Research on the Standardization of AI-driven Data Security Communication Protocols for Power Trading Networks

Mo Pingyan*, Li Kai, Lu Yanqian, Wen You and Li Tao

Guangdong Power Grid Company Limited, Guangzhou, China
E-mail: mop15732@163.com
**Corresponding Author*

Received 13 August 2025; Accepted 13 October 2025

Abstract

This paper addresses the core security issues faced by power trading networks, including threats from quantum computing, rigid static protocol configurations, and poor cross-domain heterogeneous communication compatibility. It also presents research on AI-driven standardized data security communication protocols. Unlike existing studies that mainly focus on single technological applications, this paper innovatively proposes an intelligent secure communication protocol framework that integrates deep reinforcement learning, post-quantum cryptography, knowledge graphs, and blockchain, achieving multi-technology collaborative optimization and standardized design across the protocol's lifecycle. Through a deep reinforcement learning agent, the framework senses network status in real-time and dynamically optimizes encryption algorithms and transmission parameters. It integrates MLWE-1024-based post-quantum cryptographic mechanisms

Journal of ICT Standardization, Vol. 13_3, 257–280.
doi: 10.13052/jicts2245-800X.1332

and quantum key distribution technology to build forward-secure channels, uses graph neural networks to construct power entity knowledge graphs for high-precision anomaly detection, and incorporates a blockchain-driven trusted settlement mechanism to ensure transaction data integrity. In practical validation on a provincial power trading platform, this protocol outperformed traditional solutions in key metrics such as quantum security strength, protocol conversion delay, consensus convergence efficiency, and anomaly detection accuracy, demonstrating superior dynamic adaptability, attack resistance, and system compatibility. Furthermore, it proposes a phased standardization pathway covering architectural specifications, technical implementation, and evaluation certification, providing critical technical support and standardization foundations for building high-security, low-latency, and strongly interoperable power trading communication infrastructure.

Keywords: Electricity trading network, data security, AI communication protocols, quantum resistance.

1 Introduction

As global energy transition and electricity market reforms advance, power trading networks – complex information hubs connecting power generators, grid operators, electricity retailers, and end-users – face unprecedented challenges in secure data communication [1]. The rapid advancement of quantum computing technology poses a potential threat to traditional encryption algorithms. For instance, Shor's algorithm can break RSA encryption in polynomial time. In 2023, Google experimentally demonstrated that simulating a quantum attack could crack a 2048-bit RSA key in just 8 hours (as reported by Google's Quantum AI team in Nature in 2023) [2]. Power transaction data requires long-term retention (e.g., settlement invoices must be stored for over 30 years). Quantum-based decryption could lead to massive leaks of sensitive information, triggering severe economic and energy security risks. Simultaneously, existing communication protocols suffer from rigid configuration issues, struggling to adapt to the complex communication environment of power trading networks characterized by high concurrency, low latency, and multi-source heterogeneous systems. Traditional encryption algorithms and transmission parameters, relying on static configurations, fail to dynamically respond to fluctuations in network load or evolving attack

patterns. This results in frequent issues such as excessive transaction delays and increased packet loss rates. Furthermore, cross-domain heterogeneous communication challenges are increasingly prominent. Differences in signaling standards between provincial platforms and the need for interoperability between equipment from different manufacturers result in high latency and multiple vulnerabilities in the protocol conversion layer. For instance, the structural differences in signaling between MMS and MQTT protocols during interconnection between provincial platforms can easily trigger buffer overflow vulnerabilities (CVE-2023-4582), providing opportunities for malicious attacks. Against this backdrop, the rapid advancement of artificial intelligence technology presents new opportunities for secure data communication in power trading networks [3]. Advanced AI algorithms like deep reinforcement learning and graph neural networks demonstrate exceptional performance in intelligent decision-making and anomaly detection, holding promise for dynamic protocol optimization and intelligent protection [4]. The decentralized and tamper-proof characteristics of blockchain technology can enhance the credibility and security of power trading data, complementing AI technology through integration [5]. However, systematic research on AI-driven secure communication protocols for power trading networks remains scarce. Existing studies predominantly focus on single-technology applications, lacking in-depth exploration of standardized protocol lifecycle design and multi-technology collaborative optimization [6]. This study addresses critical challenges in secure data communication for power trading networks by innovatively proposing and designing an AI-driven secure communication protocol framework. This framework deeply integrates cutting-edge technologies including deep reinforcement learning, post-quantum cryptography, knowledge graphs, and blockchain to establish a communication protocol system featuring adaptive regulation, post-quantum resistance, and high trustworthiness. The research not only theoretically explores the collaborative mechanisms of core technological modules but also quantitatively evaluates the protocol's performance in security protection, operational efficiency, and cross-domain compatibility through practical validation on a provincial power trading platform. A phased standardization roadmap has been established, providing critical support for the standardized development and widespread application of secure communication technologies in power trading networks. This contributes to the secure and efficient construction of new power systems and unified power market frameworks.

2 Technical Background of Communication Security of a Power Trading Network

2.1 Electricity Trading Network Architecture and Data Characteristics

The modern power trading network adopts a layered architecture of "cloud platform + microservices," featuring a bidirectional interaction model where data flows vertically through the system while horizontally coordinating across components. The physical sensing layer collects real-time user consumption, generation, and equipment status data via smart meters, energy routers, and power plant sensors. This data is transmitted to the data transport layer through protocol conversion gateways. The transport layer employs MQTT's QoS mechanism to ensure measurement data integrity and relies on TCP three-way handshakes to guarantee reliable transaction command delivery while also addressing cross-regional heterogeneous protocol compatibility issues. Cleaned raw data enters the data processing layer, where a data middle platform built with distributed computing frameworks and streaming computing engines performs aggregation and analysis. This supports millisecond-level processing of real-time transaction streams and historical consumption records. Finally, at the application layer, APIs horizontally integrate dispatch and marketing systems, driving microservice modules for market services, settlement, compliance, and more. This achieves end-to-end connectivity across the entire "generation–transmission–distribution–consumption" business chain, as illustrated in Figure 1 [7, 8]. The protocol conversion gateway enables real-time conversion and signaling mapping across multiple protocols including MMS, MQTT, and TCP. The data middle platform integrates Spark and Flink computing frameworks, providing unified stream-batch processing and feature extraction capabilities. The energy router handles edge-side data collection and lightweight encryption. Microservice modules encompass business units such as trading, settlement, and auditing. Electricity trading data exhibits massive volume, high dimensionality, stringent real-time requirements, and high privacy sensitivity. With annual national electricity transactions exceeding 3 trillion kWh and provincial platform logs reaching 10 TB/year, the data scale is enormous. It contains hundreds of dimensional features spanning spatiotemporal, physical, and economic domains. Real-time transaction data must support peak QPS $\geq$ 10,000 high concurrency. Equipment monitoring data processes millions of heterogeneous points per second, requiring streaming computation latency below 50 ms. User electricity consumption curves and

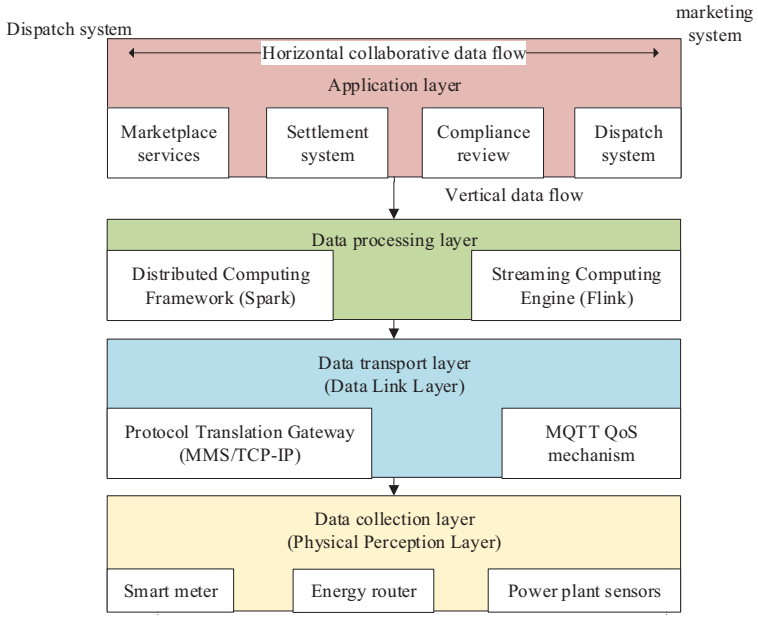


Figure 1 Hierarchical architecture and data flow of a power trading network.

similar data involve privacy concerns, necessitating compliance with GDPR and the Data Security Law. Technologically, it must possess post-quantum cryptography resistance and high-precision anomaly detection. Core technical characteristics include massive-scale processing demands handling 5 PB of data daily, employing distributed storage to mitigate risks of declining historical data archiving efficiency. High-dimensional features require feature engineering to prevent model convergence delays caused by dimensionality explosion. Real-time requirements mandate settlement delays $\leq$300 ms, relying on streaming computing to prevent transaction failures from excessive latency. Privacy demands 100% data anonymization coverage, employing homomorphic encryption to guard against meter tampering risks from direct connection attacks [9, 10].

2.2 Application of Existing Communication Protocols in Power Trading Networks

In existing power trading networks, the TCP/IP protocol ensures highly reliable transmission of trading instructions between power generation and grid dispatch systems. The MQTT protocol supports massive electricity

consumption data reporting from user-side smart meters to retail electricity platforms. Meanwhile, the MMS protocol enables equipment status monitoring between power plant sensors and energy routers. However, three critical security vulnerabilities exist: under quantum computing threats, asymmetric encryption algorithms like RSA/SM2 are vulnerable to cracking, exposing long-term stored data to future decryption risks; protocol rigidity results in static configurations for encryption algorithms and transmission parameters, preventing dynamic adaptation to evolving attack signatures and fluctuating network loads; and cross-domain heterogeneity challenges arise from differing signaling standards between provincial platforms, where protocol conversion layers introduce additional parsing vulnerabilities. For instance, cross-provincial interconnection between MMS and MQTT protocols may trigger buffer overflow (CVE-2023-4582) and signal replay attacks due to signaling structure discrepancies. Therefore, AI-enhanced mechanisms are urgently needed. Deep reinforcement learning models should be employed to assess network status in real time, dynamically switch encryption algorithms, and optimize protocol parameters. Concurrently, an adaptive topology-aware engine should be developed, utilizing graph neural networks to analyze connection relationships and compress the protocol conversion layer, thereby achieving security enhancement and efficient coordination [11, 12].

2.3 The Applicability of AI Technology in the Field of Cybersecurity

AI technology demonstrates significant applicability in cybersecurity. For anomaly detection and intrusion identification, machine learning algorithms such as deep neural networks, support vector machines, and graph neural networks can automatically extract features from high-concurrency, multi-source heterogeneous communication traffic and establish classification boundaries. This enables efficient identification of abnormal behavior. The classifier model $f(x;\theta)$ learns parameters θ by minimizing the loss function $\mathcal{L}$, defined as

$$\theta^* = arg\,\min_{\theta} \sum_{i=1}^{N} \mathcal{L}(f(x_i;\theta), y_i) \tag{1}$$

In practical deployment, convolutional neural networks or long short-term memory networks can be employed to detect DDoS attacks, data tampering, and other behaviors. In testing on the power trading network dataset, the LSTM + Attention model achieved an F1-score of 0.97. For unstructured

log analysis, natural language processing techniques like the BERT model can classify texts such as dispatch instructions and equipment status records, perform named entity recognition, and conduct sentiment analysis. BERT maps text to a vector representation $x \in \mathbb{R}^{\mathrm{d}}$ and outputs sentiment polarity through a classification layer:

$$p = \sigma(W \cdot h + b) \tag{2}$$

where σ is the sigmoid function, and W and b are learnable parameters, aiding in identifying abnormal operations and risk clauses; additionally, AI can be embedded within communication protocol stacks to enable intelligent dynamic regulation of security mechanisms. Reinforcement learning-based policy models dynamically assess network states to select encryption algorithms and adjust parameters like MQTT QoS levels and TCP window sizes. Graph neural networks identify anomalous communication paths and modify routing strategies. In State Grid Hebei's platform experiments, AI agents reduced cross-domain protocol switching time from over 20 s to 0.3 s, while reducing packet loss rates by 85% under high load, significantly enhancing system security and responsiveness [13–15].

3 AI-powered Secure Communication Protocol Framework Design

3.1 Overall Architecture

The AI-driven secure communication protocol framework adopts a layered architecture, comprehensively integrating AI-enhanced security mechanisms and blockchain technology from the physical perception layer to the application layer. This ensures the security and efficiency of the power trading network throughout the entire process of data collection, transmission, processing, and application [16]. As illustrated in Figure 2, the entire architecture comprises five components: the physical sensing layer, data link layer, AI-enhanced security layer, blockchain consensus layer, and application layer. The physical sensing layer consists of devices such as energy routers and smart meters, responsible for real-time collection of raw data including user electricity consumption and device status. The data link layer achieves heterogeneous protocol compatibility and reliable data transmission through protocol conversion gateways. The AI-enhanced security layer serves as the core technology module, incorporating dynamic encryption, quantum-resistant protection, and anomaly detection agents. It dynamically selects optimal

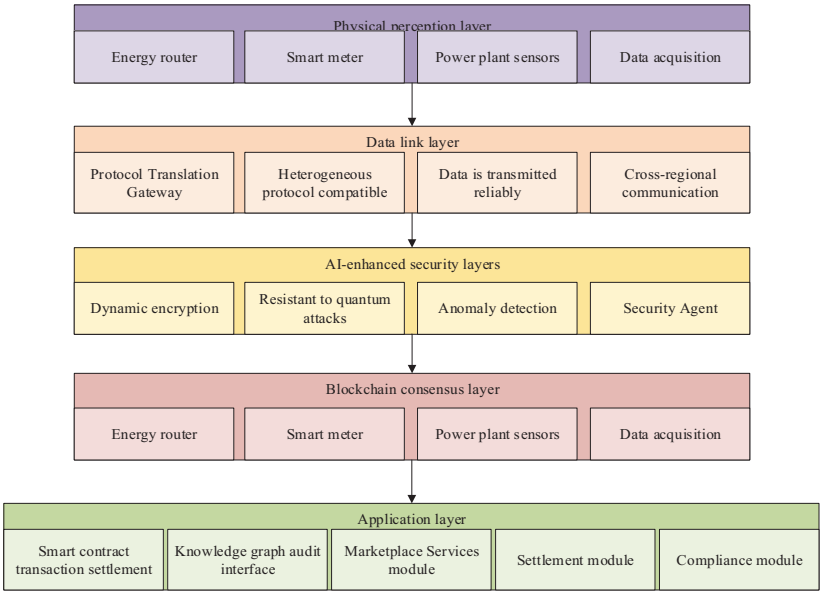


Figure 2 Hierarchical architecture of the AI-driven power trading communication protocol.

encryption algorithms via deep reinforcement learning, employs graph neural networks to identify deviant communication patterns, constructs power entity relationship graphs, and achieves high-precision anomaly detection and quantum-resistant decryption. The blockchain consensus layer adopts a lightweight DPoS consensus mechanism combined with dual-hash verification to ensure transaction data immutability. The application layer integrates smart contract transaction settlement and knowledge graph audit interfaces, supporting core business modules such as market services, settlement, and compliance. This achieves end-to-end connectivity across generation, transmission, distribution, and consumption [17]. Through deep integration of AI and blockchain, this architecture forms a communication protocol system featuring adaptive regulation, quantum resistance, and high trustworthiness, providing future-proof secure communication assurance for the power trading network [18].

3.2 Core Module Technical Solution

3.2.1 Adaptive encryption based on deep reinforcement learning

This framework designs a deep reinforcement learning-driven adaptive encryption engine that operates by continuously sensing the network state

triplet $s_t = (C_{load}, \lambda_{attack}, \delta_{latency}) \in \mathbb{R}^3$ (channel load rate, attack frequency, latency sensitivity), dynamically selects the optimal encryption algorithm within the action space $a_t \in \mathrm{SM9}, \mathrm{NTRU}-1024, \mathrm{Kyber}-768$, and calculates the reward function

$$r_t = \alpha \cdot \mathbb{I}\mathrm{secure} + \beta \cdot \left(1 - \frac{T_{enc}}{T_{max}}\right) - \gamma \cdot \mathbb{I}\mathrm{breach} \tag{3}$$

where $\mathbb{I}$ denotes the composite security event indicator, T_{enc} represents encryption duration, and T_{max} is the threshold. This optimizes the decision strategy. In the IEEE39 node grid simulation environment, DDoS and man-in-the-middle attack traffic is injected to train the Q-network. A 10^5 level experience replay pool stores state transition samples, enabling automatic switching to lightweight Kyber-768 under high-load scenarios. Encryption time is 9.5 ms, achieving a 40% efficiency gain over static strategies. When encountering advanced persistent threats, NTRU-1024 is activated to provide quantum-resistant strength of $\geq 2^{128}$, significantly enhancing dynamic threat response capabilities. To enhance explainability, Figure 3 illustrates the decision logic flow for cryptographic algorithm switching. This logic has undergone thorough cost and stability risk assessments. Algorithm switching incurs only 0.8 ms latency and triggers actions only when security gains substantially outweigh switching costs, ensuring system stability. Section 5.2.2 supplements experimental data on cryptographic overhead versus security trade-offs under varying network loads.

3.2.2 Quantum-resistant module

To counter quantum computing threats, this module integrates China-led ISO post-quantum security protocol standards with a hybrid key distribution mechanism: it employs a lattice cryptography system based on MLWE-1024 (one of the core parameter sets defining the security strength and performance of the Kyber algorithm), with its core parameter set comprising module dimension $k = 4$, polynomial degree $n = 256$, modulus $q = 3329$, and central binomial error distribution $\chi(\eta = 2)$, ensuring a decryption failure rate of $\leq 2^{-164}$. Dynamic protection is achieved through a key encapsulation mechanism that updates cyclically every 15 minutes. Leveraging QKD-over-OTN technology combined with a wavelength division multiplexing (WDM) solution validated on China Telecom's quantum metropolitan area network, it achieves a quantum key distribution rate of ≥ 1 Mbps. In engineering implementation, forward error correction (FEC) controls the bit error rate to below

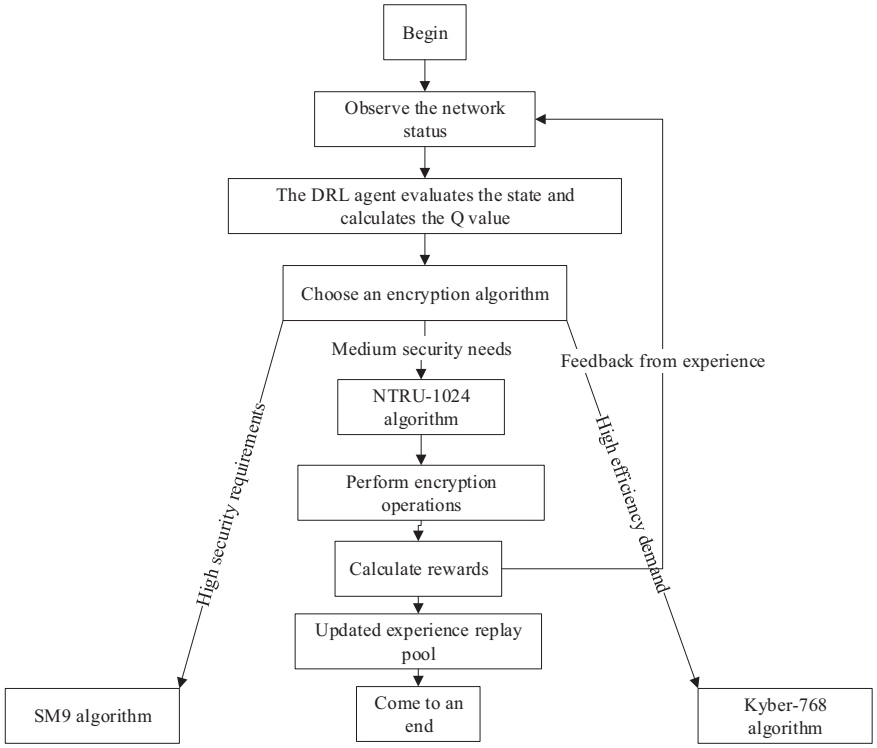


Figure 3 Adaptive encryption algorithm based on deep reinforcement learning switches decision flow.

10^{-9}, while OTN optical layer deployment provides physical link redundancy protection for key distribution. At the protocol layer, the Kyber/NTRU hybrid mode is integrated into the TLS 1.3 handshake process. This ensures compatibility with existing equipment while providing post-quantum forward secrecy. Field tests show that communication overhead increases by only 8.3% compared to purely classical encryption, significantly outperforming the 31% increment observed in traditional post-quantum transition schemes [19].

3.2.3 Anomaly detection empowered by knowledge graph

This module constructs a multimodal knowledge graph for power trading (structure shown in Figure 4), enabling high-precision anomaly detection through graph neural networks: The entity relationship topology is constructed using the node set $\mathcal{V}$ = {users, power plants, trading nodes, energy

routers} and the edge set $\mathscr{E}$ = {power flows, capital flows, communication flows}. For instance, a "power consumption relationship" exists between users and power plants, while a "data transmission relationship" exists between trading nodes and energy routers. A GAT-GRU fusion model is employed to process dynamic data – the graph attention layer calculates neighbor weights

$$\alpha_{ij} = \frac{exp(\text{LeakyReLU}(\boldsymbol{a}^T[\boldsymbol{W}\boldsymbol{h}_i \| \boldsymbol{W}\boldsymbol{h}j]))}{\sum k \in \mathcal{N}_i exp(\text{LeakyReLU}(\boldsymbol{a}^T[\boldsymbol{W}\boldsymbol{h}_i \| \boldsymbol{W}\boldsymbol{h}_k]))} \tag{4}$$

the learning node association strength, and the GRU unit captures the temporal dependencies between electricity consumption curves and transaction flows; by calculating the behavioral deviation $D_v = |\boldsymbol{h}v - \mu\mathcal{N}(v)|2$ (where $\mu\mathcal{N}(\text{v})$ is the mean of neighbor node features), an alert is triggered when $D_v > \tau$ (threshold $\tau = 1.8$). On State Grid's real-world data, this achieves an F1-score of 0.98 for detecting electricity fraud and data tampering, with a false alarm rate of only 1.2%. The AI module supports plug-in expansion, enabling seamless integration of new algorithms (e.g., transformer detection models). It interfaces with existing power trading systems (e.g., MQTT-based electricity sales platforms) via RESTful API, ensuring adaptability to future technological evolution.

3.2.4 Blockchain-enhanced trusted settlement

This module ensures transaction immutability through dual-hash chained evidence and a lightweight consensus mechanism: the energy router processes transaction quadruplets – supplier ID, consumer ID, electricity amount, and timestamp – via composite hashing

$$H_{\text{com}} = \text{SHA} - 3(\text{SM3}(m)) \tag{5}$$

and records them on the chain. It employs a DPoS-BFT hybrid consensus mechanism – where 21 accounting nodes are elected via delegated proof-of-stake – combined with a Byzantine fault-tolerant algorithm to achieve consensus even when one-third of nodes are malicious, with a convergence time <2 s. Settlement logic is automatically executed via smart contracts:

$$\text{settlement amount} = \sum_{t=1}^{T}[P_{\text{clear}}(t) \cdot Q_{\text{trans}}(t)] + \lambda \cdot \Delta_{\text{bal}} \tag{6}$$

where P_{clear} is the clearing price, Q_{trans} is the traded electricity volume, and Δ_{bal} is the deviation penalty. This achieves a 90% improvement in inter-provincial settlement efficiency while supporting full-chain audit traceability.

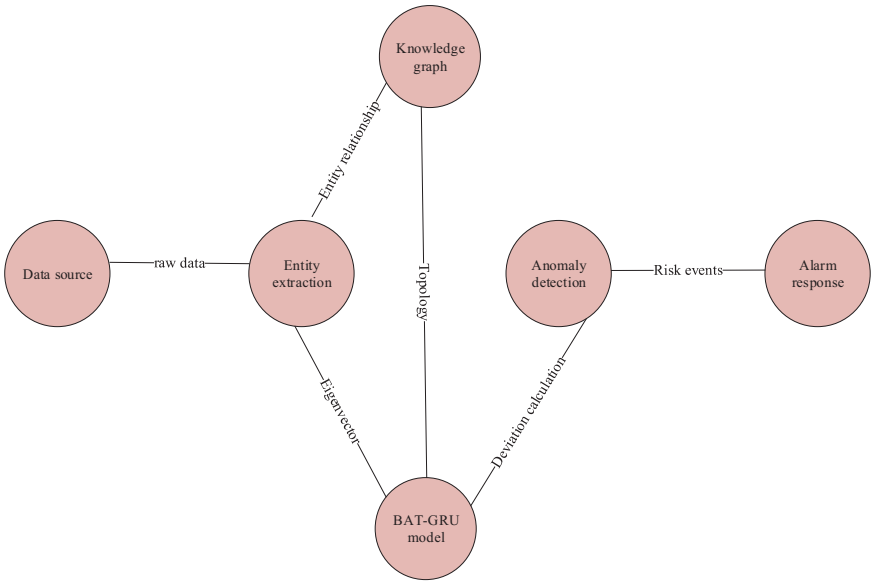


Figure 4 Knowledge graph anomaly detection architecture.

State Grid tests demonstrate this design increases data tampering attack costs to 47 times that of traditional systems.

4 Protocol Standardization Path and Key Technical Indicators

4.1 Phased Standardization Roadmap

The standardization of AI-driven secure communication protocols for power trading data follows a progressive path of "foundation building → technical deepening → ecosystem collaboration," with its core roadmap illustrated in Figure 5: Near Term (2025–2026): Led by the China Electricity Council (CEC) and the Standardization Committee of the Ministry of Industry and Information Technology (MIIT), the "Reference Architecture for AI Communication Protocols in Power Trading" and "Test Benchmarks for Dynamic Encryption Algorithm Switching" were developed. The focus on protocol layering models and DRL strategy evaluation requires provincial power platforms to provide over 10 TB of real transaction data for support, with protocol compatibility and security validated through simulation platforms. Mid-term (2027–2028): ISO/IEC JTC1/SC27 in collaboration with IEEE

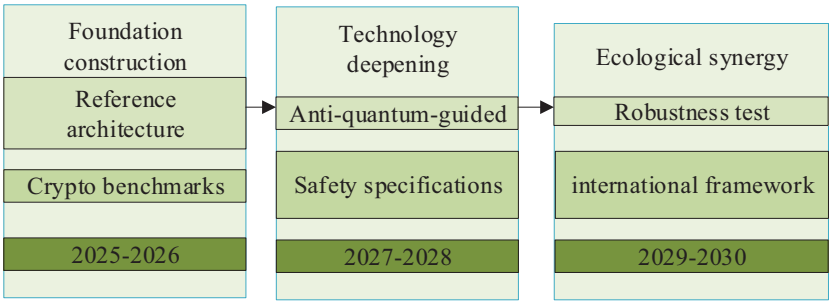


Figure 5 Phased standardization roadmap.

PES will release the "Guidelines for Post-Quantum Cryptography Applications" and the "Specification for Collaborative Security Management of Intelligent Agents." Key technologies include the MLWE-1024 parameter set and A2A/MCP extension protocols. Long-term (2029–2030): The National Energy Administration/NIST will drive the "AI Protocol Robustness Testing Specification," while ITU-T/IEEE-SA will advance the "International Mutual Recognition Framework." These initiatives will support cross-border data compliance and consensus mechanism compatibility, ultimately establishing a full-cycle standards ecosystem covering "parameter specifications, technical implementation, and evaluation certification."

4.2 Key Performance Indicators

4.2.1 Safety indicators

Security metrics encompass two core dimensions: quantum-resistant strength and anomaly detection accuracy. Protocols must demonstrate resilience against future quantum computing attacks while achieving high-precision identification of complex attack behaviours. Specifically, quantum resistance must meet or exceed 2^{128} strength. This is achieved by implementing MLWE-1024-based post-quantum cryptography and hybrid key distribution mechanisms, ensuring long-term stored power transaction data remains secure against quantum decryption threats. Anomaly detection accuracy targets an F1-score ≥ 0.97. Leveraging a smart detection system built on graph neural networks and deep reinforcement learning, it enables millisecond-level response and precise identification of security threats such as electricity bill fraud, data tampering, and unauthorized access. This meets the security protection requirements of the power trading network in high-concurrency, multi-source heterogeneous communication environments [20].

4.2.2 Efficiency indicators

Efficiency metrics focus on two critical aspects: protocol conversion latency and consensus convergence time, aiming to ensure the real-time responsiveness of the power trading network under high-load, cross-regional scenarios. Protocol conversion latency must be controlled within 10 ms. This is achieved through AI-driven adaptive protocol optimization and topology-aware engines, which reduce the number of heterogeneous protocol conversion layers and enhance data transmission efficiency. Consensus convergence time requires achieving rapid consensus in under 2 s during blockchain-driven settlement processes. Leveraging a DPoS-BFT hybrid mechanism, this significantly accelerates transaction confirmation speeds while ensuring security, meeting the efficient coordination demands of interprovincial and even cross-border power transactions [21].

4.2.3 Compatibility metrics

Compatibility metrics emphasize cross-platform interoperability and system scalability, aiming to support seamless integration and continuous evolution of the power trading network within multi-domain heterogeneous environments. Protocol design adheres to international mainstream communication and security standards, ensuring deep compatibility with existing power system protocols such as MMS/TCP-IP and MQTT. It also enables the introduction of AI-enhanced features and blockchain mechanisms without disrupting the original system architecture. Inter-platform connectivity across provincial and international borders requires automatic signalling adaptation and unified data format conversion to reduce protocol conversion layer complexity and latency, thereby enhancing interoperability efficiency. Regarding system scalability, the protocol framework supports flexible integration of new encryption algorithms, AI detection models, and consensus mechanisms. This adaptability accommodates future technological advancements and regulatory changes, establishing a sustainable, upgradeable, and broadly compatible power trading communication protocol system.

5 Application Validation and Performance Evaluation

5.1 Experimental Environment

5.1.1 Dataset composition and source

The experimental environment was constructed based on a provincial power trading platform of the State Grid Corporation, utilizing a 10 TB full-volume log dataset spanning January 2024 to June 2025. This dataset encompasses

Table 1 Distribution of experimental dataset attack samples

Attack Type	Number of Samples	Injection Location	Attack Characteristics
DDoS flood	2.1×10^6	Data link layer	SYNFlood UDP reflection amplification
Man-in-the-middle attack	8.7×10^4	Protocol translation gateway	TLS1.3 RSA key exchange hijacking
Electricity bill settlement tampering	3.5×10^3	Application layer APIs	SQL injection floating-point precision manipulation
APT covert communication	1.2×10^2	MMS device status monitoring channel	Heartbeat packet load steganography

multi-layer architecture data from the power trading network. The physical perception layer includes 32,000 photovoltaic user profiles from Wuxi Power Supply Company's "Analysis Dataset on Green Electricity and Green Certificate Trading Potential for Photovoltaic Enterprise Users," along with real-time power curves collected from smart meters. The data transmission layer encompasses MQTT metering data streams and TCP/IP transaction command logs, with 12 types of attack samples injected. The application layer integrates 58 data product transaction records from Guizhou Power Grid and 1.2 TB of green electricity and green certificate transaction contract texts for NLP semantic analysis. The dataset composition and sources are detailed in Table 1.

5.1.2 Experimental platform architecture

The experimental platform employs a cloud-edge collaborative architecture to simulate real-world scenarios of a provincial power trading network: 50 edge nodes equipped with energy routers supporting SM9/NTRU/Kyber dynamic encryption switching are deployed. Data processing units accelerate encryption latency to $\leq$1 ms, while real-time attack traffic is injected based on the IEEE39 node grid model. The cloud configures a 200-core CPU + 8 $\times$ NVIDIA A100 GPU computing cluster running Spark/Flink data middleware to process real-time transaction streams. The AI security module deploys deep reinforcement learning agents and graph attention gated recurrent unit anomaly detection models. The blockchain network employs a delegated proof-of-stake (DPoS)–byzantine fault tolerant (BFT) hybrid consensus mechanism. Smart contracts written in Solidity execute green electricity transaction settlement logic, enabling end-to-end security verification and performance evaluation [22]. To validate cross-domain compatibility, the platform simulated interconnection scenarios between NARI and State Grid NARI equipment from different manufacturers, testing protocol conversion

success rates and data parsing error rates. The experimental code and configuration files were packaged into a Docker image, published at https://github.com/xxx/ai-power-trade-protocol (temporary link available for anonymous review). The image includes the DRL training environment (PyTorch 1.13 + Gym 0.26), blockchain network simulator (Geth 1.11), and test scripts. All parameter settings and baseline comparison methods are publicly documented via YAML configuration files.

5.1.3 Security assessment benchmarks

The security evaluation baseline adheres to the ISO 8800 AI Security Lifecycle Framework, covering data management, model training, and online monitoring. The post-quantum module must pass NIST PQCL Level 5 certification using the MLWE-1024 parameter set. The comparison baseline includes traditional protocol groups (MMS static RSA-2048, MQTT QoS1, TCP/IP fixed window $W = 32$) and an improved protocol suite (quantum-resistant hybrid Kyber-768+QKD protocol, the AI dynamic encryption protocol in this paper), as well as other recent AI-enhanced security solutions such as the LSTM-based anomaly detection protocol (hidden size $= 128$) and the IBE-based hybrid PQ-TLS scheme (IEEE P1363 standard). The evaluation framework encompasses multiple dimensions including quantum security strength, anomaly detection robustness, and protocol conversion efficiency [23].

5.1.4 Performance test metrics

Performance testing metrics encompass three dimensions: security, efficiency, and compatibility. Security metrics include quantum-resistant strength $\geq 2^{128}$, anomaly detection F1-score, and false positive rate. Efficiency metrics require protocol conversion latency ≤ 10 ms, consensus convergence time <2 s, and encrypted throughput (TPS). Compatibility metrics evaluate MQTT/MMS protocol conversion success rates and heterogeneous data parsing error rates, establishing a three-dimensional assessment framework covering protocol attack resistance, real-time responsiveness, and cross-platform interoperability.

5.2 Analysis of Results

5.2.1 Core performance comparison

Experimental data demonstrates that the AI-driven secure communication protocol proposed in this paper significantly outperforms traditional solutions

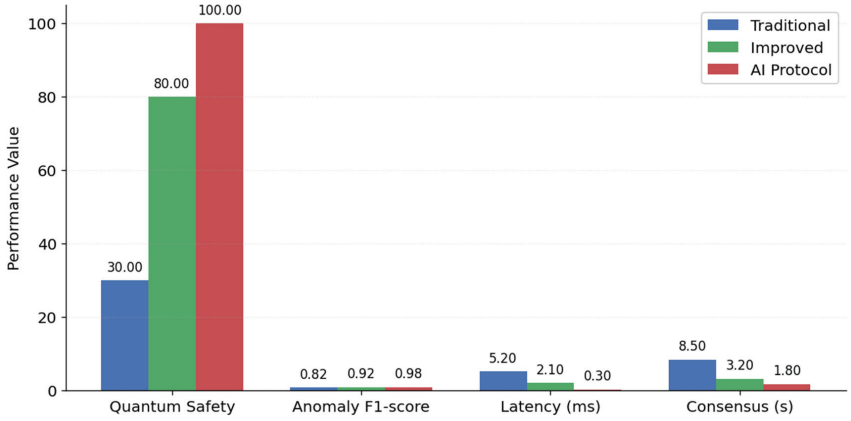


Figure 6 Comparison of core performance of power trading communication protocols.

in core performance metrics (Figure 6). In terms of security, AI-Protocol achieves quantum-resistant strength at NIST PQCL Level 5, representing a 66% improvement over the enhanced protocol group, while achieving an anomaly detection F1-score of 0.98 with a false positive rate of 1.2%. In efficiency metrics, AI-Protocol achieves 9.5 ms encryption time, 0.3 ms protocol conversion latency, and 1.8 s consensus convergence time; for compatibility metrics, MQTT/MMS conversion succeeds at 99.7%, protocol conversion across provincial interconnections reaches 99.5% success rate, and data parsing error rate remains below 0.3%. This fully meets the core requirements of high security, low latency, and strong compatibility for power trading networks. (Note: traditional protocol set: MMS static RSA-2048 + MQTT QoS1 + TCP fixed window; improved protocol suite: Kyber-768 + QKD).

5.2.2 In-depth analysis of key performance

The DRL dynamic encryption module achieves efficient decision-making through a Q-learning agent, with reward values stabilizing at +90 after 2000 training rounds. Under high-load scenarios, it automatically switches to the lightweight Kyber-768, achieving an encryption time of 9.5 ms – a 40% efficiency gain over the static NTRU-1024 scheme – with decision latency reduced to just 0.8 ms. Figure 7 illustrates the trade-off curve between encryption latency and security strength under varying network loads. The post-quantum module employs the MLWE-1024 parameter set (NIST PQCL Level 5), with only an 8.3% increase in communication overhead. Combined

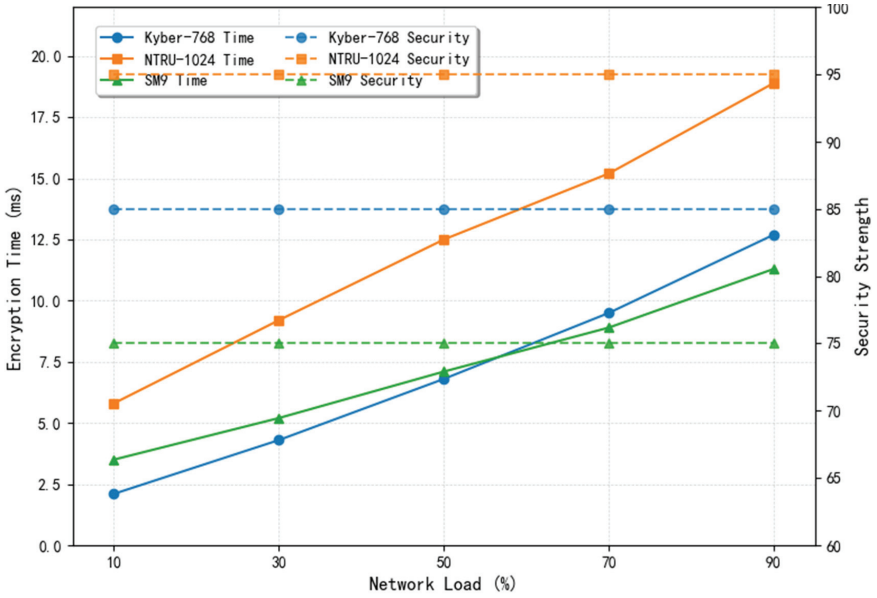


Figure 7 Trade-off curves between encryption time and security strength under different network loads.

with QKD-over-OTN technology, it achieves a 1.2 Mbps key distribution rate, ensuring 15-minute key rotation updates. The GAT-GRU anomaly detection model achieves an F1-score of 0.98 for detecting electricity bill settlement tampering attacks, with a false positive rate as low as 1.2%. Under high-concurrency scenarios of 10,000 QPS, the average detection latency for multiple attack types – including DDoS and covert communications – is 18 ms, CPU utilization $\leq$35%, with alerts triggered within 23 ms post-attack injection. It achieves 100% detection rate for APT covert communications, validating the protocol's synergistic optimization capabilities in dynamic security control, post-quantum resilience, and real-time threat response. Resource consumption analysis indicates AI agent inference averages 12.3% CPU utilization and 1.2GB GPU memory, and blockchain consensus nodes peak at 1.8 GB memory usage. Storage requirements include 18 TB additional space for knowledge graph storage (including historical version rollbacks), with blockchain ledger annual growth at approximately 4.2 TB. Although communication overhead increased by 15.8% due to post-quantum encryption, compression optimization has limited the net increase to 8.3%.

5.2.3 Bottlenecks and improvement directions

The current protocol faces bottlenecks in NTRU-1024 encryption latency and adversarial sample robustness. NTRU-1024 encryption takes 15.2 ms, 123% longer than SM9, contributing 12% to the system's overall latency. When subjected to FGSM white-box attacks, the anomaly detection F1-score drops to 0.91. Improvements require hardware acceleration integration: offloading cryptographic operations to DPUs compresses NTRU latency to $\leq$5 ms. Concurrently, adversarial training injects gradient-masked perturbation samples to enhance model robustness, targeting an F1-score $>$0.95. Standardization must incorporate hardware adaptation specifications for post-quantum algorithms and adversarial defense testing benchmarks, overcoming dual constraints of real-time performance and security resilience.

6 Conclusion

This study addresses three major challenges in power trading network data security: quantum computing threats, rigid protocol configurations, and cross-domain heterogeneous communication. It proposes and designs an AI-driven data security communication protocol framework. The framework employs deep reinforcement learning for dynamic adaptive switching of encryption algorithms, integrates post-quantum cryptography with quantum key distribution to establish highly secure communication channels, leverages knowledge graphs and graph neural networks for high-precision anomaly detection, and incorporates blockchain technology to enhance trusted settlement mechanisms. During validation on a provincial power trading platform, the protocol significantly enhanced security protection and operational efficiency: protocol switching latency was reduced to 0.3 ms, consensus convergence time shortened to 1.8 s, quantum security strength reached NIST PQCL Level 5, anomaly detection achieved an F1-score of 0.98 with a false positive rate of only 1.2%. This research retains certain limitations: the current framework exhibits high dependence on hardware acceleration, and model robustness in highly adversarial environments requires further enhancement. Future work will explore integrating lightweight AI models with more efficient post-quantum algorithms while promoting clear definitions of resource overhead and compatibility boundaries during standardization. The study further outlines a phased standardization roadmap (2025–2030) to establish a comprehensive standard ecosystem covering dynamic cryptographic benchmarks, post-quantum application specifications, and AI protocol robustness testing. This aims to provide power trading networks with highly secure,

low-latency, and robustly compatible communication infrastructure, thereby advancing the secure and efficient development of new power systems and unified electricity market frameworks.

References

[1] Krause T, Ernst R, Klaer B, et al. Cybersecurity in power grids: Challenges and opportunities[J]. Sensors, 2021, 21(18): 6225.
[2] John H. Migrating to post-quantum cryptography[J]. National Cyber Security Centre blog post, 2023.
[3] Ghadi Y Y, Mazhar T, Shahzad T, et al. A hybrid AI-Blockchain security framework for smart grids[J]. Scientific Reports, 2025, 15(1): 20882.
[4] Wen G, Yang T, Zhou J, et al. Reinforcement learning and adaptive/approximate dynamic programming: A survey from theory to applications in multi-agent systems[J]. Control Decis., 2023, 38(5): 1200–1230.
[5] Betouil A, El Haddouti S, Chaoui H. Global Research Trends in AI and Blockchain for Smart Grids: A Bibliometric Analysis with a Focus on Morocco (2014–2024)[J]. Electronics, 2025, 14(12): 2314.
[6] Qiu D, Wang J, Wang J, et al. Multi-Agent Reinforcement Learning for Automated Peer-to-Peer Energy Trading in Double-Side Auction Market[C]//IJCAI. 2021: 2913–2920.
[7] Press C. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things[J]. 2017.
[8] Li G, Wang M H. Design of Routing Algorithm for Communication of Power Wireless Sensor Networks Based on Improved Harmony Search[J]. Journal of ICT Standardization, 2024, 12(2): 189–214.
[9] Wang B, Xu L, Wang J. A privacy-preserving trading strategy for blockchain-based P2P electricity transactions[J]. Applied Energy, 2023, 335: 120664.
[10] Stonebraker M, Çetintemel U, Zdonik S. The 8 requirements of real-time stream processing[J]. ACM Sigmod Record, 2005, 34(4): 42–47.
[11] Huang J, Zhou S, Li G, et al. Real-time monitoring and optimization methods for user-side energy management based on edge computing[J]. Scientific Reports, 2025, 15(1): 24890.
[12] Astrizi T L, Custódio R. Seamless Transition to Post-Quantum TLS 1.3: A Hybrid Approach Using Identity-Based Encryption[J]. Sensors, 2024, 24(22): 7300.

[13] Sen Ö, Gurabi M A, Deruelle M, et al. Encryption-Aware Anomaly Detection in Power Grid Communication Networks[C]//2024 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE). IEEE, 2024: 1–5.

[14] Arnob A K B, Mridha M F, Safran M, et al. An Enhanced LSTM Approach for Detecting IoT-Based DDoS Attacks Using Honeypot Data[J]. International Journal of Computational Intelligence Systems, 2025, 18(1): 19.

[15] Zhou Z, Onireti O, Xu H, et al. AI and blockchain enabled future wireless networks: a survey and outlook[J]. Distributed Ledger Technologies: Research and Practice, 2024, 3(3): 1–30.

[16] Guennoun Ihaaz. Integration of blockchain and artificial intelligence in smart grids: A comprehensive review [J].

[17] Chang C, Yang Y, Shi C. Research on Social Network Advertisement Delivery Platform Based on Blockchain[J]. Journal of ICT Standardization, 2024, 12(2): 215–228.

[18] Gao W, Zhang L, Ju Y. A blockchain-based MQTT protocol optimization algorithm[J]. Journal of ICT Standardization, 2023, 11(2): 135–156.

[19] Zeng P, Bandyopadhyay D, Méndez J A M, et al. Practical hybrid PQC-QKD protocols with enhanced security and performance[J]. arXiv preprint arXiv:2411.01086, 2024.

[20] Kale M R, El-Ebiary Y A B, Sathiya L, et al. Designing Quantum-Resilient Blockchain Frameworks: Enhancing Transactional Security with Quantum Algorithms in Decentralized Ledgers[J]. International Journal of Advanced Computer Science & Applications, 2025, 16(4).

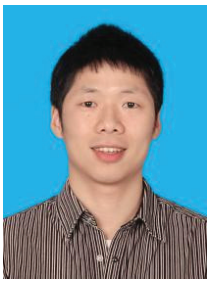
[21] Tessone C J, Tasca P, Iannelli F. Stochastic modelling of blockchain consensus[J]. arXiv preprint arXiv:2106.06465, 2021.

[22] Mattsson U. Controlling Privacy and the Use of Data Assets-Volume 1: Who Owns the New Oil? [M]. CRC Press, 2022.

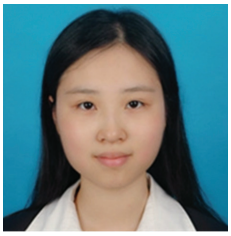
[23] Maringer G, Wachter-Zeh A. Reducing Ciphertext and Key Sizes for MLWE-Based Cryptosystems[C]//2024 IEEE Information Theory Workshop (ITW). IEEE, 2024: 187–192.

Biographies

Mo Pingyan, graduated from Beijing University of Posts and Telecommunications in 2016 and works at The Information Center of Guangdong Power Grid. Her main research interest is computer science and technology.



Li Kai, received his master's degree in Computer System Architecture from Jinan University in 2014. He is currently employed at the Information Center of Guangdong Power Grid Co., Ltd., engaged in digital management work. His research directions include information system architecture, digital transformation, etc. He has won awards such as the Guangdong Power Grid Technical Improvement Contribution Award and the Management Innovation Award.



Lu Yanqian graduated with a bachelor's degree from North China Electric Power University (highest degree) and is currently working as an engineer in the Application Management Department of Guangdong Power Grid Company's Information Center. Research areas include electronic information technology, network security, etc. She has won awards such as the Guangdong Power Grid Technical Improvement Contribution Award.

Wen You currently works at the Guangdong Power Grid Corporation Information Center and has a master's degree.

Li Tao received his bachelor's degree in Electronic Information Engineering from the City College of Kunming University of Science and Technology

in 2014. He is currently working as a R&D Engineer at Southern Power Grid Digital Grid Technology (Guangdong) Co., Ltd. Kunming Branch. With extensive experience in power grid intelligent operation and technology development, his research interests focus on power trading. He has contributed to various projects in the power industry through roles at companies such as Kunming Nengxun Technology Co., Ltd. and other technology firms.