedding update mechanism integrating event-driven and periodic scheduling

Based on a unified timestamp and node index system, the above multi-source modal features are synchronously aligned and fused into a unified state tensor. Prior to fusion, each modality undergoes domain-specific normalization: load sequences are Z-score standardized; communication metrics (latency, packet loss, utilization) are min-max scaled to [0, 1]; topology embeddings are L2-normalized; security events are one-hot encoded and aligned to the temporal grid via nearest-event interpolation. The resulting normalized vectors are concatenated along the feature dimension to form $X_t \in \mathbb{R}^{N\times(5d_{load}+d_{comm}+d_{topo}+d_{sec})}$, which serves as the sole observation input to the QPPO agent.

$$S_t = \left[X_t^{load}, X_t^{comm}, A_t^{sec}, G_t^{topo}\right] \tag{9}$$

This tensor is used as environmental observation input and embedded into the agent's policy network to support its optimal action selection and dynamic response generation in the tasks of power load forecasting and network risk linkage control.

2) Action Space Definition

In this study, the action space A_t of the reinforcement learning agent is designed around the two core tasks of "load forecasting" and "risk response", and a continuous vector form is used to achieve joint optimization of multi-objective control. In each decision cycle, the agent outputs an action vector containing two main types of control instructions based on the current state tensor S_t.

In terms of load forecasting, the agent generates a power load forecast sequence for the next H time steps through a regression model:

$$\widehat{Y}_t = \{\widehat{y}_{t+1}, \widehat{y}_{t+2}, \ldots, \widehat{y}_{t+H}\} \tag{10}$$

The output dimension of this sequence is consistent with the prediction window length H, which serves as a guide for power grid operation and resource scheduling. The sliding window mechanism is used to dynamically embed the prediction results into the training framework, effectively improving the temporal coherence and error control capabilities of the prediction.

In terms of risk response, a risk score generation module is integrated into the action space to output node-level or link-level risk vectors based on joint modeling of structure and security features:

$$R_t^{risk} = \{r_{t,1}^{risk}, r_{t,2}^{risk}, \ldots, r_{t,N}^{risk}\} \tag{11}$$

N represents the total number of observed nodes in the current topology. The risk score integrates the multi-modal information of topological embedding G_t^{topo}, communication status X_t^{comm}, and security event encoding A_t^{sec} through a nonlinear mapping module, extracts discriminant features, realizes the quantitative expression of potential system threats, and supports the formulation of early warning triggers and risk control strategies. This risk score is not an auxiliary output but a causal modulator of the load forecasting process. Specifically, it gates the attention weights in the policy network's load prediction branch and dynamically scales the edge weights in the GraphSAGE aggregation for affected nodes. When a high-risk score is assigned to node i, its historical load contribution to neighbors is down-weighted during topology embedding, and its future load trajectory receives higher gradient emphasis during training. This mechanism establishes a direct, differentiable pathway from security perception to load prediction, ensuring that detected threats actively reshape the forecasting dynamics rather than merely coexist as parallel signals.

3) Reward Function Design

The reward function R_t designed in this study aims to achieve a balance between the load forecasting accuracy,

safety risk perception accuracy, and system resource control overhead of the reinforcement learning agent. The reward function adopts a multi-index weighted form to quantitatively give feedback on the comprehensive performance of each round of decision-making behavior.

In terms of load forecasting, after the agent outputs the forecast sequence at time t, it compares the forecast value with the actual load data Y_t and constructs the forecast error loss term:

$$R_t^{error} = MSE(\widehat{Y}_t, Y_t) \tag{12}$$

This loss term is used to penalize the deviation of load forecasting and promote the model to continuously improve the accuracy and stability of multi-step time series forecasting.

In terms of security risk perception, the system uses actual attack logs and risk labels to build a "real risk baseline" and compares it with the node-level risk score vector $\widehat{r}_t^{risk}$ output by the model. For high-risk nodes that are not accurately identified, a risk omission penalty term $R_t^{risk\_penalty}$ is designed. This penalty term enhances the model's recognition sensitivity for high-risk events and improves the system's risk perception ability and security defense response efficiency.

To avoid excessive regulation or unnecessary high-frequency response of the model during strategy execution, the system applies a resource consumption cost function, R_t^{cost}, which covers two main types of expenses, namely computing resource cost and network regulation cost. To enhance the long-term stability of the strategy, the reward function applies a time discount factor $\gamma \in (0, 1)$ to balance the immediate reward with future potential benefits, prompting the agent to learn a strategy sequence with global optimality and improve the sustainability of the overall response.

Based on the above design, the reward function expression is as follows:

$$R_t = -\lambda_1 \cdot MSE(y_t, \widehat{y}_t) - \lambda_2 \cdot RiskPenalty_t - \lambda_3 \cdot Cost_t \tag{13}$$

λ_1, λ_2 and λ_3 are weight coefficients, which are dynamically adjusted according to the multi-objective priorities in the training phase. During the training process, the policy gradient system is used to backpropagate the reward signal to guide the reinforcement learning agent to continuously optimize the load forecasting accuracy, risk response sensitivity, and resource regulation balance ability under continuous time series.

4) QPPO Agent Design

After completing the system construction of state space, action space, and reward function, this paper designs a QPPO agent architecture with structural perception and task decoupling capabilities for the complex task of network security and load forecasting in 5G energy internet. The agent consists of a policy network and a value network, integrating graph feature encoding, modal fusion, and multi-channel output mechanism to achieve efficient modeling and coordinated response to multi-source heterogeneous information. Its specific structure is shown in Figure 3:

The policy network is based on the Multi-Layer Perceptron (MLP) and combines residual connections and layer normalization modules to improve the stability and generalization of deep feature representation. The network front-end integrates a graph feature encoding module to perform structured processing on the current power communication topology G_t, and embeds and fuses it with multi-modal information such as load time series data, communication status, and security events to generate a unified state tensor S_t as the input basis for policy decision-making.

To meet the dual goals of network security load forecasting, a multi-channel output structure is designed at the end of the strategy network: on the one hand, a power load forecast sequence for the next H steps is generated to guide the system operation trend; on the other hand, a node-level risk score vector is output to provide decision support for precise regulation of high-risk areas. The two types of outputs are independently modeled by task-specific branches, and information sharing is dynamically adjusted through a gating mechanism, ensuring task complementarity while improving information utilization.

IV. SYSTEM EFFECTIVENESS EVALUATION

A. EXPERIMENTAL SETUP

1) Experimental Environment Configuration

This study conducts experiments on a high-performance hardware and software platform to ensure the efficiency of model training and the credibility of evaluation results. The server used in the experiment runs the Ubuntu 20.04 LTS system, equipped with an Intel Xeon Gold 6338 processor (2.0 GHz, 32 cores), 64 GB DDR4 ECC memory, and a 4 TB NVMe solid-state drive, providing support for large-scale data processing and parallel computing. Model training and inference are accelerated on the NVIDIA Tesla A100 GPU, which effectively improves computing efficiency and convergence speed.

The software environment is based on the PyTorch 1.12 framework, with CUDA 11.6 and cuDNN 8.4 for GPU acceleration, and integrates common libraries such as NumPy, Matplotlib, and Scikit-learn to complete data processing and performance analysis. The experiment relies on the self-developed power system and 5G slice joint simulation platform, covering modules such as power grid topology construction, load scheduling, communication modeling, and security event injection. It can simulate the multi-source dynamic interaction process in the power-communication coupling environment and provide realistic simulation support for intelligent agent strategy learning.

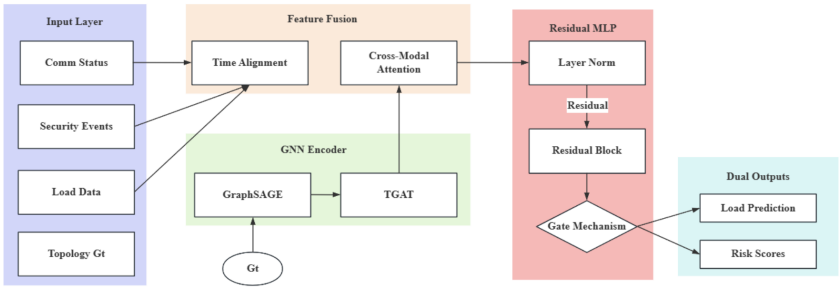

FIGURE 3. QPPO agent structure diagram

2) Experimental Data

The data set used in this experiment is consistent with the model training stage in the previous paper to ensure the consistency of the training evaluation process and the repeatability of the system verification. The data comes from the log of the power-communication collaborative system actually running in a certain area, covering three main dimensions: about 7.1 million power load samples, covering the power demand changes of multiple time periods and nodes; about 2.3 million communication status data, including key performance indicators such as link bandwidth, latency, and packet loss rate; 134,000 security event records, including abnormal power fluctuations, communication anomalies, equipment alarms, and potential attacks. Of these, 70% of the load samples (approximately 5.0 million), communication records (1.6 million), and security events (94,000) constitute the offline pre-training dataset, covering historical operational and disturbance scenarios. The remaining 30% (2.1 million load samples, 0.7 million communication records, and 40,000 security events) form the online fine-tuning environment, where data streams simulate real-time topology mutations and novel attack patterns. During fine-tuning, the agent receives data via a sliding window of 100 time steps and updates its policy every 100 steps using an initial learning rate of 0.001, which is adaptively decayed by a factor of 0.95 whenever the policy loss plateaus for more than 5 consecutive updates.

3) Comparison of System Settings

In order to comprehensively evaluate the performance of the constructed system, this study sets up four representative comparison systems, covering traditional statistical modeling, mainstream deep learning technology, and the current more advanced reinforcement learning and time series modeling algorithms. Control Group 1 is a prediction system based on the traditional statistical model ARIMA, which has good linear prediction capabilities; Control Group 2 is a prediction system based on the classic deep learning model Long Short-Term Memory (LSTM), which is suitable for processing the long-term dependency characteristics of time series; Control Group 3 is a prediction system based on the Transformer model with self-attention mechanism, which is good at global time series modeling and multivariate fusion; Control Group 4 is a prediction system based on Multi-Agent Deep Reinforcement Learning (MADRL), which can cope with complex dynamic environments through distributed agent collaborative decision-making. All the models required by the system are trained and evaluated under the unified data set and experimental platform to ensure the fairness and comparability of the results.

B. EXPERIMENTAL PROCESS AND RESULTS ANALYSIS

1) Load Forecasting Effect Analysis

In the load forecasting performance evaluation experiment, this study uses the load data of 10 typical nodes in the experimental data set and uses each group of systems to perform rolling forecasts on the node loads for the next hour. During the experiment, for each time step, the predicted value of each group and the corresponding true load value are recorded. Based on the collected forecast data, the MAPE and MSE of each group on the 10 nodes are calculated to quantify their forecast accuracy. To ensure the stability of the results, the forecasting experiment is repeated 10 times, and the average is taken as the final result. The results are shown in Figures 4 and 5:

From the experimental results of Figures 4 and 5, it can be seen that the system constructed in this paper shows the best performance in the load forecasting tasks of 10 typical nodes. The average MAPE of QPPO is 2.2%, and the average MSE is 0.84, which is significantly better than other comparison systems, indicating that it maintains high prediction capabilities under the interference of dynamic topology and security risks. This advantage can be attributed to the synergy between quantum reinforcement learning and dynamic topology perception: quantum strategy optimization improves the model's exploration efficiency of high-dimensional state space, while the real-time modeling of network structure evolution by graph neural network enhances the model's adaptability to topological perturbations. Transformer and MADRL have the second-highest prediction accuracy, with average MAPE of 3.57% and 3.88% and average MSE of 1.53 and 1.73, respectively. Transformer captures global temporal dependencies through the self-attention mechanism, while MADRL uses multi-agent collaborative decision-making to cope with a dynamic environment. Both have certain structural perception capabilities, but their prediction stability is still weaker than QPPO when dealing with sudden load patterns and security

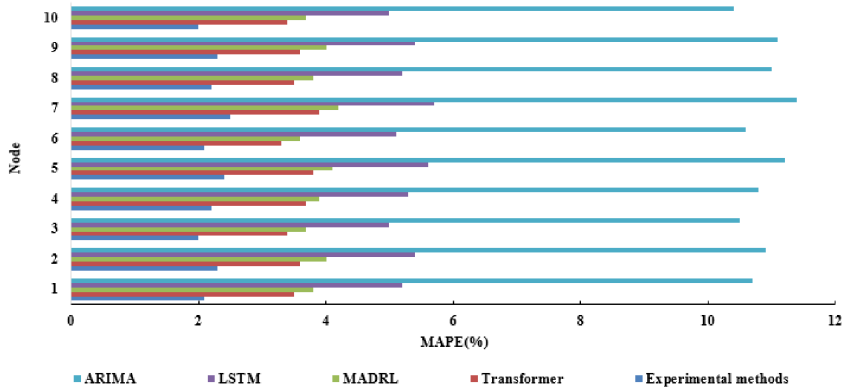

FIGURE 4. MAPE results of each group

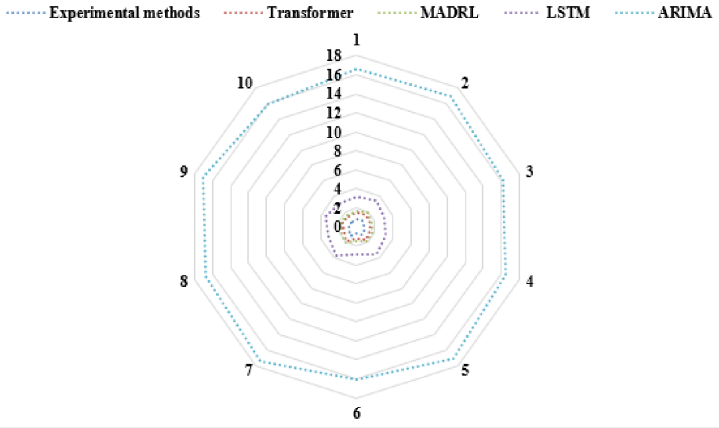

FIGURE 5. MSE results of each group

incident interference in 5G energy internet.

2) System Real-Time Analysis

In order to evaluate the response speed of each system in the actual deployment scenario, this study conducts a system real-time test experiment. The experiment uses 1,000 sets of continuous node status data selected from the experimental data set as input. Each set of data completes a complete forward reasoning process and records the time required for the process. Finally, the average reasoning delay and standard deviation of each group on all samples are calculated. The experimental results are shown in Table 1:

TABLE 1. Statistics of average inference latency and standard deviation of each group

Method	Average inference latency (ms)	Standard deviation (±ms)
Experimental methods	28.5	± 3.2
Transformer	82.1	± 7.6
MADRL	135.4	± 12.3
LSTM	45.8	± 5.1
ARIMA	9.7	± 1.5

As can be seen from the data in Table 1, different systems have significant differences in single inference latency, and the stability of their latency is closely related to model complexity. The ARIMA model performs best in terms of inference efficiency, with an average inference latency of 9.7 ms and a standard deviation of ± 1.5 ms. This is mainly due to its structural simplicity based on linear modeling, which can complete predictions without complex calculations. However, the static modeling characteristics of ARIMA make it difficult to adapt to dynamic topological structures and complex security risk environments, limiting the breadth of its practical application scenarios. The system in this paper takes into account both accuracy and real-time requirements with an average inference delay of 28.5 ms and a standard deviation of ± 3.2 ms. This performance advantage is mainly due to the lightweight structure of the designed quantum reinforcement learning mechanism and dynamic topology perception module: the quantum variational circuit effectively compresses the strategy search space through parameterized quantum gates.

A comprehensive comparison of the performance of each system shows that the system constructed in this paper achieves a better balance between real-time reasoning and stability. Its average latency and standard deviation are significantly lower than those of Transformer and MADRL, verifying the effectiveness of quantum strategy optimization

and topology perception mechanism in improving prediction efficiency and robustness. The results show that QPPO has the potential to achieve low-latency, high-stability load forecasting and risk response in the dynamic environment of 5G energy internet, and has good edge deployment feasibility. Although ARIMA performs best in terms of inference latency, its lack of prediction accuracy limits its promotion value in complex application scenarios.

3) System Robustness Analysis

To comprehensively evaluate the prediction stability and fault tolerance performance of each system under dynamic abnormal conditions, this study constructs three typical disturbance scenarios based on the original simulation environment: line fault disconnection, sudden increase in load side, and node disconnection and reconnection. Each type of disturbance setting generates 10 groups of disturbance samples, the disturbance duration is set to 15 minutes, and the prediction target is maintained as "node load in the next 1 hour". In each disturbance scenario, the prediction error of each system is recorded separately, and the fluctuation amplitude and standard deviation of its MAPE are calculated to measure the stability of the model prediction performance. The experimental results are shown in Table 2:

TABLE 2. Records of MAPE fluctuation range and standard deviation of each group under different disturbances

Disturbance scenario	Method	MAPE fluctuation range (%)	Standard deviation (±%)
Line fault disconnection	Experimental methods	2.8	± 0.9
	Transformer	5.1	± 1.6
	MADRL	6.3	± 2.1
	LSTM	7.9	± 2.7
	ARIMA	14.2	± 3.8
Sudden increase in load side	Experimental methods	3.2	± 1.1
	Transformer	5.5	± 1.8
	MADRL	6.7	± 2.3
	LSTM	8.4	± 3.0
	ARIMA	15.6	± 4.2
Node disconnection and reconnection	Experimental methods	2.5	± 0.8
	Transformer	4.9	± 1.5
	MADRL	6.0	± 2.0
	LSTM	7.6	± 2.6
	ARIMA	13.9	± 3.6

From the experimental data in Table 2, it can be seen that the prediction stability of each system under different disturbance scenarios shows significant differences. The MAPE fluctuation amplitude of QPPO in three typical disturbances is controlled within the range of 2.5%–3.2%, and the standard deviation does not exceed ± 1.1%, which is significantly better than other comparison systems. This advantage is mainly due to the real-time encoding ability of its dynamic topology perception module for network structure changes– through the collaborative modeling of graph neural network and TGAT, the system can quickly capture dynamic features such as topological fracture and node reconstruction and rely on the strategy optimization ability of quantum reinforcement learning to maintain prediction robustness in a high uncertainty environment. In contrast, the fluctuation ranges of Transformer and MADRL are in the range of 4.9%–5.5% and 6.0%–6.7%, respectively, and their standard deviations are much higher than those of the system in this paper, reflecting the lack of adaptability of deep learning models to topological dynamics and the delayed effect of multi-agent collaboration. Due to the inherent timing dependence of recurrent neural networks, the MAPE fluctuation of LSTM in the load surge scenario reaches 8.4% (standard deviation ± 3.0%), exposing the defect of lagging response to mutation trends. The traditional ARIMA performs the worst in all disturbance scenarios, with fluctuations as high as 13.9%–15.6%. Its linear assumptions and static modeling mechanism cannot cope with the dynamic topology reconstruction and security risk impact of the 5G energy internet. It is worth noting that the sudden increase in load poses the greatest challenge to the prediction stability of all systems, and the MAPE fluctuations are generally large, which shows that sudden load changes have higher requirements for the model's timing sensitivity.

C. ABLATION AND SENSITIVITY ANALYSIS

1) Ablation of Topology-Aware Module on and off

In order to systematically evaluate the performance contribution of the topology-aware module in the model, this study designs and conducts a multi-variant ablation experiment of the topology-aware module. The experiment is conducted using the same load data and security event scenarios as the main experiment. By gradually removing or replacing the key mechanisms in the module, the effects of different module configurations on the model's load prediction accuracy and security detection capabilities are compared. To this end, this study sets up five model variants for comparison: complete model, removing topology awareness module, replacing dynamic graph modeling with static graph embedding with fixed topology structure, using static GNN to extract node features, removing topology evolution awareness and retaining timing update strategy, and removing topology modeling capability. The experiment records load forecast error indicators (MAPE, MSE) and safety detection performance indicators (missing rate and false alarm rate) under each configuration to quantify the performance differences of each variant. The results are shown in Figure 6:

As shown in Figure 6, this module plays a key role in improving the prediction accuracy and safety detection capabilities of the model. The complete model performs best in terms of load forecast error, with a MAPE of 2.2%, an MSE of 0.84, and a false alarm rate of 3.2% and a false alarm rate of 1.8%, respectively, indicating that the model can achieve strong anomaly recognition capabilities with high accuracy. When the topology perception module is completely removed, the MAPE rises to 4.23%, the MSE increases to 2.15%, and the false alarm rate and false alarm rate rise to 4.7% and 2.9%, respectively, with a significant drop in performance, which verifies the importance of this module in modeling structural changes and risk diffusion in a dynamic network environment.

Further comparison of different variant configurations

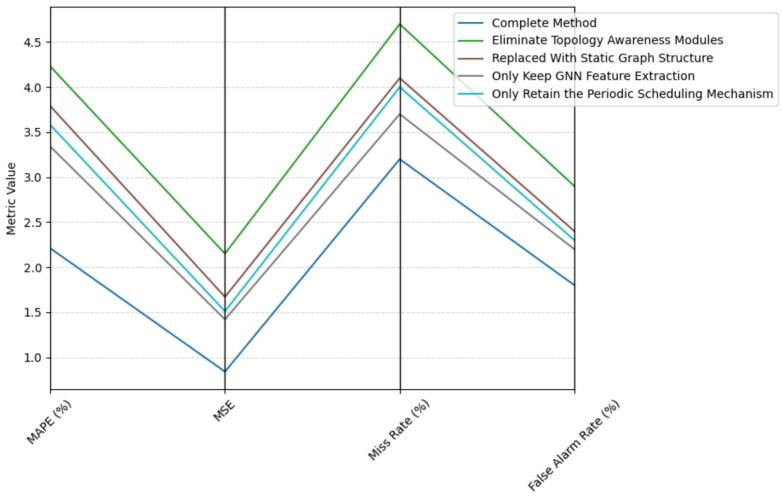

FIGURE 6. Results of the topology-aware module opening and closing ablation experiment.

shows that even if some structural modeling capabilities are retained, the model performance is still limited. After replacing the dynamic graph with a static graph structure, the MAPE and MSE are 3.79% and 1.67%, respectively, and the detection indicators also deteriorate to varying degrees, indicating that the static graph cannot effectively adapt to the complex dynamic characteristics brought about by the evolution of network topology over time. The model that only retains the GNN feature extraction mechanism is slightly better than the static graph solution in terms of error indicators, but in the absence of time-series scheduling support, its response to sudden risk events is still lagging. The configuration that only retains the periodic scheduling mechanism is slightly inferior to the GNN retention solution in various indicators, further demonstrating the core value of topology perception in event prediction and discrimination.

To evaluate the incremental contribution of all three core components—Dynamic Topology Perception (DTP), Security Feature Integration (SFI), and QPPO-based forecasting—we constructed four variants: (1) Full model;

(2) Full model without SFI (i.e., security event inputs and risk scoring removed); (3) Full model with static adjacency matrix replacing DTP; (4) QPPO backbone with only load time series (no topology or security inputs). All variants were evaluated on the same test set. Table 3 reports their MAPE scores: (1) 2.2%, (2) 2.8%, (3) 3.1%, (4) 4.2%. This demonstrates that both DTP and SFI provide non-redundant, additive performance gains, and that the system's complexity is fully justified by empirical gains.

TABLE 3. Ablation study of the three core components

Model Variant	MAPE (%)
Full model	2.2
– Security Feature Integration	2.8
– Dynamic Topology Perception (static graph)	3.1
QPPO backbone only (load sequences)	4.2

2) Impact of Different Quantum Circuit Depths and Quantum Bit Numbers

To evaluate the impact of quantum module structural parameters on model performance, this study designed a dual-factor experiment of quantum circuit depth and quantum bit number to systematically examine its role in training convergence speed and prediction accuracy. In terms of variable settings, the quantum circuit depth is selected as 2 layers, 4 layers, 6 layers and 8 layers, representing the number of stacked layers of parameterized quantum gates; the number of quantum bits is selected as 4, 6, 8 and 10 to control the dimension of mapping input features to quantum state space, forming a total of 16 groups of combined models for experimental comparison. During the experiment, the convergence speed of the model training process under each group of settings is recorded, that is, the number of iterations required for the loss function to enter the stable range, the MAPE and MSE of the model in the load forecasting task, and the false alarm rate and false alarm rate in the security incident detection task. The experimental results are shown in Table 4:

Based on the experimental results shown in Table 4, different combinations of quantum circuit depth and quantum bit number have a significant impact on model performance. In terms of training convergence, as the circuit depth and quantum bit number increase, the model generally shows a faster convergence speed, and the number of iterations required for convergence gradually decreases from 140 in the shallow structure to 104 under the optimal combination. However, when the circuit is too deep, or the number of bits is too large, the number of convergence rounds rises slightly, indicating that the training efficiency may be affected after the structural complexity increases.

In the load forecasting task, both MAPE and MSE decrease significantly with structural optimization, and the best results also appear in the 6-layer loop and 8-bit combination, reaching 2.28% and 0.83, respectively, which is signifi-

TABLE 4. System performance records under different quantum circuit depths and quantum bit numbers

Quantum circuit depth	Number of qubits	Iteration rounds	MAPE	MSE	Miss Rate	False Alarm Rate
2	4	140	3.84	1.96	5.1	3.0
2	6	135	3.61	1.72	4.8	2.7
2	8	132	3.55	1.65	4.5	2.6
2	10	130	3.52	1.61	4.4	2.6
4	4	120	3.12	1.34	4.0	2.4
4	6	110	2.75	1.12	3.6	2.2
4	8	105	2.51	0.95	3.3	2.0
4	10	103	2.47	0.91	3.2	1.9
6	4	115	2.98	1.18	3.8	2.3
6	6	108	2.56	0.96	3.3	2.0
6	8	104	2.28	0.83	3.1	1.8
6	10	105	2.29	0.84	3.2	1.8
8	4	120	3.05	1.22	4.0	2.5
8	6	112	2.62	0.98	3.5	2.1
8	8	108	2.34	0.86	3.1	1.9
8	10	110	2.33	0.85	3.2	1.9

cantly improved compared with the shallow structure. This shows that medium-depth and high-dimensional quantum state mapping can help improve the fitting accuracy of the model and capture more complex nonlinear time series relationships.

To rigorously justify the practical benefit of the quantum component, we conducted a controlled ablation experiment comparing the full QPPO agent against a classical PPO baseline. The PPO variant retains the identical state tensor, action space formulation, and reward function design, differing only in the replacement of the quantum variational policy network with a classical MLP.

As shown in Table 5, QPPO achieves a MAPE of 2.2% versus 2.9% for PPO, an MSE of 0.84 versus 1.12, and maintains a narrower MAPE fluctuation range under disturbances (2.5%–3.2% vs. 3.1%–4.0%). The inference latency of QPPO (28.5 ms) is also lower than that of PPO (31.2 ms), confirming that the quantum circuit enhances both convergence efficiency and real-time robustness rather than introducing superfluous complexity.

TABLE 5. Performance comparison between QPPO and classical PPO under identical experimental conditions

Method	MAPE (%)	MSE	Inference Latency (ms)	MAPE Fluctuation Range (%)
QPPO	2.2	0.84	28.5	2.5–3.2
PPO	2.9	1.12	31.2	3.1–4.0

V. CONCLUSION

The 5G energy internet network security load forecasting system based on quantum reinforcement learning and dynamic topology perception proposed in this paper shows significant advantages in multi-dimensional performance evaluation, translating directly into enhanced stability and security for critical industrial infrastructure, which is particularly beneficial for automated high-precision operations in the industry. Experimental results show that the system has an average MAPE of only 2.2% and an MSE of 0.84 in the load forecasting task of 10 typical nodes, which is significantly better than other comparison methods, proving that it can still maintain high-precision prediction capabilities under the interference of dynamic topology and security threats. At the same time, the average inference delay of the system is only 28.5 milliseconds, and the MAPE fluctuation amplitude in various disturbance scenarios is controlled within the range of 2.5%–3.2%, showing excellent real-time robustness. In addition, the system achieved a 3.2% false alarm rate and a 1.8% false alarm rate in the security incident detection task, and the F1-score reached 0.92, verifying its ability to accurately identify network security threats. These results show that the system in this paper has achieved the modeling capability of millisecond-level dynamic reconstruction of network structure through the dynamic topology perception module, effectively solving the problem of the surge in prediction errors caused by the lag in topological evolution in traditional methods. The QPPO framework significantly improves the strategy convergence efficiency and security threat response accuracy in complex environments through the high-dimensional strategy search capability and multi-modal feature modeling of quantum variational circuits, providing a solution that combines accuracy, efficiency, and robustness for network security load forecasting in 5G energy internet.

Although the effectiveness of the system in this paper has been verified in a simulation environment, there are still two limitations. On the one hand, the current quantum variational circuit relies on a classical-quantum hybrid architecture, which is limited by the size of quantum bits and noise interference. The actual deployment requires further optimization of quantum circuit design. On the other hand, the evaluation is conducted on a high-fidelity simulation platform, and the complex working conditions and long-term stability in real scenarios still need to be verified. In addition, the adaptability of dynamic topology modeling to changes in network structure and the completeness of security event labels may affect the generalization performance of the model.

In response to the above shortcomings, future work will advance along three directions: The first step includes

extending the use of large-scale quantum processors while eliminating barriers associated with quantum bits and error-correcting codes; also improving strategy optimization efficiency. The second phase will involve developing a secure decentralized environment in conjunction with other technologies such as blockchain and federated learning. This allows for improved response capabilities for advanced persistent threats. Finally, the goal of this project is to demonstrate the flexibility and extensible nature of the quantum processors when used in a dynamic topology system, such as intelligent transportation systems or in the context of an industrial internet.

AUTHOR CONTRIBUTIONS

Conceptualization –Wangdong Wu, Yongdong Dai, Shenyu Wang, Maofei Wang, Weijian Xiao and Yi Zhou; methodology – Wangdong Wu, Yongdong Dai, Shenyu Wang, Maofei Wang and Weijian Xiao; investigation – Wangdong Wu, Yongdong Dai, Shenyu Wang, Maofei Wang, Weijian Xiao and Yi Zhou; writing-original draft preparation – Wangdong Wu, Yongdong Dai, Shenyu Wang, Maofei Wang, Weijian Xiao and Yi Zhou. All authors have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

FUNDING

This research was supported by State Grid Jiangsu Electric Power Co., Ltd. Technology Project (J2021124 Research and Application of 5G Deterministic Network Technology and Power Business Adaptability).

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

[1] D. Hemanand, D. S. Jayalakshmi, U. Ghosh, A. Balasundaram, P. Vijayakumar, and P. K. Sharma, "Enabling sustainable energy for smart environment using 5G wireless communication and internet of things," IEEE wireless communications, vol. 28, no. 6, pp. 56-61, 2022, doi: 10.1109/MWC.013.2100158.

[2] H. Heidari, O. Onireti, R. Das, and M. Imranet, "Energy harvesting and power management for IoT devices in the 5G era," IEEE Communications Magazine, vol. 59, no. 9, pp. 91-97, 2021, doi: 10.1109/MCOM.101.2100487.

[3] B. Zhou, J. Zou, C. Y. Chung, H. Wang, N. Liu, N. Voropai, et al., "Multi-microgrid energy management systems: Architecture, communication, and scheduling strategies," Journal of Modern Power Systems and Clean Energy, vol. 9, no. 3, pp. 463-476, 2021, doi: 10.35833/MPCE.2019.000237.

[4] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence Internet of Things and 5G for nextgeneration smartgrid: A survey of trends challenges and prospect," IEEE Access, vol. 10, pp. 4794-4831, 2022, doi: 10.1109/ACCESS.2022.3140595.

[5] S. Ahmadzadeh, G. Parr, and W. Zhao, "A review on communication aspects of demand response management for future 5G IoT-based smart grids," IEEE Access, vol. 9, pp. 77555-77571, 2021, doi: 10.1109/ACCESS.2021.3082430.

[6] S. Malathy, P. Jayarajan, H. Ojukwu, F. Qamar, M. H. D. N. Hindia, K. Dimyati, et al., "A review on energy management issues for future 5G and beyond network," Wireless Networks, vol. 27, pp. 2691-2718, 2021, doi: 10.1007/s11276-021-02616-z.

[7] Y. Chen, Y. A. Sambo, O. Onireti, and M. A. Imran, "A survey on LPWAN-5G integration: Main challenges and potential solutions," IEEE Access, vol. 10, pp. 32132-32149, 2022, doi: 10.1109/ACCESS.2022.3160193.

[8] H. N. Fakhouri, S. Alawadi, F. M. Awaysheh, I. B. Hani, M. Alkhalaileh, and F. Hamad, "A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions," Electronics, vol. 12, no. 22, pp. 4604-4648, 2023, doi: 10.3390/electronics12224604.

[9] H. Liu, X. Xiong, B. Yang, Z. Cheng, K. Shao, and A. Tolba, "A power load forecasting method based on intelligent data analysis," Electronics, vol. 12, no. 16, pp. 3441-3458, 2023, doi: 10.3390/electronics12163441.

[10] Y. Yan, Y. Liu, J. Fang, Y. Lu, and X. Jiang, "Application status and development trends for intelligent perception of distribution network," High Voltage, vol. 6, no. 6, pp. 938-954, 2021, doi: 10.1049/hve2.12159.

[11] L. Ge, Y. Li, Y. Li, J. Yan, and Y. Sun, "Smart distribution network situation awareness for high-quality operation and maintenance: a brief review," Energies, vol. 15, no. 3, pp. 828-852, 2022, doi: 10.3390/en15030828.

[12] N. Fazrina, "Securing distributed sensor systems through adaptive encryption algorithms in 5G-based smart energy networks," Open Journal of Robotics, Autonomous Decision-Making, and Human-Machine Interaction, vol. 9, no. 11, pp. 18-27. https://openscis.com/index.php/OJRADHI/article/view/2024-11-10, 2024.

[13] C. Tarmanini, N. Sarma, C. Gezegin, and O. Ozgonenel, "Short term load forecasting based on ARIMA and ANN approaches," Energy Reports, vol. 9, pp. 550-557, 2023, doi: 10.1016/j.egyr.2023.01.060.

[14] M. Almiani, A. AbuGhazleh, Y. Jararweh, and A. Razaque, "DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network," International Journal of Machine Learning and Cybernetics, vol. 12, no. 11, pp. 3337-3349, 2021, doi: 10.1007/s13042-021-01323-7.

[15] Z. Zhang and C. Wang, "Service function chain migration: a survey," Computers, vol. 14, no. 6, pp. 203-217, 2025, doi: 10.3390/computers14060203.

[16] B. Zhang, Q. Fan, X. Zhang, Z. Fu, S. Wang, J. Li, et al., "A survey of VNF forwarding graph embedding in B5G/6G networks," Wireless Networks, vol. 30, no. 5, pp. 3735-3758, 2024, doi: 10.1007/s11276-021-02741-9.

[17] Z. Li, J. Ding, and Z. Ma, "GTFP: Network fault prediction based on graph and time series," International Journal of Software Engineering and Knowledge Engineering, vol. 34, no. 03, pp. 489-510, 2024, doi: 10.1142/S0218194023500560.

[18] A. Majeed, A. M. Alnajim, A. Waseem, A. Khaliq, A. Naveed, S. Habib, et al., "Deep learning-based symptomizing cyber threats using adaptive 5G shared slice security approaches," Future Internet, vol. 15, no. 6, pp. 193-209, 2023, doi: 10.3390/fi15060193.

[19] K. Noor, A. L. Imoize, C. T. Li, and C. Y. Weng, "A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond," Mathematics, vol. 13, no. 7, pp. 1088-1151, 2025, doi: 10.3390/math13071088.

[20] Y. Shen, J. Zhang, S. H. Song, and K. B. Letaief, "Graph neural networks for wireless communications: From theory to practice," IEEE Transactions on Wireless Communications, vol. 22, no. 5, pp. 3554-3569, 2022, doi: 10.1109/TWC.2022.3219840.

[21] Z. Wang, J. Hu, G. Min, Z. Zhao, Z. Chang, and Z. Wang, "Spatial-temporal cellular traffic prediction for 5G and beyond: A graph neural networks-based approach," IEEE Transactions on Industrial Informatics, vol. 19, no. 4, pp. 5722-5731, 2022, doi: 10.1109/TII.2022.3182768.

[22] D. Abdelkader, H. Fouzi, K. Belkacem, and S. Ying, "Graph neural networks-based spatiotemporal prediction of photovoltaic power: a comparative study," Neural Computing and Applications, vol. 37, no. 6, pp. 4769-4795, 2025, doi: 10.1007/s00521-024-10751-9.

[23] Y. Zhu, J. Guo, H. Li, S. Liu, and Y. Li, "TSAGNN: Temporal link predict method based on two stream adaptive graph neural network," Intelligent Data Analysis, vol. 28, no. 1, pp. 77-97, 2024, doi: 10.3233/IDA-237367.