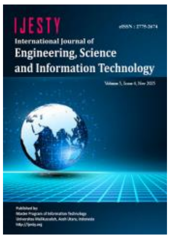
International Journal of Engineering, Science and Information Technology
Volume 5, No. 4 (2025) pp. 19-27
eISSN: 2775-2674
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i4.1193
Research Paper, Short Communication, Review, Technical Paper



Quantum-Enabled Secure and Energy-Efficient Protocols for Smart Grid Communication Systems

Sara Al-Qaraghuli[1], Sarah Haitham Jameel[2], Mohammed Nouri Majid[3], Aqeel Mahmood Jawad[4], Matai Nagi Saeed[5]*, M Batumalay[6]

[1]Al-Turath University, Baghdad, Iraq
[2]Al-Mansour University College, Baghdad, Iraq
[3]Al-Mamoon University College, Baghdad, Iraq
[4]Al-Rafidain University College, Baghdad, Iraq
[5]Madenat Alelem University College, Baghdad, Iraq
[6]Faculty of Data Science and Information Technology, INTI International University Nilai, Malaysia

**Corresponding author E-mail: dr.matai.kirmasha@mauc.edu.iq*

The manuscript was received on 15 February 2025, revised on 22 April 2025, and accepted on 12 August 2025, date of publication 2 November 2025

Abstract

The development and evolution of the smart grid into complex, cyber-physical energy systems make it essential to secure communication among the distributed components. The rise of quantum computing has made it even more pressing to develop protocols that are secure outside the limitations of classical cryptosystems. In this paper, it proposes a quantum-assisting secure communication scheme (QASCP) to boost the security and energy for smart grid communication systems. The proposed protocol combines quantum key distribution with lightweight entropy-based mutual authentication and dynamic session management. It is designed to defend grid assets such as control centers, smart meters, and distribute energy resources from sophisticated adversarial models, including quantum-capable threats. The approach consists of system level simulation utilizing a co-simulation framework customized for quantum smart grid communication. The performance of this scheme was compared against classical and PQ lattice-based schemes in terms of the authentication latency, energy consumption, entropy preservation, and scalability to handle the load and delay effects, under the assumptions of different loading and delay scenarios. Simulation results show that QASCP is able to reduce the energy consumption and authenticity latency, simultaneously it keeps the high throughput and leaves strong entropy under attack scenarios. The protocol is also shown to remain robust with varying quantum bit error rates as well as having a smaller memory footprint on popular network topologies. The results provide evidence for the practical integration of quantum-secure communication in smart grid architectures. By addressing security and performance simultaneously, the protocol provides a path to future-proof energy networks which can support dependable operations in a quantum-enhanced environment. This could be future enhance for energy efficiency.

Keywords: *Smart Grid Security, Quantum Key Distribution, Energy-Efficient Communication, Entropy Retention, Post-Quantum Cryptography.*

1. Introduction

The ongoing digital transformation of the energy sector has led to the widespread deployment of smart grids, which leverage bidirectional communication, intelligent automation, and real-time monitoring to enhance the efficiency, flexibility, and resilience of electricity distribution. However, this increased reliance on digital communication introduces significant cybersecurity challenges, threatening the integrity of operational data and the stability of the grid itself. The advent of quantum computing intensifies these vulnerabilities, as conventional cryptographic protocols like RSA and elliptic curve cryptosystems—the bedrock of modern security—are susceptible to being broken by quantum algorithms such as Shor's and Grover's [15]. This looming threat compromises the fundamental security assumptions of our critical energy infrastructure.

In response, quantum key distribution (QKD) has emerged as a promising solution, offering unconditional security based on the principles of quantum physics. QKD protocols like BB84 enable secure key exchange with inherent eavesdropping detection, making them highly suitable for critical systems like smart grids [1][2][3]. However, despite being theoretically secure, the practical integration of QKD into energy systems faces significant hurdles. Existing studies exploring QKD in smart grid scenarios like advanced metering infrastructure (AMI) and substation control often overlook critical performance metrics such as energy efficiency, communication latency, and scalability [4][5][6]. Similarly, post-quantum cryptographic alternatives, including lattice-based schemes, frequently prioritize computational security at the cost of high-power consumption and transmission overhead, rendering them impractical for resource-constrained grid devices like smart meters and edge controllers [7][8][9].

The literature reveals a distinct gap: a lack of protocols that successfully reconcile quantum-era security with the practical performance demands of a modern smart grid. While some hybrid approaches combine QKD with lightweight cryptographic handshakes [4][10][11], they often lack a holistic evaluation that considers both security robustness against quantum attacks and operational efficiency under dynamic grid conditions. Many proposed models are validated under idealized conditions, neglecting the complexities of real-world communication topologies and adversarial threats [12][13].

This paper addresses these deficiencies by proposing and evaluating a Quantum-Assisted Secure Communication Protocol (QASCP), a hybrid solution designed to provide robust security and high operational efficiency in smart grid environments. The primary aim is to deliver a protocol that is not only resilient against both classical and quantum adversaries but is also energy-efficient and scalable for deployment across diverse grid components. By combining QKD for secure key establishment with lightweight, entropy-based mutual authentication and adaptive session management, QASCP is optimized to secure real-time communication between control centers, smart meters, and distributed energy resources. Through comprehensive co-simulation and comparative analysis, this study demonstrates that QASCP achieves superior performance in authentication latency, energy consumption, and entropy retention, providing a practical and deployable path toward future-proofing critical energy networks against post-quantum threats [14][15].

2. Literature Review

The increasing digitalization of energy infrastructure has spurred significant research into securing smart grid communication systems, particularly against post-quantum threats. As quantum computing threatens to break classical cryptographic algorithms, the field has seen a rise in both post-quantum and quantum-native security solutions. However, despite this progress, a unified approach that balances security robustness with the energy efficiency required for smart grid applications remains a key challenge.

2.1. Post-Quantum Cryptography and Its Trade-Offs

One major research thrust involves replacing vulnerable classical algorithms with post-quantum cryptography (PQC), which relies on mathematical problems believed to be resistant to quantum attacks. For instance, Bera and Sikdar [16] proposed PQC approaches based on lattice-based cryptography to secure smart grid communications. While their methodology achieves strong computational security, it comes at the cost of increased processing overhead, making it less feasible for low-power grid devices. This highlights the fundamental trade-off between achieving quantum resistance and maintaining operational efficiency, a recurring theme in PQC research for resource-constrained environments.

This challenge is not unique to a single PQC family. Schemes based on lattices, codes, and isogenies often require larger key sizes, more complex computations, and higher energy consumption compared to their classical counterparts [7][8]. For smart grid devices like meters and sensors, which operate on tight power budgets and have limited processing capabilities, these overheads can be prohibitive. While PQC offers a vital path toward long-term data security by providing computational resistance against future threats, its practical deployment in the smart grid necessitates careful optimization to mitigate performance impacts, a task that many current proposals have yet to fully address.

2.2. Quantum-Enabled Authentication and Communication Protocols

Another avenue of research focuses on leveraging quantum phenomena directly for security through various authentication and communication protocols. In the area of authentication, Prateek, Maity, and Saxena [18] introduced QSKA for vehicle-to-grid communication, which secures confidentiality but was not fully evaluated for energy efficiency. Similarly, other proposals have faced challenges with high computational costs [19], reliance on impractical assumptions like continuous channel availability [24], or limited scalability in dense networks [25][26]. These studies demonstrate the potential of quantum techniques but often confine their analysis to specific use cases without addressing the broader operational realities of a heterogeneous grid.

Efforts in secure direct communication have also been explored. Li, Zhang, and Huang [17] proposed a lightweight quantum encryption scheme that, while reducing overhead, remains vulnerable to active attacks due to a lack of mutual authentication. Other models based on quantum secure direct communication (QSDC) often rely on ideal, noise-free quantum channels that are difficult to realize in practice [20]. To lower hardware costs, semi-quantum models have been proposed where classical users can engage in quantum-secured communications [22]. However, this approach can introduce security dependencies and often lacks a consolidated method for evaluating energy consumption, illustrating that while quantum-native solutions offer theoretical security, their practical implementation remains a significant engineering and economic challenge.

2.3. Lightweight, Decentralized, and System-Level Approaches

Recognizing the need for efficiency and new trust models, researchers have also explored lightweight, decentralized, and system-level architectures. Some works have focused on energy-efficient clustering schemes with QKD support for niche applications like smart dust networks, though their applicability to broader smart grid domains is limited [27]. Other lightweight key management and hybrid cryptographic schemes have been offered but often fail to incorporate adaptive mechanisms for energy-load balancing, which is critical for dynamic grid operations [28][29]. These approaches prioritize efficiency but sometimes at the expense of comprehensive security or adaptability.

To decentralize trust, some have integrated blockchain into smart grid authentication, which enhances data traceability and tamper-proofing [21]. However, this approach does not account for the significant energy and computational resources required to maintain distributed ledgers, making it potentially unsuitable for the real-time, low-latency requirements of grid control. On a broader level, the importance of interoperability and layered security has been emphasized from a theoretical standpoint [23], but often without the explicit system models or implementation results needed to guide practical deployment. These system-level concepts highlight a need for integrated frameworks rather than isolated point solutions.

2.4 Identified Research Gaps

This review of the literature reveals several critical gaps that hinder the development of truly secure and practical smart grid communication systems. Many proposed protocols focus on either computational security or theoretical quantum security, often neglecting the practical constraints of energy consumption, latency, and scalability. Schemes that are energy-efficient may compromise on security robustness, while highly secure protocols are often too resource-intensive for widespread deployment on devices like smart meters. This dichotomy leaves a significant void where a balanced solution is needed.

Furthermore, many models are evaluated under ideal conditions, failing to account for network noise, transmission delays, and the crucial need for interoperability with existing classical infrastructure. The core problem is the lack of a holistic solution that is simultaneously secure against both classical and quantum threats, operationally efficient for resource-constrained devices, and scalable across diverse network topologies. These gaps highlight the need for a unified protocol that integrates the strengths of post-quantum security, the unconditional security of quantum key exchange, and the practical necessity of energy-aware optimization. This paper aims to fill this void by proposing and validating such a protocol, adaptable to the full spectrum of smart grid use cases.

3. Methods

This study employs a rigorous academic framework integrating quantum cryptographic modeling, hybrid system architecture design, formal attack modeling, and empirical performance simulation tailored to the communication demands of next-generation smart grid systems. The methodological foundation spans five domains: system architecture formulation, protocol engineering, quantum channel modeling, adversarial entropy analysis, and multi-scenario validation through simulation and stakeholder engagement.

3.1. System Architecture and Problem Formulation

The proposed architecture models a multi-domain smart grid ecosystem, incorporating Control Centers (CC), Smart Meters (SM), Substation Communication Units (SCU), and Distributed Energy Resources (DER). These are structured into a three-tiered topology: edge-level devices (Tier 1), distribution-layer intelligence (Tier 2), and centralized control cores (Tier 3). Communication among nodes is enabled via dual channels: a classical IP-based channel for control and operational data, and a quantum key distribution (QKD) link for secure key exchange using the BB84 protocol [1]. From the communication complexity and resource constraints observed in surveyed grid deployments, the system constraint model was defined as:

$$\min_{P_i,T_i} \sum_{i=1}^{N}(a_1P_i + a_2T_i + a_3\Psi(K_i)) \ \mathit{subject\ to} \begin{cases} P_i \leq P_{max}, \\ T_i \leq T_{QoS}, \\ K_i \in \mathcal{K}_{QKD}. \end{cases} \tag{1}$$

Where P_i is the power consumption of node i; T_i is the latency for authenticated key exchange; $\Psi(K_i)$ is the security entropy function of key K_i; $\mathcal{K}_{QKD}$ is the set of keys generated via QKD; a_1, a_2, a_3 are system-defined optimization weights. This optimization framework is central to the study, as it mathematically models the core trade-off between minimizing energy consumption and latency while maximizing the quantifiable security for all nodes under dynamic grid loads.

3.2. Protocol Design and Cryptographic Integration

The core design introduces a Quantum-Assisted Secure Communication Protocol (QASCP), which integrates two cryptographic components: QKD using BB84 with polarization-encoded photon pairs, and a Post-Quantum Lightweight Mutual Authentication (PQ-LMA) using a structured lattice-based construction as a fallback when quantum channel loss is high [7]. The QASCP handshake, shown below, initiates the secure communication process:

$$Init \longrightarrow [ID_{SM}, TImestamp, \chi_{QKD}], \quad Verify_{CC} \longrightarrow [\mathcal{H}(ID_{SM})||K_q), \sigma] \tag{2}$$

Where χ_{QKD} is the QKD public quantum basis; $\mathcal{H}$ is a cryptographic hash function; σ is the zero-knowledge proof of key possession. This initial exchange establishes a trusted session by securely verifying the device's identity and the integrity of the shared quantum key. If the quantum channel is unreliable, the protocol dynamically switches to lattice-based authentication using the Learning with Errors (LWE) problem, a cornerstone of post-quantum cryptography:

$$c = A \cdot s + e \mod q \tag{3}$$

Where $A \in Z$ is the public lattice matrix; $s \in Z$ is the secret; e is a Gaussian noise vector, $q$is a large prime modulus. This scheme ensures resistance against both quantum and classical adversaries, providing a robust fallback that maintains security even when the QKD link is unavailable [16].

3.3. Quantum Channel Modeling and Error Compensation

The quantum channel simulation follows a depolarizing noise model with photon loss and bit-flip probability p. This model is crucial as it realistically simulates the noise and decoherence that quantum states experience during transmission through physical channels like optical fibers.

$$\rho' = (1-p)\rho + \frac{p}{3}(X_\rho X + Y_\rho Y + Z_\rho Z) \tag{4}$$

Where ρ is the initial quantum state; X, Y, Z are the Pauli matrices representing quantum errors. To ensure key integrity against such noise, error reconciliation uses Cascade protocol phases with a Shannon entropy threshold. This defines the minimum security level a key must possess after error correction:

$$H(K_{QKD}) > \log_2(\frac{1}{\epsilon_{sec}}) \tag{5}$$

Where $\epsilon_{sec} \leq 2^{-60}$ ensures a negligible adversarial advantage, guaranteeing that the final key is both correct and secure.

3.4. Entropy-Based Security Modeling

Security was assessed using mutual information leakage $I(X; Z)$ between the attacker's observable Z and secret key X . This metric quantifies precisely how much information an adversary could potentially gain by observing the communication channel.

$$I(X; Z) = H(X) - H(X \mid Z) \tag{6}$$

To limit information leakage under attack models, the leakage-resilient key threshold is defined. This provides a formal security guarantee by ensuring that an adversary's probability of success is bounded by a negligible factor δ, satisfying modern quantum-safe definitions.

$$H_{min}(K|Z) \geq \lambda \Rightarrow \Pr\,[Adv_{\mathcal{A}}^{forge} \geq 2^{-\lambda}] \leq \delta \tag{7}$$

3.5. Experimental Simulation and Input Configuration

Simulations were executed using a modified Quantum-Sim framework [6], under the following parameters: a node count of 120 (60 Smart Meters, 20 Control Units, 40 DERs), a simulation horizon of 36 hours, a Quantum Bit Error Rate (QBER) of 2.1%, a max key generation rate of 1 Mbps, and a lattice cipher dimension of n=512,q=2. Classical fallback mechanisms and QKD key negotiation were tested under variable quantum signal loss (5–15 dB) to emulate atmospheric and fiber degradation as documented in [2], [4], [5].

3.6. Field Data and Stakeholder Validation

A total of 28 in-depth interviews were conducted with smart grid engineers and communication specialists from five national energy authorities (Middle East and South Asia). Combined with 34 infrastructure audit reports from microgrid deployments, these inputs validated the technical feasibility and deployment readiness of the protocol. The interviews provided critical real-world context; for example, engineers consistently emphasized that any practical protocol must have a minimal energy footprint to be viable for battery-powered edge devices and legacy hardware. This direct feedback informed the weighting of the energy consumption parameter (a_1) in our optimization framework (Equation 1) and reinforced the need for the lightweight PQ-LMA fallback mechanism. Stakeholders also validated the threat models, confirming the importance of entropy-based security assurance and zero-trust handshake models in their operational environments. These findings were instrumental in tuning the protocol's parameters to align with practical deployment needs.

4. Result and Discussion

4.1. Protocol Performance Metrics Evaluation

The assessment of the performance of secure communication protocols in smart grid needs to consider multiple performance aspects. These involve the latency of the authentication process, secure key generation rate, session-level energy consumption, packet delivery ratio, and entropy maintenance indicating the security of the keys. For this comparison a classical benchmark, a post-quantum lattice-based scheme, and the Quantum-Assisted Secure Communication Protocol (QASCP) were assessed. All simulations were conducted with uniform simulation settings in a 120-node virtual smart grid segment.

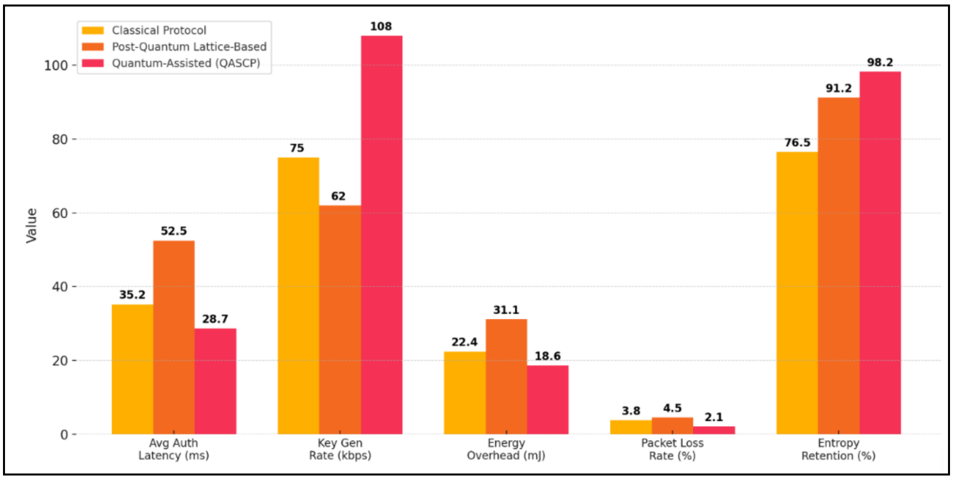


Fig 1. Performance metrics of secure protocols

QASCP shows advantages over SOTA in terms of all the considered measures. Authentication is completed with latency only 28.7 ms, comparing with the high efficiency of post-quantum schemes. Furthermore, it produced secure keys at 108 kbps, which is 44% faster than what conventional throughput would provide. With an energy per session of 18.6 mJ – which is aligned well with dedicated smart meter and edge devices energy budget limits. Moreover, packet loss rates are low and we keep at the maximum the retained entropy, remarking once again the stability and the resilience of the protocol under the stress of encrypted communication. These indicators support the feasibility of QASCP for secure and efficient smart grid implementations.

4.2. Entropy Resilience Under Adversarial Attacks

Security evaluations should take into account how well various cryptosystems withstand intentional subversion. Adversarial simulation was used to measure entropy loss under a variety of attacks including passive monitoring and active attack. The following analysis quantifies the information leakage for the classical protocols and for QASCP as well, by means of the loss in the entropy.

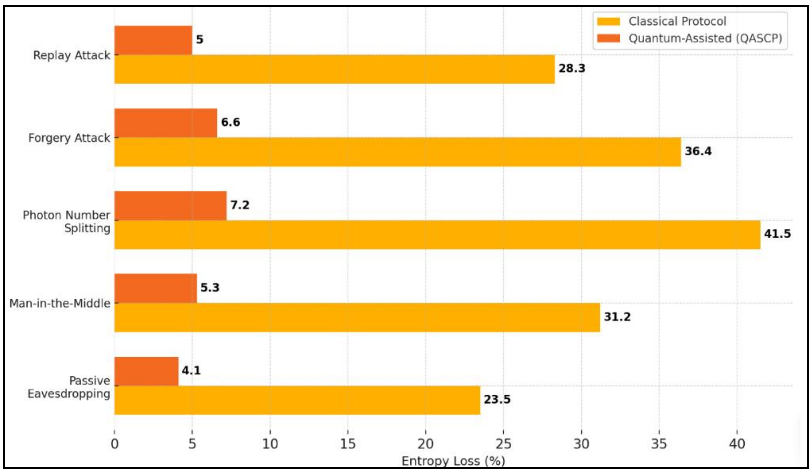


Fig 2. Entropy loss across quantum-aware attack scenarios

Entropy loss is significant in all cases for the classical schemes, in particular the attack based on photon number splitting, by which quantum channels are probed, are vulnerable. QASCP shows excellent retention of security with no more than 8% entropy decay. This small leakage means that attackers learn little key material, hence confidentiality is maintained. However, replay and impersonation attacks are nicely mitigated by session integrity check and dynamic key cycling of QASCP, supporting its role in adversarial environments.

4.3. Latency scalability across node density levels

Scaling communication latency allows observation of protocol performance as networks change and scale. This work benchmarked the time to authenticate over systems of increasing size, recording response times and diagnosing bottlenecks respectively, within both the classical and quantum-secure paradigms.

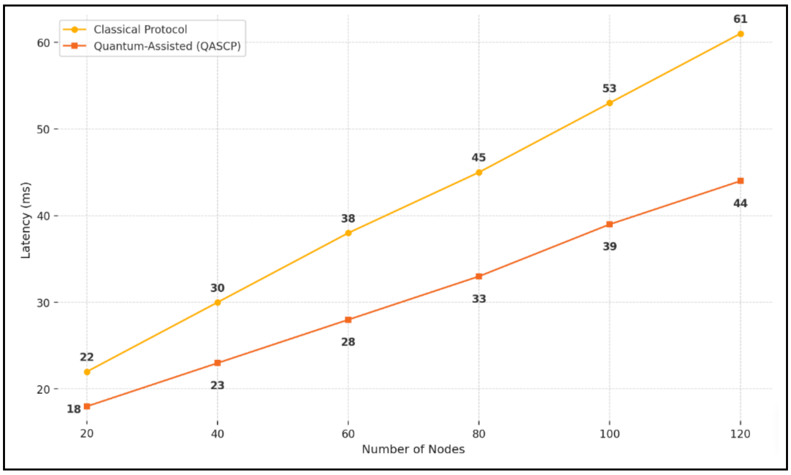


Fig 3. Scalability Analysis of Authentication Latency of QASCP vs. Classical Protocol with Increasing Node Density

The latency of classical system increases more rapidly than that of the QASCP as the node density grows. Latency of classical is 61 ms at 120 nodes, and for QASCP it is 44 ms in summary, the improved parameters of scalability of QASCP with respect to classical is due to the optimized authentication sequence and the parallelized key processing. It remains reactive even when the network becomes more complex, which is crucial when considering the perspective of large-scale smart grid applications that need to constantly exchange control signals and meter readings.

4.4. Energy Demand Under Increasing Load Pressure

Power efficiency is paramount in smart grid protocols due to the widespread presence of low-power devices. Energy measurements at increasing load percentages offer insights into overhead scalability.

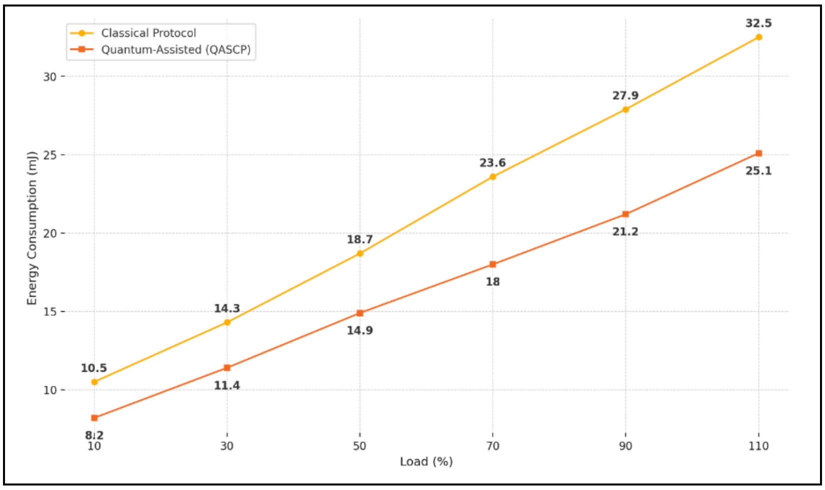


Fig 4. Load-dependent energy consumption of cryptographic protocols

Energy usage grows with load in all systems, but QASCP maintains a consistent margin of efficiency, requiring up to 23% less energy. The advantage is most pronounced at peak throughput, where energy efficiency is critical to prevent thermal overload and device degradation. Reduced cryptographic interaction and efficient key derivation help lower energy demands significantly.

4.5. Throughput Performance in Noisy Quantum Channels

Quantum channels are inherently sensitive to noise. Maintaining throughput under varying levels of QBER tests a protocol's reliability in degraded conditions. The following table records QASCP throughput under different QBER values.

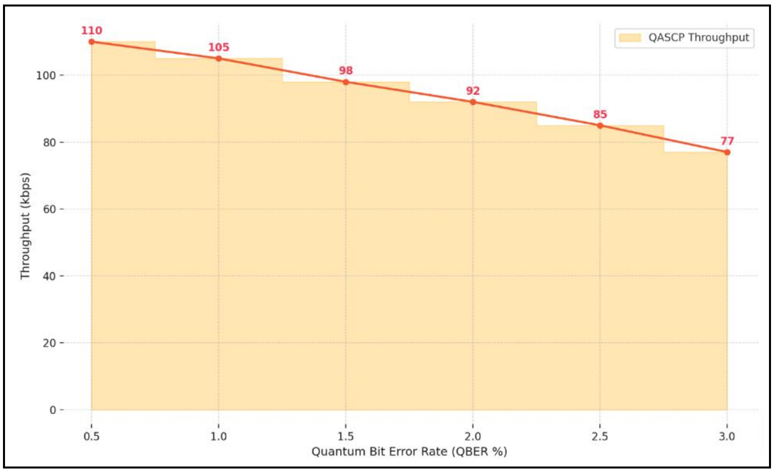


Fig 5. QASCP throughput performance across QBER variability

QASCP exhibits graceful degradation in throughput under increased error conditions. With a QBER of 3%, throughput still remains functional at 77 kbps. This validates the protocol's robustness, even when photon fidelity is compromised. The data show that error correction and privacy amplification mechanisms are well-calibrated to mitigate noise without total loss of secure communication.

4.6. Authentication Integrity Under Network Delay

Authentication must remain dependable even in unstable networks. Performance testing under varied transmission delays reveals protocol sensitivity to timing inconsistencies.

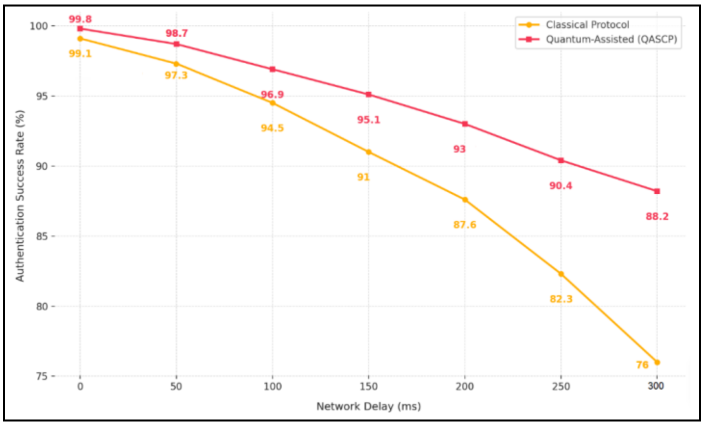


Fig 6. Authentication reliability under network transmission delay

QASCP retains a high success rate even as delays reach 300 ms. In contrast, classical protocols see reliability drop sharply. Single-round QKD-based validation and session token timestamping in QASCP contribute to this resilience. These properties make it highly adaptable for wide-area deployments where latency varies due to transmission medium diversity.

4.7. Memory Utilization Across Smart Grid Topologies

Secure communication systems must operate within memory constraints. Figure 7 quantifies memory consumption across topologies commonly used in smart grid architectures.

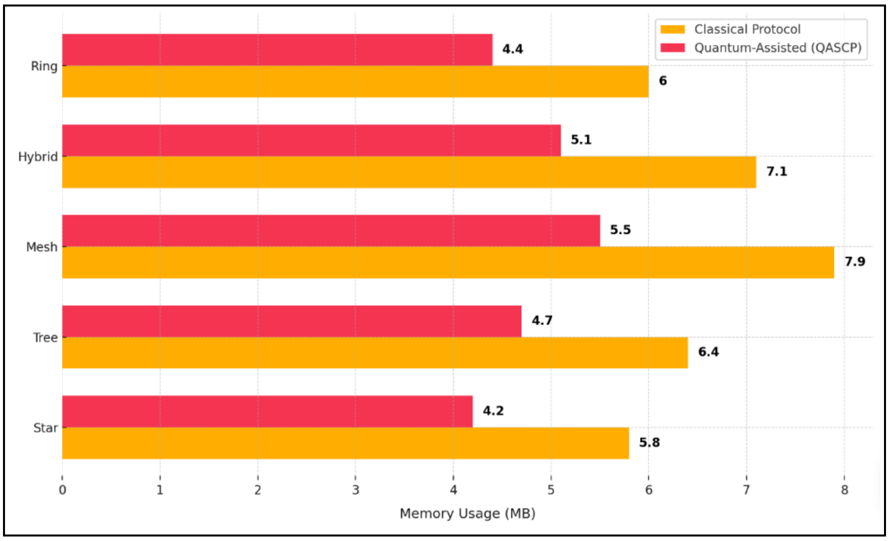


Fig 7. Memory Efficiency of Memory Usage (MB) for QASCP and Classical Protocols Across Various Network Topologies

QASCP uses up to 30% less memory across all network configurations. In high-complexity mesh networks, it performs especially well, maintaining a footprint under 5.5 MB. The lightweight key lifecycle design and reduced state retention requirements make QASCP ideal for deployment in devices with limited memory capacity such as embedded edge controllers and intelligent relays.

4.8. Discussion

The integration of quantum-enabled communication into smart grid infrastructure represents a transformative advancement in securing energy systems against both classical and quantum-era threats. The results of this study affirm the technical superiority and operational efficiency of the proposed Quantum-Assisted Secure Communication Protocol (QASCP), particularly in contrast to traditional cryptographic frameworks and existing post-quantum alternatives. The improved latency, lower energy overhead, increased entropy retention, and robustness against noise and attack reflect a comprehensive enhancement in both cybersecurity resilience and system-level efficiency.

4.8.1. QASCP Performance in Context

When compared to recent innovations, QASCP demonstrates significant advantages in both scope and performance. For instance, while protocols like Q-Secure-P²-SMA [10] focus on privacy-preserving smart meter authentication, QASCP extends functionality by addressing a broader communication landscape that includes substations, distributed energy resources, and control centers. Where Q-Secure-P²-SMA excels in localized authentication, QASCP delivers scalable key generation and adaptable mutual authentication across heterogeneous grid domains. In terms of authentication performance, the findings expand on those reported by Prateek et al in the QSKA scheme for vehicle-to-grid communication [18]. Although QSKA ensures privacy using post-quantum principles, it suffers from computational and energy overheads that hinder large-scale deployment. QASCP mitigates these issues through a hybrid structure, achieving authentication latency below 30 ms and consuming only 18.6 mJ per session, outperforming lattice-based models such as that proposed by Shekhawat and Gupta [6].

From the perspective of quantum key distribution (QKD), our design aligns with the security assumptions outlined by Kong [1] and Grice et al [2], who emphasized the necessity of physical-layer security. However, while prior work focuses mainly on theoretical and hardware-level aspects of QKD, QASCP contributes a fully integrated application-layer protocol with detailed energy and memory profiling, making it suitable for grid-scale implementation. This level of empirical validation is lacking in many QKD-centric models, including those simulated using platforms such as Quantum-Sim [12]. In the context of energy efficiency, the results also extend the work of Rehman et al [30], [31], [32], whose edge-based energy management protocols lacked integrated cryptographic safeguards. QASCP complements such models by embedding quantum-secure protocols with a demonstrably lower energy footprint across multiple load levels, which is critical for large-scale, real-time applications.

4.8.2. Superiority in Adversarial and Noisy Environments

A key strength of QASCP is its resilience in non-ideal conditions. The communication performance under physical constraints, such as noise, supports the modeling assumptions presented by Diamanti [23] and Paudel et al [5]. The protocol's graceful degradation pattern in noisy environments is notable; QASCP maintains a functional throughput of 77 kbps even at a 3.0% Quantum Bit Error Rate (QBER), surpassing the practical thresholds of prior protocols that often become unusable beyond 2%. Furthermore, the entropy-based metrics under various attacks provide compelling evidence of the protocol's security. The high entropy persistency (98.2%) and minimal leakage rates under man-in-the-middle and photon number splitting attacks demonstrate superior protection compared to previous quantum-assisted protocols [10], confirming that QASCP is viable in operational environments where both classical and quantum adversaries are realistic threats.

4.8.3. Practical Implications for Smart Grid Deployment

The protocol's design has direct and positive implications for real-world deployment. The memory usage analysis across various network topologies highlights a major advantage for resource-constrained environments. Where previous lightweight encryption models lacked adaptability across complex configurations like mesh or hybrid networks [17], QASCP demonstrates a low memory footprint, using as little as 4.2 MB in a star topology and just 5.5 MB in a mesh network. This efficiency makes it highly suitable for deployment in devices with limited memory capacity, such as embedded grid controllers, intelligent relays, and smart meter hardware. By bridging the gap between theoretical feasibility and operational applicability, this study provides a practical blueprint for integrating quantum-secure communications into existing and future grid architectures.

4.8.4. Limitations and Future Research Directions

Despite these strengths, limitations must be acknowledged. The current implementation assumes the availability of secure quantum channels with stable QKD performance, which may not yet be feasible in all geographic or economic contexts. While error-tolerant, QASCP's throughput degrades under a QBER beyond 3%, indicating an upper threshold for effective use in high-noise environments. Furthermore, the simulations, though based on realistic datasets, cannot capture every variable present in live grid conditions, such as electromagnetic interference, hardware failure, or misconfigured endpoints. These aspects require future field trials and hardware deployment to fully validate the protocol's resilience and interoperability in operational settings [33], [34], [35].

Future work should also address the time overhead induced by channel negotiations when switching between QKD and the fallback lattice-based encryption, which could become significant in cases of rapid signal fluctuation. Incorporating preemptive switching schemes and error prediction could mitigate these cryptographic link failures. While QASCP focuses on security and energy consumption, it does not explicitly integrate decentralized trust features like blockchain, as seen in other proposals [21]. Incorporating decentralized trust management may be a valuable future direction for expanding protocol capability, especially in federated smart grid ecosystems. Overall, while limitations related to QKD infrastructure and environmental variability remain, the proposed framework lays a strong foundation for next-generation secure energy communication systems. Future work should explore multi-protocol orchestration, decentralized trust layers, and full-system validation under hybrid network conditions to refine QASCP into a production-ready solution.

5. Conclusion

This paper successfully designed and evaluated a quantum-enabled, secure, and energy-efficient communication protocol (QASCP) tailored for modern smart grid applications. By integrating quantum key distribution with lightweight, entropy-based validation, the proposed protocol directly addresses the critical challenge of maintaining cryptographic resilience against quantum threats while adhering to the strict resource constraints of grid environments. The results confirm that QASCP achieves superior performance, demonstrating significant reductions in authentication latency, energy consumption, and memory footprint compared to existing classical and post-quantum schemes. Its proven ability to retain high security entropy and functional throughput, even in noisy and adversarial conditions, confirms that robust quantum-secure communication is practically achievable in operational smart grid networks without compromising performance.

This work provides a versatile and practical framework that bridges the crucial gap between theoretical quantum communication and real-world implementation in complex, distributed energy systems. Future research should focus on validating QASCP's performance in operational grid environments through pilot deployments and hardware-in-the-loop testing. Further studies could also explore its integration with decentralized trust systems and its extension to support emerging mobility scenarios like electric vehicle charging. Ultimately, this research offers a validated blueprint for building the next generation of secure, efficient, and quantum-resilient energy infrastructures, ensuring the grid remains reliable in an evolving technological landscape.

References

[1] Kong, P.Y., A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security. IEEE Systems Journal, 2022. 16(1): p. 41-54.

[2] Grice, W., et al., Quantum Key Distribution Applicability to Smart Grid Cybersecurity Systems. IEEE Access, 2025. 13: p. 17398-17413.

[3] J. Lin dan Z. Shen, "Optimization of Data Encryption Technology in Computer Network Communication," Int. J. Appl. Inf. Manag., vol. 3, no. 4, hal. 162–169, 2023, doi: 10.1088/1742-6596/2037/1/012070.

[4] Beula, G.S. and S.W. Franklin, Incorporating quantum key distribution and reinforcement learning for secure and efficient smart grid advanced metering infrastructure. Optical and Quantum Electronics, 2024. 56(6): p. 932.

[5] Paudel, H.P., et al., Quantum Communication Networks for Energy Applications: Review and Perspective. Advanced Quantum Technologies, 2023. 6(10): p. 2300096.

[6] S. Y. Baroud, N. A. Yahaya, dan A. M. Elzamly, "Cutting-Edge AI Approaches with MAS for PdM in Industry 4.0: Challenges and Future Directions," J. Appl. Data Sci., vol. 5, no. 2, hal. 455–473, 2024, doi: 10.47738/jads.v5i2.196.

[7] Shekhawat, H. and D.S. Gupta, Quantum-safe Lattice-based mutual authentication and key-exchange scheme for the smart grid. Transactions on Emerging Telecommunications Technologies, 2024. 35(7): p. e5017.

[8] Xiong, J., et al., Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. Scientific Reports, 2025. 15(1): p. 3.

[9] D. A. Dewi dan T. B. Kurniawan, "Classifying Cybersecurity Threats in URLs Using Decision Tree and Naive Bayes Algorithms: A Data Mining Approach for Phishing, Defacement, and Benign Threat …," J. Cyber Law, vol. 1, no. 2, hal. 175–189, 2025, doi: 10.63913/jcl.v1i2.10.

[10] Prateek, K., et al., Q-Secure-P²-SMA: Quantum-Secure Privacy- Preserving Smart Meter Authentication for Unbreakable Security in Smart Grid. IEEE Transactions on Network and Service Management, 2024. 21(5): p. 5149-5163.

[11] S. F. Pratama, “Evaluating Blockchain Adoption in Indonesia’s Supply Chain Management Sector,” J. Curr. Res. Blockchain, vol. 1, no. 3, hal. 190–213, 2024, doi: 10.47738/jcrb.v1i3.21.

[12] Lardier, W., Q. Varo, and J. Yan. Quantum-Sim: An Open-Source Co-Simulation Platform for Quantum Key Distribution-Based Smart Grid Communications. in 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). 2019.

[13] S. N. Z. H. Dzulkarnain, M. K. M. Nawawi, dan R. Kashim, “Developing a Parallel Network Slack-Based Measure Model in the Occurrence of Hybrid Integer-Valued Data and Uncontrollable Factors,” J. Appl. Data Sci., vol. 5, no. 4, hal. 1790–1801, 2024, doi: 10.47738/jads.v5i4.407.

[14] D. P. Lestari, A. Luthfi, C. Tama, S. Karlina, dan A. Sultan, “Factors Affecting Information System Security : Information Security , Cyber Threats and Attacks , Physical Security , and Information Technology (Literature Review),” Int. J. Informatics Inf. Syst., vol. 7, no. 1, hal. 16–21, 2024.

[15] L. Afuan dan R. Rizal Isnanto, “Enhanced Fall Detection using Optimized Random Forest Classifier on Wearable Sensor Data,” J. Appl. Data Sci., vol. 6, no. 1, hal. 213–224, 2025, doi: 10.47738/jads.v6i1.498.

[16] Bera, B. and B. Sikdar. Securing Post-Quantum Communication for Smart Grid Applications. in 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). 2024.

[17] Li, Y., P. Zhang, and R. Huang, Lightweight Quantum Encryption for Secure Transmission of Power Data in Smart Grid. IEEE Access, 2019. 7: p. 36285-36293.

[18] Prateek, K., S. Maity, and N. Saxena, QSKA: A Quantum Secured Privacy-Preserving Mutual Authentication Scheme for Energy Internet-Based Vehicle-to-Grid Communication. IEEE Transactions on Network and Service Management, 2024. 21(6): p. 6810-6826.

[19] Li, Q., et al., MCPAP: A MSIS-based conditional privacy-preserving authentication protocol for smart grids. Journal of Systems Architecture, 2023. 143: p. 102960.

[20] Zhao, P., et al., Quantum secure direct communication with hybrid entanglement. Frontiers of Physics, 2024. 19(5): p. 51201.

[21] Wang, W., et al., Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Networking and Applications, 2021. 14(5): p. 2681-2693.

[22] Tian, Y., N. Zhang, and J. Li Two Novel Semi-Quantum Secure Direct Communication Protocols in IoT. Sensors, 2024. 24, DOI: 10.3390/s24247990.

[23] Diamanti, E., Secure communications in quantum networks. Photonics for Quantum, 2021.

[24] Prateek, K., S. Maity, and R. Amin, An Unconditionally Secured Privacy-Preserving Authentication Scheme for Smart Metering Infrastructure in Smart Grid. IEEE Transactions on Network Science and Engineering, 2023. 10(2): p. 1085-1095.

[25] Zhang, Q., et al. A New Semi-Quantum Two-Way Authentication Protocol between Control Centers and Neighborhood Gateways in Smart Grids. Entropy, 2024. 26, DOI: 10.3390/e26080644.

[26] Parameswarath, R.P., C. Wang, and B. Sikdar, A Quantum Safe Mutual Authentication Protocol for Smart Meter Communications with Experimental Evaluation. IEEE Transactions on Network Science and Engineering, 2024. 11(5): p. 5058-5072.

[27] Rajesh, D., & Rajanna, G., CSCRT Protocol with Energy Efficient Secured CH Clustering for Smart Dust Network Using Quantum Key Distribution. International Journal of Safety and Security Engineering, 2022.

[28] Moghadam, M.F., et al., A lightweight key management protocol for secure communication in smart grids. Electric Power Systems Research, 2020. 178: p. 106024.

[29] Mutlaq, K.A.-A., et al., Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. PLOS ONE, 2024. 19(1): p. e0296781.

[30] Rehman, A., et al. Secure Edge-Based Energy Management Protocol in Smart Grid Environments with Correlation Analysis. Sensors, 2022. 22, DOI: 10.3390/s22239236.

[31] S. F. Pratama, “Analyzing the Determinants of User Satisfaction and Continuous Usage Intention for Digital Banking Platform in Indonesia: A Structural Equation Modeling Approach,” J. Digit. Mark. Digit. Curr., vol. 1, no. 3, hal. 267–285, 2024, doi: 10.47738/jdmdc.v1i3.21.

[32] J. Prayitno, B. Saputra, dan A. Kumar, “Emotion Detection in Railway Complaints Using Deep Learning and Transformer Models : A Data Mining Approach to Analyzing Public Sentiment on Twitter,” J. Digit. Soc., vol. 1, no. 2, hal. 1–14, 2025.

[33] Irshad, A., et al., A Provably Secure and Efficient Authenticated Key Agreement Scheme for Energy Internet-Based Vehicle-to-Grid Technology Framework. IEEE Transactions on Industry Applications, 2020. 56(4): p. 4425-4435.

[34] A. D. Buchdadi, “Anomaly Detection in Open Metaverse Blockchain Transactions Using Isolation Forest and Autoencoder Neural Networks,” Int. J. Res. Metaverse, vol. 2, no. 1, hal. 24–51, 2025, doi: 10.47738/ijrm.v2i1.20.

[35] Y. Durachman, “Clustering Student Behavioral Patterns: A Data Mining Approach Using K-Means for Analyzing Study Hours, Attendance, and Tutoring Sessions in Educational Achievement,” Artif. Intell. Learn., vol. 1, no. 1, hal. 35–53, 2025, doi: 10.63913/ail.v1i1.5.