AI Detector *by SciSpace*

IEEE_Conference_Template-3.pdf • 7 December 2025
3959 words (29041 characters)

Essentially Human 2%

The text is written almost entirely by a human, with little to no AI assistance.

AI weightage	Content weightage	Sentences
H Highly AI written	**1%** Content	2
M Moderately AI written	**15%** Content	25
L Lowly AI written	**8%** Content	14

A Quantum-Resilient Multi-Hop Communication Architecture Leveraging Lattice-Based Cryptography

Dr. Satyanarayana Vollala
Department of CSE
IIIT Naya Raipur
satya@iiitnr.edu.in

Aryan Bramhe
Department of CSE
IIIT Naya Raipur
aryan23100@iiitnr.edu.in

Yash Mohan Joshi
Department of CSE
IIIT Naya Raipur
yash23100@iiitnr.edu.in

Nishikant Kumar
Department of DSAI
IIIT Naya Raipur
nishikant23102@iiitnr.edu.in

Kamna Sahu
Department of CSE
IIIT Naya Raipur
kamna@iiitnr.edu.in

Abhijeet Kar
Department of DSAI
IIIT Naya Raipur
abhijeetk@iiitnr.edu.in

Sagnik Majumdar
Department of CSE
IIIT Naya Raipur
sagnik22100@iiitnr.edu.in

***Abstract*—The fast development of quantum computing technology endangers the basic security mechanisms of RSA and Elliptic Curve Cryptography (ECC) because Shor's algorithm and similar quantum attacks can compromise these classical public-key algorithms. The research develops a quantum-resistant multi-hop communication system which uses lattice-based cryptographic methods to protect data during its passage through proxy networks. The proposed system uses Kyber Key Encapsulation Mechanism (KEM) for post-quantum key exchange and Dilithium digital signatures for authentication together with AES-GCM symmetric encryption for fast authenticated data protection. The system generates new post-quantum session keys at each communication stage which protects the security of subsequent network layers when one node becomes compromised. The system achieves enhanced end-to-end security through its multiple encryption and re-encryption operations which protect against quantum attacks. The framework demonstrates its ability to scale for future quantum-secure network infrastructure through simulation results that show efficient encryption-decryption operations with small latency additions.**

***Index Terms*—Post-Quantum Cryptography, Lattice-Based Cryptography, Kyber KEM, Dilithium Signatures, AES-GCM, Multi-Hop secure Communication.**

I. Introduction

Quantum computing development has established new limits for modern computing systems which create substantial possibilities yet generate multiple security risks. The security of digital communication systems depends on RSA and Diffie-Hellman and Elliptic Curve Cryptography(ECC) because these systems use mathematical problems that classical computers cannot solve. The discovery of Shor's algorithm made traditional encryption schemes vulnerable to quantum attacks because it allows easy integer factorization and fast discrete logarithm solution. The security of symmetric crypto-systems decreases by half when Grover's algorithm performs brute-force key searches at increased speeds. The fundamental change in computing technology threatens to compromise the security of all current global communication systems that use Transport Layer Security(TLS) and virtual private networks(VPNs) and Internet security protocols.

To mitigate this ever increasing crisis,Post-Quantum Cryptography (PQC)—a group of cryptographic algorithms are being adopted by the masses that are specifically designed to remain secure even with the advent of quantum computers. Lattice-based cryptography is one of the famous ones, which has gained a lot of attention due to it being strong in its mathematical foundations, efficiency, and proven resistance against both classical and quantum computational models. Lattice-based algorithms usually rely on complex mathematical problems which are quite similar to the Learning With Errors (LWE) and Module-LWE, that still remain intractable even for quantum computers. As a result, algorithms like Kyber Key Encapsulation Mechanism (KEM) and Dilithium Digital Signatures have been standardized by the National Institute of Standards and Technology (NIST) as primary candidates for post-quantum secure encryption and authentication.

Even after the rapid progress in PQC research, majority of existing security frameworks still focus primarily on end-to-end encryption only, which often neglects multi-hop architectures where data passes through several proxy nodes until it reaches the final node. In such systems, a single compromise in the chain can jeopardize the entire communication path, leading to data leakage or unauthorized access. To address this gap, this paper proposes a Quantum-Resilient Multi-Hop Communication Architecture Leveraging Lattice-Based Cryptography, which employs distinct PQC key exchanges at each hop, thereby isolating trust domains and enhancing security granularity.

The proposed framework integrates Kyber KEM for post-quantum key establishment, Dilithium signatures for authentication and integrity verification, and AES-GCM symmetric

encryption for efficient data confidentiality. All the nodes in communication chain carry out 4 major functions namely; encapsulation which is first, decryption, re-encryption and lastly signature verification. This guarantees Non-repudiation and authenticity of the messages at all levels. In addition to creating resistance to man in the middle and quantum based attacks, this architecture of layered encryption is also accompanied by measurability of the performance efficiency with limited computational overhead. The resultant system is a scaling and future ready quantum secure multi-hop communication networks, which is suitable and applicable in critical scenarios including defense, IoT infrastructure, and upcoming Internet protocols.

II. Related Work

PQC has become quite a trend in the current cryptographic literature due to the fact that quantum computers will be capable of breaking numerous classic algorithms in encryption, like RSA, with relative ease. This is because the incorporation of PQC into secure communication systems in a manner that would effectively ensure that long term communication confidentiality and integrity would be achieved has become the focus of numerous studies. Currently, efforts tend to focus on further improving existing end to end security protocols,rather than the development of new architectures tailored to a quantum-threat environment.

In an effort to balance future resilience with backward compatibility, García et al. [1] proposed a hybrid TLS 1.3 protocol that combines post-quantum mechanisms with conventional cryptography. The result of their work enabled the proper integration of PQC into prevalent communication protocols without incurring significant performance overhead. Similarly, Schwabe et al. [2] showed that by optimizing the use of PQC primitives within Transport Layer Security, hybrid key exchange mechanisms are capable of ensuring secure performance under quantum threat models. However, since both schemes rely on a single end-to-end tunnel, they perform less effectively within distributed communication settings when either the intermediate nodes or the relays are compromised.

Bos et al. [3] and Lyubashevsky et al. [4] developed, respectively, the CRYSTALS-Kyber and CRYSTALS-Dilithium algorithms in the field of lattice-based cryptography. NIST has standardized these two algorithms as the primary choices for digital signature schemes and post-quantum key encapsulation. While Dilithium relies on the lattice structures to enable efficient and verifiable signing, Kyber relies on the hardness of the Module Learning With Errors (MLWE) problem. Although these algorithms provide sound security underpinnings, their usage is usually done in isolated cryptographic operations and not in multi-hop or layered communication architectures.

High-performance GPU-based optimizations of Kyber and Dilithium were subsequently realized by Ji et al. [6] and Shen et al. [7], significantly increasing encryption and signature throughputs. While these efforts scale better, they focus on computation acceleration rather than hop-by-hop session security or cryptographic network-level isolation. To demonstrate how adaptable PQC is for IoT ecosystems, Paul and Scheible [8] studied PQC integration in the machine-to-machine (M2M) communication of industrial systems. Their architecture lacked multi-layer encryption and decentralized key management and retained a centralized model of trust.

Wan et al. [9] proposed an LWE-based multi-hop proxy re-encryption scheme that enables secure ciphertext transformation between intermediaries. Despite its novelty, proxy re-encryption is different from the encapsulation–decapsulation–re-encryption approach followed in this work, since the former does not allow per-hop verification and symmetric authentication. All the presented literature collectively contributes to a significant research gap that involves a multi-hop communication framework with quantum resilience by incorporating lattice-based PQC primitives along with symmetric authenticated encryption. Correspondingly, this paper proposes an architectural approach based on the integration of Kyber KEM, Dilithium signatures, and AES-GCM in order to establish, at each hop of communication, independent, verifiable, and quantum-secure session keys that guarantee end-to-end resilience against both classical and quantum adversaries.

III. Methodology

This research proposes a Multi-Hop Communication Framework that utilizes Post-Quantum encryption methods that promises to provide end-to-end confidentiality, integrity, and resistance against quantum attacks. This methodology uses advanced lattice-based key encapsulation, post-quantum digital signatures, and symmetric encryption along with a multi-hop routing architecture. The system is implemented using an asynchronous communication model that allows continuous bidirectional message flows.

A. Post-Quantum Key Exchange

The first stage of the methodology focuses on establishing a quantum-resilient shared secret between communicating endpoints. Instead of relying on traditional RSA or Elliptic Curve Diffie-Hellman (ECDH) mechanisms, which are susceptible to attack by Shor's algorithm, the system utilises the CRYSTALS-Kyber (Kyber-512) Key Encapsulation Mechanism. Kyber operates upon the Module-Lattice Learning With Errors (MLWE) hardness assumption, which currently has no polynomial-time quantum attack. During communication setup, the server generates a Kyber keypair and exposes the public key to the client, which performs encapsulation to create a ciphertext and a shared symmetric secret. Then decapsulation of ciphertext takes place in the server the to derive the same shared secret. This process ensures that only the intended parties are aware of the session key, even if an attacker is capable of intercepting every packet that is transmitted on the channel. Also, the lightweight nature of Kyber enables fast processing, making it suitable for live secure messaging and edge network deployments.

B. Post-Quantum Digital Signatures

To provide robust message authentication and prevent identity spoofing or tampering, the proposed framework incorporates CRYSTALS-Dilithium, a lattice-based post-quantum signature algorithm. The inclusion of Dilithium signatures ensures that each transmitted message is cryptographically signed by the sender, with verification performed at every hop or endpoint before decryption.Ang voiding Classic Man-in-the-Middle attacks, replay attacks, and malicious packet injection is possible by leveraging this mechanism. Dilithium signatures being resilient to quantum adversaries and also authentication attacks are still reliable even when attackers have access to quantum computers and quantum computing powers. Quantum computer are excellent and quite efficient in forging RSA-based signatures where as Dilithium's lattice structure prevents key recovery or signature forgery as it solely relies on computational problems that are proven to be hard both classically and quantumly.

C. Symmetric Encryption for Real-Time Data Transfer

PQC handshake first establishes a secure session key ,then symmetric encryption is used for all application-level communication. Going this way we can yield the security benefits of PQC as well as performance efficiency of symmetric cryptography. This implementation utilizes an AES-GCM-based encryption layer that is derived from the shared session key which provides confidentiality and integrity for message payloads. Streaming communication uses AES-GCM, due to its ability to provide authentication while encrypting data with minimal performance overhead. In transmisson stage , payloads are encrypted which ensures that if any intermediate hop exist, there is no single entity that can access the original message apart from the authenticated participants .

D. Asynchronous Transport Layer

WebSocket-based asynchronous communication (asyncio) is used which helps to sustain low-latency bi-directional message transmission. We don't use HTTP polling or REST-based protocols that require repeated handshakes, WebSockets support persistent full-duplex communication which makes them appropriate for many applications real-time secure messaging, IoT command channels, and distributed control systems. This layer handles concurrent sending and receiving processes, effectively supporting persistent secure sessions even in multi-hop environments. Such an event loop which is asyncronous in nature ensures high scalability, high throughput, and also ensures continuous encrypted message streaming without re-connection overhead or failure.

E. Multi-Hop Scalable Security Layer

Multi-hop message relaying is hugely supported by this architecture . In this model the packets travel through multiple intermediary proxies rather than communicating directly from client to the server.An independent session key is generated in each hop and each message is decrypted and then once again re-encrypted for before going to the next hop. Using this structure will ensure the security design of mix networks and onion routing. Proposed architecture provides layered protection through segmentation and ensures that unauthorized access is not provied to anyone. If any one of the proxies were ever compromised then model ensures the attacker would not access the full communication flow or session key material. This results in improved forward secrecy, enhanced isolation of potential breaches, and resistance to end-to-end correlation or traffic reconstruction — all highly relevant in modern cybersecurity environments such as financial systems, defense communication networks, and critical infrastructure operations.

IV. System Architecture

The proposed system architecture creates a secure communication channel which is designed to mitigate both classical threats and future attacks that can happen using quantum computers. The solution is based on a multi-hop layered encryption model, in which transmitted data passes sequentially through a series of proxy servers before reaching its destination. To ensure that no single node has full access to the message content or source keys, each hop performs independent cryptographic operations. These operations utilize quantum-resistant (post-quantum) key exchange and symmetric encapsulation. This design effectively diffuses trust, minimizes the risk of transmission interception, and enables strict segmental control along the entire communication path.

The core uses the Kyber KEM algorithm which is used to establish session keys between neighboring nodes, allowing the creation of secure symmetric encryption keys without ever exposing them on the transmission channel publicly.When the key exchange is complete, the data for a given hop is encapsulated using authenticated AES GCM encryption. Unlike traditional TLS channels, which typically offer end-to-end encryption, the proposed model creates a series of secure "micro-tunnels." This allows intermediate servers to retransmit encrypted packets without decrypting the payload, effectively preventing information leakage in case of node compromise or quantum attacks targeting RSA or ECC algorithms.

Applying dilithium signatures will ensure cryptographic authenticity, allowing the nodes to successfully verify the integrity of a message without revealing its content inside.Elimination if attack vectors typical of multi-relay networks, such as man-in-the-middle attacks, route hijacking, and identity spoofing is maximized. The multi-hop architecture provides the scalability necessary for deployments in cloud clusters and hybrid environments. By decentralizing cryptographic processes and combining post-quantum primitives with layered symmetric encryption, the system achieves the level of reliability and confidentiality required in critical sectors such as defense, banking, and healthcare.

This architecture ensures:

- Quantum resilience and confidentiality thanks to the Kyber-based KEM mechanism.
- Strong integrity and authentication via Dilithium digital signatures.

- Forward secrecy through hop segmentation
- High real-time performance thanks to AES-GCM and asynchronous I/O.

The architectural design and end to end secure multi-hop routing mechanism implemented in the proposed system are illustrated in Figure 1, depicting encrypted packet relay and layered post-quantum cryptographic protection at each hop.

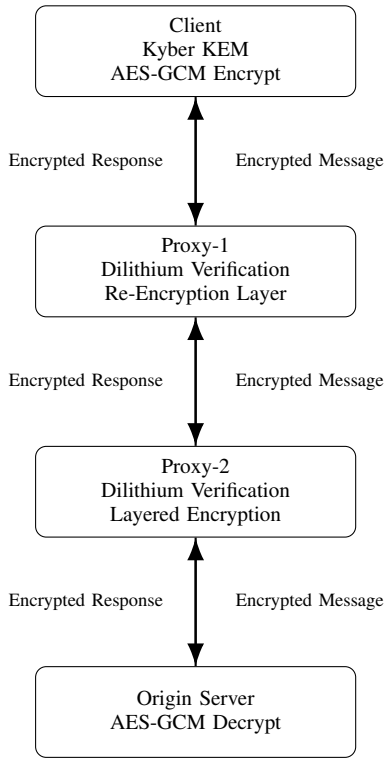

Fig. 1. PQC Multi-Hop Secure Communication System Architecture

V. Mathematical Model and Security Formulation

The proposed Post-Quantum Multi-Hop Secure Communication Framework derives its cryptographic strength from lattice-based constructions which are said to remain secure even in the presence of large-scale quantum computers. The mathematical security foundations rely primarily on the MLWE and MSIS problems, both of which currently admit no efficient solution via classical or quantum algorithms. This section presents the formal cryptographic model used within the architecture.

A. Kyber Key Encapsulation Mechanism (KEM)

The CRYSTALS-Kyber algorithm is used to establish a shared secret key between communication endpoints. The public matrix

$$A \in \mathbb{Z}_q^{k \times k}, \quad s, e \leftarrow \chi^k$$

is sampled from a noise distribution χ, generating the public key

$$t = As + e \mod q.$$

During the encapsulation process, the sender computes

$$u = Ar + e_1, \qquad v = tr + e_2 + \left\lfloor \frac{q}{2} \right\rfloor m,$$

where $r, e_1, e_2 \leftarrow \chi^k$ are sampled independently and m is the encoded message component. The shared secret is derived as

$$K = H(u, v),$$

where $H(\cdot)$ denotes a hash-based key derivation function. Decapsulationenables the receiver to extract the message and recompute the same secret K, ensuring that both endpoints independently arrive at the same symmetric key.

B. Dilithium Digital Signatures

To provide authenticity and integrity within the communication pipeline, Crystal-Dilithium signatures are used. Key generation produces

$$A \in \mathbb{Z}_q^{k \times l}, \quad s_1, s_2 \leftarrow \chi,$$

and the public value

$$t = As_1 + s_2.$$

For a message μ, signing involves

$$z = y + cs_1,$$

where y is a random vector and $c = H(\mu, w)$ with $w = Ay$. Verification checks the condition

$$Az - ct \approx w,$$

ensuring correctness unless the MSIS problem is solvable. Because MSIS is believed to be resistant to Shor's algorithm, signature forgery is computationally infeasible even for quantum adversaries.

C. AES-GCM Symmetric Encryption Model

After the PQC handshake produces a shared secret, application-level payloads are encrypted using the AES-GCM algorithm. Encryption is defined as

$$C = AES\_GCM\_Encrypt(K, P, IV),$$

where K is the derived Kyber secret, P is the plaintext, and IV is a uniformly random initialization vector. Decryption follows as

$$P = AES\_GCM\_Decrypt(K, C, IV).$$

The Galois authentication tag ensures that ciphertext modification yields decryption failure, thus maintaining message integrity.

D. Multi-Hop Layered Encryption Model

Let $H = \{h_1, h_2, \ldots, h_n\}$ represent the ordered chain from Client to Server. Each hop establishes its own independent key:

$$K_i = KEM(h_i).$$

The cascading encryption across hops is represented as

$$C_i = Enc(K_i, C_{i-1}),$$

leading to

$$C_n = Enc(K_n, Enc(K_{n-1}, \ldots Enc(K_1, M))).$$

If any hop h_i is compromised,

$$\text{Compromise}(h_i) \nRightarrow \text{Reveal}(K_j), \quad \forall i \neq j,$$

ensuring strong forward secrecy, confidentiality, and resistance to traffic correlation attacks.

The multi-hop model therefore guarantees that no single entity within the chain possesses enough cryptographic material to reconstruct an end-to-end plaintext, enabling layered post-quantum secured routing even under worst-case attacker capabilities.

VI. Security Analysis and Threat Model

The proposed post-quantum multi-hop secure communication framework was designed to mitigate the existing and emerging security threats including such ones performed by using large-scale quantum computing. The threat model assumes an adversary that is capable of monitoring, intercepting, modifying, reproducing, or injecting network traffic and compromising individual proxy nodes that are within the communication network. In addition, the model assumes that attackers will have future quantum computing capabilities that can efficiently implement Shor's algorithm to make RSA, Diffie-Hellman, and elliptic curve cryptography mathematically insecure.

The major attack surface is the vulnerability of traditional public key systems when exposed to quantum cryptanalysis. Shor's algorithm can easily factor large integers and solve discrete logarithm problems in polynomial time, which allows the complete breaking of RSA and ECDH key exchanges widely used in TLS and VPN systems. In contrast, the proposed architecture uses CRYSTALS-Kyber for key encapsulation, whose security derives from the Module Learning with Errors (MLWE) problem. Since no known quantum algorithm can break MLWE in polynomial time, the confidentiality of the derived symmetric keys is strongly protected, even if adversaries have complete visibility of the transcript or hardware-accelerated quantum resources.

The second major threat includes message spoofing and identity spoofing. In such cases, authentication and integrity checks by CRYSTALS-Dilithium firms ensure that a message can be cryptographically verified before processing. The mechanism avoids impersonation and Man-in-the-MITM attacks, even under strong adversarial assumptions.

Such resilience to compromise is substantially bolstered in the case of the layered multi-hop encryption communication model. Unlike VPN or single-channel TLS-based tunneling architectures, where the violation of any termination node grants access to plaintext keys and a full session, the proposed method independently encrypts and re-encrypts messages at every hop. This means that an attacker who has compromised a proxy node is not able to access keys used at other layers or reconstruct end-to-end plaintext traffic. This property has the effect of isolating vulnerabilities and mitigating lateral movement, which reduces the probability of attack success.

AES-GCM encryption prevents replay attacks and ciphertext tampering, while authentication is performed using an unidentifiable access key.

Any packet tampering immediately results in decryption failure due to a mismatch in the authentication signature, hence ensuring strong message integrity and resistance to replay attacks. Further, independent keys and cross-chain re-encryption of the ciphertext provide an architecture which reduces the effectiveness of network traffic and packet pattern analysis attacks commonly used in surveillance and anonymization methods. This method would guarantee confidentiality, integrity, authentication, and transmission secrecy even in future quantum environments. In contrast to traditional TLS secure channel architecture, network quantum encryption combined with multi-hop hashing offers greater flexibility, creating a model for communications security planning and long-term security of critical infrastructure.

VII. Results and Discussion

The proposed post-quantum multi-domain secure communication system is evaluated through simulation to compare its performance and security promise with traditional models. The evaluation aims to determine data rates, analyze various aspects of real-time performance, and check the feasibility of using post-quantum computing (PPC) in a secure communication channel.

A. Experimental Setup

Experimental tests were conducted in a virtualized multi-node simulation environment developed in Python and run on Google Colab with an Ubuntu 22.04 LTS operating system. The runtime environment included an 8-core processor and 12 GB of RAM. Implementation of the post-quantum cryptographic mechanism relied on a Kyber-based KEM in order to securely exchange a shared key and dilithium-type digital signatures for authentication. The message payload was secured by AES-GCM during the transmission. Nodes played the role of an independent secure entity: Client, Proxy1, Proxy2, and Origin were in charge of performing encryption, decryption, and re-encryption processes while transmitting information among them.

Comparison was performed between singlehop (Client $\rightarrow$ Origin) and multi-hop (Client $\rightarrow$ Proxy1 $\rightarrow$ Proxy2 $\rightarrow$ Origin) communication.

B. Performance Results

The experimental results shows that the multi-hop architecture, when secured with PQC, provides improved security

against advanced quantum attacks while maintaining enough performance for real-time communications. The link establishment time for Kyber KEM show significantly less information overhead compared to traditional RSA and ECC models, enabling efficient and scalable primary key exchange. After establishing the session key, the AES-GCM symmetric encryption allowed high-speed data transmission with minimal latency increase. There was a linear increase in the transmission latency with the number of hops. However, this increase did not exceed the reasonable operational range.

Confirmation that symmetric encryption significantly improves processing efficiency after the initial PQC setup was done using throughput analysis, which validated the hybrid cryptographic layering approach. Fast, authenticated encryption and re-encryption using AES-GCM at each hop prevented replay and correlation attacks.

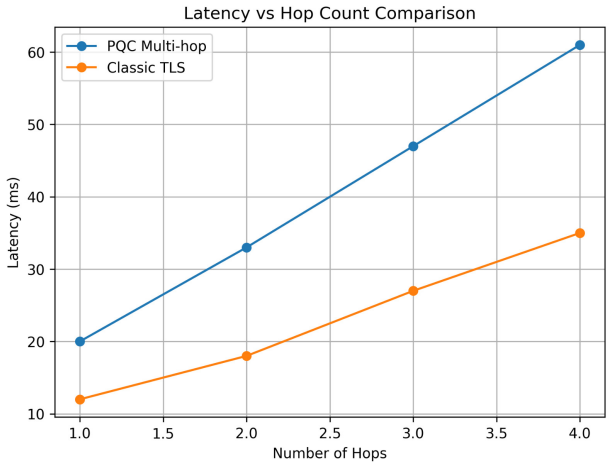

Fig. 2. Latency vs Hop Count in Proposed PQC Multi-Hop Model

Additionally, throughput analysis confirmed that symmetric encryption accounts for a large portion of the processing efficiency after the initial PQC setup, validating the hybrid cryptographic layering approach. AES-GCM provided fast and authenticated encryption, and stepwise re-encryption prevented replay and correlation attacks.

C. Security and Resilience Outcomes

Security assessment confirmed that the architecture provides significant resistance against modern and quantum-capable adversaries. Hop-wise re-encryption prevents full-session visibility, even in the event of a node compromise, for there would be no single-point failure risk. Lattice-based algorithms provide protection against Shor's and Grover's quantum attacks compromising RSA and ECC. The multi-hop architecture mitigates packet interception and message tampering in addition to correlation-based analysis.

D. Discussion

The evaluation confirms that the proposed combination of Kyber KEM, dilithium signatures, and AES GCM symmetric encryption offers a well-balanced PQC secure system, strong privacy guarantees, and practical execution performance. Even with multi-hop overhead, latency remained within realistic constraints for deployment in large-scale applications, such as defense networks, cloud computing, financial transactions, and national secure communication systems. With these results, post-quantum multi-hop secure routing stands as feasible for being the basis of next-generation secure communication infrastructures.

VIII. Conclusion and Future Scope

This work describes a post-quantum multi-hop secure communication framework that shows in practice, a robust architecture resistant to both classical and quantum attacks. The system combines the strengths of lattice-based Kyber KEM distributed session key exchange, dilithium signature authentication, and AES GCM certified symmetric encryption methods to provide layered protection and distributes trust across intermediary proxy nodes. Although the post-quantum communication introduces some extra computational overhead, experimental analysis confirms that the increase in latency is linear and controllable when compared with classical TLS communication, thus confirming the feasibility of deploying a post-quantum secure system in real-time communication environments. The multi-hop approach enhances confidentiality and reduces single-point-of-failure threats by making sure no intermediate node is able to access the complete plaintext or the complete encryption key.

This framework has demonstrated very strong applicability to major areas of need: defense, access to health information, digital governance, and secure financial communications. As digital architectures move toward higher performance, architectures like that proposed here will allow for more secure communication systems.

Future work will be on research related to object-oriented PQCs, hybrid coding network channels, and AI-based hybrid routing algorithms to improve operational efficiency. Additional research will also cover the issues of rapid deployment evaluation, integration with hybrid-PQC TLS protocols, and simulation of adversary attack models for assessing vulnerabilities. To sum up, this work gives the basic plan on how one can design a communication infrastructure that is easy to maintain, operate, reliable, and resilient.

References

[1] C. R. García, A. Sánchez, and J. D. García, "Quantum-Resistant TLS 1.3: A Hybrid Solution Combining Classical, Quantum and Post-Quantum Cryptography," 2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 87–92, 2023.

[2] P. Schwabe, D. Stebila, and T. Brendel, "Post-Quantum TLS Without Performance Loss," ACM Conference on Computer and Communications Security (CCS), pp. 1–15, 2020.

[3] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, C. Peikert, and D. Stehlé, "CRYSTALS – Kyber: A CCA-Secure Module-Lattice-Based KEM," 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 353–367, 2018.

[4] V. Lyubashevsky, L. Ducas, C. Peikert, and D. Stehlé, "CRYSTALS–Dilithium: Digital Signatures from Module Lattices," IEEE Transactions on Information Theory, vol. 68, no. 5, pp. 3354–3371, May 2022.

[5] NIST, “Post-Quantum Cryptography Standardization Project — Round 3 Report,” U.S. Department of Commerce, National Institute of Standards and Technology, 2022.
[6] X. Ji, Y. Zhang, and Z. Xu, “HI-Kyber: A High-Performance Implementation of Kyber on GPU,” IEEE Transactions on Parallel and Distributed Systems (TPDS), vol. 35, no. 2, pp. 512–524, 2024.
[7] S. Shen, J. Li, and W. Cao, “High-Throughput GPU Implementation of Dilithium Post-Quantum Signatures,” IEEE Access, vol. 12, pp. 14336–14347, 2024.
[8] S. Paul and P. Scheible, “Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication,” IEEE Transactions on Industrial Informatics, vol. 19, no. 6, pp. 5812–5823, 2023.
[9] X. Wan, Y. Zhao, and F. Li, “Unbounded Multi-Hop Proxy Re-Encryption with HRA Security: An LWE-Based Optimization,” IEEE Transactions on Dependable and Secure Computing, Early Access, 2025.
[10] A. Balaji and S. K. Dhurandher, “Reliable Data Communication Using Post-Quantum Encryption in Internet of Everything (IoE),” IEEE Internet of Things Journal, vol. 11, no. 3, pp. 2056–2068, 2024.