Post Quantum-Resistant Authentication Framework for Mobile Ad Hoc Networks Using Falcon and Dilithium Digital Signatures

Dr. M. Divya[1], S. Aishwarya[2]
[1,2]*Assistant Professor, Department of Computer Application, Hindustan College of Arts & Science, Padur, Chennai, India.*

***Abstract*—Mobile Ad Hoc Networks (MANETs) are decentralized wireless networks that enable communication among mobile nodes without relying on fixed infrastructure. Due to their dynamic topology and open communication environment, MANETs are highly vulnerable to authentication attacks, impersonation, and unauthorized access. Traditional authentication mechanisms based on RSA and Elliptic Curve Cryptography (ECC) face significant security risks with the emergence of quantum computing, which can compromise conventional public-key cryptographic systems. To address this challenge, this paper proposes a Post Quantum-Resistant Authentication Framework for MANETs using two NIST-standardized lattice-based digital signature algorithms, Falcon and Dilithium. The proposed framework integrates post-quantum digital signatures into the MANET authentication process to ensure secure node verification and trusted communication. The performance of both algorithms is evaluated using the CRAWDAD MANET dataset and NS-3 generated MANET traffic scenarios. Experiments are conducted using NS-3 Simulator, Python 3.12, NetworkX, SimPy, Open Quantum Safe (liboqs), and oqs-python libraries. Key performance metrics including Key Generation Time, Verification Time and End-to-End Delay are analyzed and compared. The results demonstrate the trade-offs between Falcon's compact signature size and fast verification capabilities and Dilithium's implementation simplicity and computational efficiency. The proposed framework enhances MANET security against future quantum threats while maintaining acceptable network performance, making it a suitable solution for next-generation secure wireless ad hoc networks.**

***Index Terms*—Mobile Ad Hoc Network (MANET), Post-Quantum Cryptography (PQC), Falcon, Dilithium, Digital Signatures, Quantum-Resistant Authentication, Network Security, Node Authentication, Lattice-Based Cryptography, Secure Routing, Quantum Computing Threats.**

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are self-configuring wireless networks composed of mobile nodes that communicate directly without relying on fixed infrastructure or centralized administration. Each node in a MANET function both as a host and as a router, enabling data packets to be forwarded through intermediate nodes to reach their destinations. Due to their flexibility, rapid deployment capability, and infrastructure-independent operation, MANETs have found applications in military communications, disaster recovery operations, emergency response systems, Internet of Things (IoT) environments, vehicular networks, and remote sensing applications [1]. As MANETs operate in an open and distributed environment, node authentication plays a crucial role in maintaining network security and trustworthiness. Authentication mechanisms ensure that only legitimate nodes participate in network communication, preventing unauthorized access, identity spoofing, and malicious activities. Reliable authentication enhances routing integrity, protects sensitive information, and establishes trust among participating nodes [2]. Despite these advantages, MANETs face significant security challenges due to their decentralized architecture, dynamic topology, limited computational resources, and absence of centralized security management. Attackers can exploit these characteristics to launch various security attacks such as impersonation attacks, Sybil attacks, blackhole attacks, wormhole attacks, and routing manipulation attacks. Therefore, robust authentication

mechanisms are essential to maintain secure and trustworthy communication within MANET environments [3].

Motivation: The emergence of quantum computing presents a substantial threat to conventional public-key cryptographic systems used in network authentication. Existing security mechanisms primarily rely on cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC), whose security is based on the computational difficulty of integer factorization and discrete logarithm problems. However, quantum algorithms, particularly Shor's algorithm, have demonstrated the theoretical capability to solve these mathematical problems efficiently, potentially compromising the security of traditional cryptographic infrastructures. As quantum computing technology continues to advance, there is an increasing need to develop authentication mechanisms that remain secure against both classical and quantum adversaries [4]. Post-Quantum Cryptography (PQC) has emerged as a promising solution by providing cryptographic algorithms based on mathematical problems believed to be resistant to quantum attacks. Among the NIST-standardized post-quantum digital signature schemes, Falcon and Dilithium have gained significant attention due to their strong security guarantees and practical deployment capabilities [5].

Problem Statement: Current authentication protocols employed in MANETs predominantly utilize traditional public-key cryptographic algorithms that are vulnerable to quantum computing attacks. As quantum technology matures, these authentication mechanisms may become ineffective, exposing MANETs to unauthorized access, identity forgery, and communication compromise. Furthermore, many existing post-quantum cryptographic solutions are designed for conventional network infrastructures and may introduce significant computational, communication, and energy overhead when applied to resource-constrained MANET environments. Therefore, there is a critical need for a lightweight, efficient, and quantum-resistant authentication framework capable of providing strong security guarantees while maintaining acceptable network performance [6]. Such a framework should support secure node authentication, minimize communication overhead, reduce verification latency, and operate effectively within the dynamic and decentralized nature of MANETs. This research addresses these challenges by proposing a Post Quantum-Resistant Authentication Framework for MANETs using Falcon and Dilithium digital signature algorithms and evaluating their performance through comprehensive simulation-based analysis.

Research Objectives: The primary objective of this research is to develop a secure and efficient post-quantum authentication framework for Mobile Ad Hoc Networks (MANETs) that can withstand emerging quantum computing threats. The proposed framework aims to integrate NIST-standardized post-quantum digital signature algorithms into the MANET authentication process to ensure secure communication among participating nodes. Specifically, the research seeks to design a quantum-resistant authentication architecture that enables secure node verification and trusted route establishment in decentralized network environments. Another important objective of this study is to conduct a comprehensive comparative analysis of two prominent post-quantum digital signature schemes, Falcon and Dilithium. Both algorithms possess unique characteristics in terms of signature size, computational complexity, implementation efficiency, and verification performance. By evaluating these algorithms under identical MANET conditions, the study aims to identify their strengths, limitations, and suitability for deployment in resource-constrained wireless ad hoc networks. Furthermore, the research aims to assess the impact of post-quantum authentication on overall network performance and security efficiency. Various performance metrics, including Key Generation Time, Verification Time, End-to-End Delay, and Energy Consumption, are analyzed to determine the effectiveness of the proposed framework. The evaluation provides insights into the trade-offs between security enhancement and network performance while ensuring resistance against future quantum attacks.

II. LITERATURE REVIEW

Mobile Ad Hoc Networks (MANETs) have attracted considerable attention due to their decentralized architecture, dynamic topology, and infrastructure-independent communication capabilities. However,

ensuring secure authentication in MANET environments remains a significant challenge because of frequent topology changes, limited resources, and vulnerability to various network attacks. Recent advancements in quantum computing have further intensified security concerns, as traditional cryptographic mechanisms may become ineffective against quantum-enabled adversaries.

Raavi et al. (2021) conducted a comparative analysis of post-quantum digital signature algorithms and highlighted the importance of evaluating security strength, computational complexity, and implementation performance of NIST finalist algorithms such as Falcon and Dilithium. Their study demonstrated that both algorithms provide strong resistance against quantum attacks while exhibiting different performance characteristics in signature generation and verification processes. With the rapid development of quantum computing technologies, researchers have increasingly emphasized the necessity of migrating from conventional cryptographic systems to post-quantum cryptographic frameworks. According to the Internet Engineering Task Force (IETF) report presented by Arora et al. (2023), current public-key cryptographic algorithms including RSA and Elliptic Curve Cryptography (ECC) are vulnerable to cryptographically relevant quantum computers, creating an urgent need for quantum-resistant authentication mechanisms [7][8].

Vidaković et al. (2023) evaluated the practical applicability of post-quantum digital signature algorithms including Dilithium, Falcon, and SPHINCS+. Their findings revealed that Falcon provides faster signature verification and smaller signature sizes, making it suitable for bandwidth-constrained environments, whereas Dilithium offers better implementation efficiency and lower computational complexity. The authors emphasized that algorithm selection should depend on the specific requirements of the target application environment. The standardization process initiated by the National Institute of Standards and Technology (NIST) has significantly accelerated research in post-quantum cryptography. NIST officially standardized CRYSTALS-Dilithium as the primary digital signature standard and selected Falcon as an additional signature scheme for specialized deployment scenarios requiring compact signatures. These standardization efforts provide a strong foundation for integrating post-quantum authentication into modern communication systems [9][10].

Cherkaoui Dekkaki et al. (2024) presented a comprehensive review of post-quantum cryptographic algorithms and discussed their deployment potential across different networking environments. The study highlighted that Dilithium is recommended as the primary NIST signature algorithm due to its implementation simplicity and strong security guarantees, while Falcon offers advantages in applications where communication overhead must be minimized [11]. Kempf et al. (2024) investigated the integration of post-quantum cryptographic algorithms into modern communication protocols and demonstrated that Falcon and Dilithium can be incorporated into secure networking infrastructures with acceptable performance overhead. Their experimental results indicated that both algorithms maintain practical handshake durations and authentication efficiency, supporting their suitability for future quantum-secure communication systems [12].

Chen (2024) explored the implementation of post-quantum digital signatures in X.509 certificate infrastructures and compared Falcon, Dilithium, and traditional cryptographic schemes. The study reported that post-quantum algorithms provide enhanced long-term security while introducing varying levels of computational and communication overhead. The findings highlighted the importance of selecting suitable post-quantum signature schemes based on deployment requirements and resource constraints [13]. García et al. (2025) focused on the formal modeling and security analysis of the Falcon digital signature scheme. Their research validated the robustness of Falcon's lattice-based design and confirmed its capability to provide secure authentication against advanced cryptographic attacks, including those originating from future quantum computers [14].

Ahmed et al. (2025) examined the readiness of widely used cryptographic libraries for post-quantum cryptography adoption. Their survey revealed increasing support for Falcon, Dilithium, and other

NIST-selected algorithms in major cryptographic frameworks, facilitating real-world deployment and integration into secure communication infrastructures. Recent studies have also investigated the applicability of post-quantum cryptography in next-generation wireless and mobile communication systems. Kudaloor and Aijaz (2026) experimentally evaluated NIST-standardized post-quantum algorithms in future 6G environments and reported that Dilithium and Falcon provide acceptable computational performance for resource-constrained wireless devices. However, the authors noted that signature size and communication overhead remain important challenges requiring optimization for bandwidth-sensitive networks [15][16].

Sakwa et al. (2026) presented a comprehensive survey of post-quantum cryptographic implementations and analyzed the practical deployment characteristics of standardized algorithms. Their study emphasized the growing importance of integrating quantum-resistant authentication mechanisms into decentralized and mobile network architectures to ensure long-term security and resilience against emerging quantum threats [17]. Although significant progress has been made in post-quantum cryptography research, limited studies have specifically addressed the integration of Falcon and Dilithium authentication mechanisms within MANET environments. Most existing works focus on standalone cryptographic performance evaluation, certificate infrastructures, or general networking applications. Therefore, a research gap exists in analyzing the impact of post-quantum digital signatures on MANET authentication performance, routing efficiency, end-to-end delay, and energy consumption. This study aims to address this gap by proposing and evaluating a Post Quantum-Resistant Authentication Framework for MANETs using Falcon and Dilithium digital signature algorithms.

III. PROPOSED FRAMEWORK

3.1 System Architecture

The proposed Post Quantum-Resistant Authentication Framework is designed to provide secure and efficient node authentication in Mobile Ad Hoc Networks (MANETs) using two NIST-standardized post-quantum digital signature algorithms, Falcon and Dilithium. The framework integrates authentication mechanisms into the MANET communication process to ensure that only legitimate nodes participate in route discovery and data transmission. By utilizing quantum-resistant digital signatures, the framework protects the network against future attacks originating from quantum computing technologies while maintaining acceptable communication and computational performance.

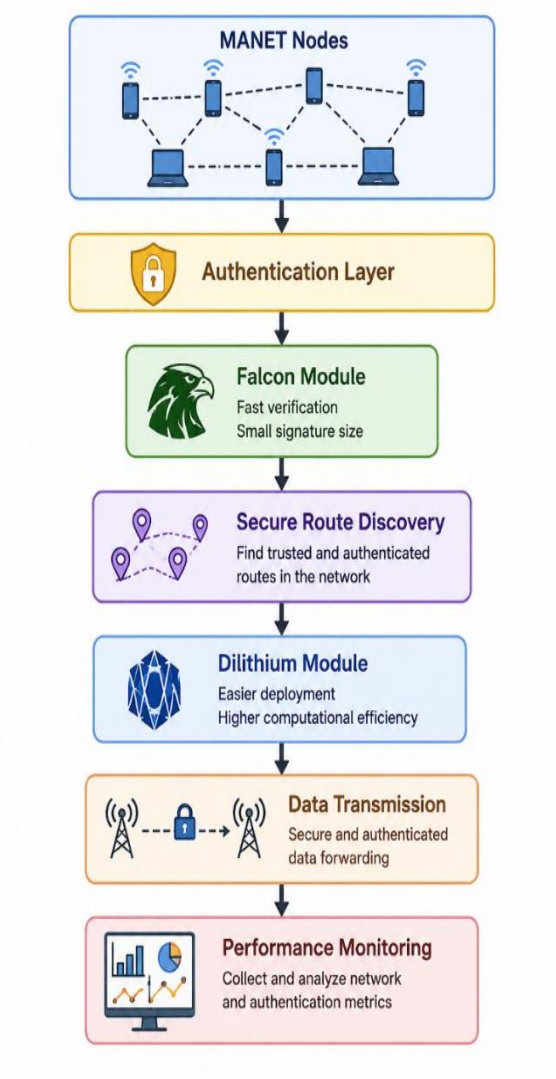

Figure 1: Proposed Architecture

The architecture consists of several functional components that operate sequentially during network communication. Initially, MANET nodes participate in the network by generating post-quantum cryptographic key pairs. The Authentication Layer serves as the primary security component responsible for validating node identities and preventing

unauthorized access. Within this layer, the Falcon Module is employed to generate and verify compact digital signatures with fast verification capabilities, reducing communication overhead during routing operations. After successful authentication, the Secure Route Discovery component identifies trusted communication paths among authenticated nodes [18][19]. Subsequently, the Dilithium Module provides an alternative authentication mechanism characterized by efficient implementation and strong security guarantees. Authenticated nodes then engage in secure data transmission, ensuring that information is exchanged only through verified routes. Finally, the Performance Monitoring component records network and authentication-related metrics for evaluation and comparative analysis. The overall architecture of the proposed framework is illustrated below. The proposed architecture combines the advantages of Falcon's compact signatures and rapid verification with Dilithium's implementation simplicity and computational efficiency, thereby establishing a robust and quantum-resistant authentication environment for MANET communications.

3.2 Framework Workflow

The proposed authentication framework follows a systematic workflow that incorporates post-quantum cryptographic operations into the MANET communication process. The workflow consists of six major stages, ensuring secure node participation, trusted route establishment, and protected data transmission.

Step 1: Node Registration

In the initial phase, each MANET node registers itself within the network by generating a public-private key pair using either the Falcon or Dilithium post-quantum digital signature algorithm. The public key is distributed to neighboring nodes, while the private key remains securely stored within the originating node. This key generation process establishes the cryptographic identity required for future authentication operations.

Step 2: Authentication Request

When a source node intends to initiate communication, it creates a routing request packet and digitally signs the packet using its private key. The generated signature serves as proof of identity and ensures the authenticity and integrity of the routing information. The signed routing request is then broadcast to neighboring nodes participating in the route discovery process.

Step 3: Signature Verification

Upon receiving the authentication request, neighboring nodes verify the attached digital signature using the sender's public key. The verification process confirms that the routing request originated from a legitimate node and that the packet contents have not been modified during transmission. Invalid signatures are immediately rejected to prevent malicious nodes from participating in the network.

Step 4: Route Establishment

After successful signature verification, authenticated nodes are allowed to participate in route discovery and forwarding operations. Trusted routes are established only through nodes that have successfully completed the authentication process. This mechanism prevents unauthorized nodes from influencing routing decisions and enhances overall network security.

Step 5: Secure Data Transmission

Once a secure route has been established, data packets are transmitted between source and destination nodes through authenticated intermediate nodes. Since all participating nodes have been verified using post-quantum digital signatures, the communication path maintains a high level of trust and security. This phase ensures secure and reliable information exchange within the MANET environment.

Step 6: Performance Collection

During and after communication, various authentication and network performance metrics are collected and stored for analysis. Key Generation Time, Verification Time, End-to-End Delay, and Energy Consumption are measured to evaluate the efficiency of the proposed framework. The collected results are subsequently used to compare the performance characteristics of Falcon and Dilithium under realistic MANET operating conditions [20].

The proposed workflow enables secure node authentication, trusted route establishment, and quantum-resistant communication while maintaining efficient network operation. By integrating Falcon and Dilithium into the authentication process, the

framework provides long-term security against both classical and quantum adversaries, making it suitable for future MANET deployments.

3.2. Falcon (Fast-Fourier Lattice-Based Compact Signatures over NTRU)

Falcon is a NIST-standardized post-quantum digital signature algorithm based on the hardness of the NTRU lattice problem. It provides quantum-resistant security with compact signatures and fast verification, making it suitable for MANET environments where bandwidth and energy efficiency are critical.

Step 1: Key Generation

The key generation phase creates a private key and a corresponding public key.

$fG-gF=q$

Where, f,g,F,G = Small lattice polynomials, q = Modulus value (typically 12289)

Public Key Generation

$h=g\cdot f^{-1}(modq)$

Random lattice polynomials are generated. The NTRU equation is satisfied. The public key h is computed. Public key is distributed to neighboring MANET nodes. Private key remains confidential.

Step 2: Message Hashing

Before signing, the message is converted into a fixed-length digest. Hash Function:

$c=H(m)$

Where, m = Original message, H = Secure hash function and c = Message digest. Hashing ensures message integrity. Any modification in the message changes the digest. The digest becomes the input for signature generation.

Step 3: Signature Generation

Falcon generates a short lattice vector signature using Fast Fourier Sampling. Signature;

$s_1+s_2h\equiv c(modq)$

Where, s_1, s_2 = Signature components, h = Public key and c = Hash value. Fast Fourier Sampling (FFS) finds a short lattice vector. Signature pair (s1, s2) is generated. Signature is attached to routing or data packets.

Step 4: Signature Verification

The receiver validates the signature using the sender's public key. Verification,

$s_1+s_2h\equiv H(m)(modq)$

Signature Norm Check

$\|s\|<\beta$

Where, $\|s\|$ = Signature norm, β = Security threshold. Receiver computes the message hash. Verification equation is evaluated. Signature norm is checked. If both conditions hold, authentication succeeds.

Falcon (Fast-Fourier Lattice-Based Compact Signatures over NTRU) is a post-quantum digital signature algorithm designed to provide secure authentication against both classical and quantum computer attacks. It is based on the mathematical hardness of the NTRU lattice problem, which is believed to remain secure even in the presence of powerful quantum computers. The operation of Falcon begins with the key generation phase, where each node creates a private key consisting of small lattice polynomials and derives a corresponding public key using NTRU lattice mathematics. The public key is shared with other nodes in the network, while the private key remains secret and is used for generating digital signatures [21].

When a source node wants to transmit a routing request or data packet in a MANET, it first computes a cryptographic hash of the message. This hash acts as a compact representation of the original message and ensures data integrity. Falcon then applies a specialized technique called Fast Fourier Sampling (FFS) to generate a short lattice vector that satisfies the required mathematical conditions. Using the private key and the message hash, the algorithm creates a compact digital signature that is attached to the packet before transmission. Due to Falcon's efficient lattice structure and Fast Fourier Transform (FFT)-based computations, the generated signatures are significantly smaller than those of many other post-quantum signature schemes.

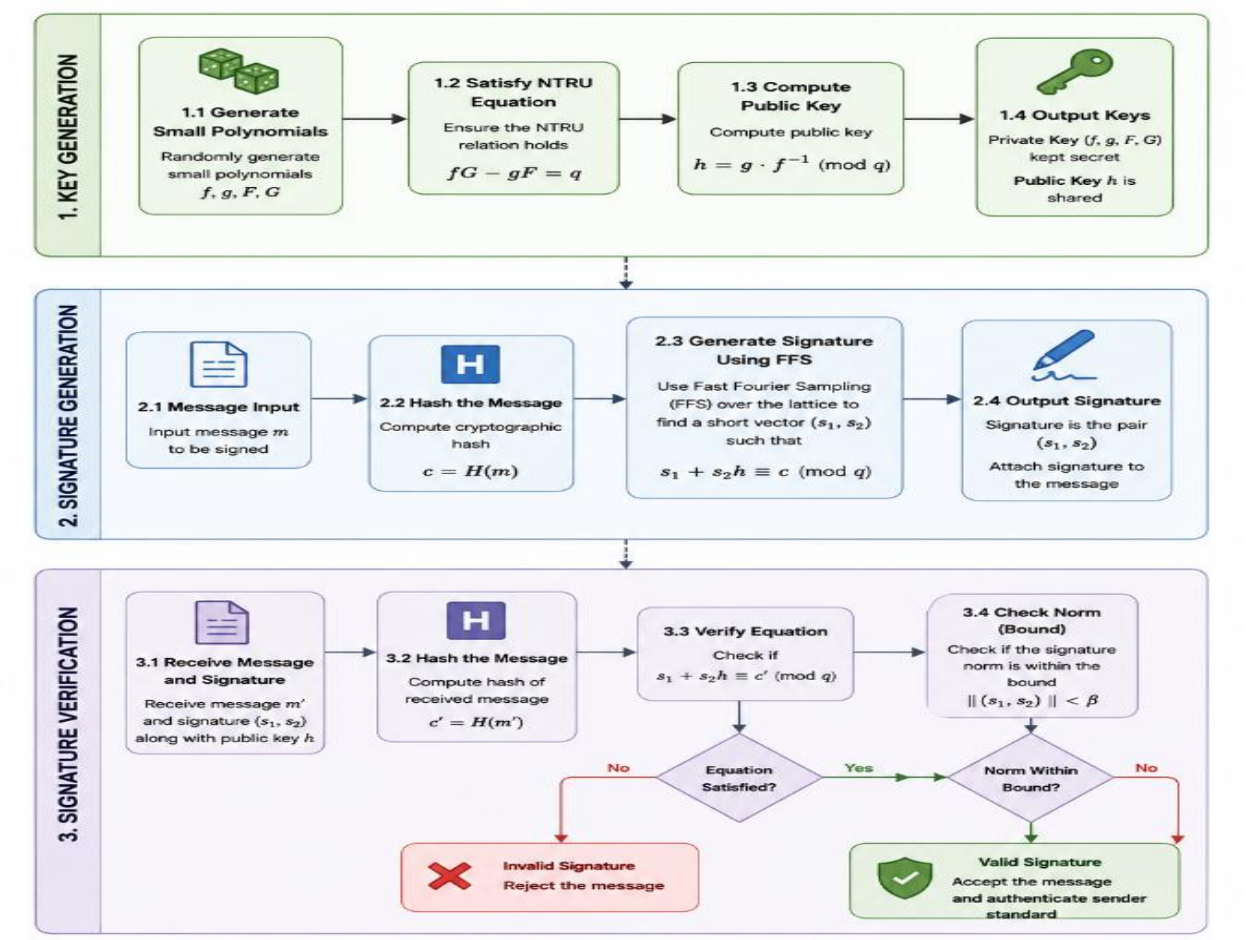

Figure 2: Workflow of Falcon

Upon receiving the packet, the destination or intermediate node performs signature verification using the sender's public key. The receiver computes the hash of the received message and checks whether the attached signature satisfies Falcon's verification equation. Additionally, the algorithm verifies that the signature lies within a predefined security bound to prevent forgery attacks. If all verification conditions are satisfied, the node is considered authentic, and the packet is accepted for further routing or processing. Otherwise, the packet is discarded as potentially malicious or modified.

The major advantage of Falcon is its compact signature size and fast verification speed, which significantly reduce communication overhead and bandwidth consumption in MANET environments. These characteristics make Falcon highly suitable for resource-constrained mobile devices where energy efficiency and network performance are critical. However, Falcon relies on sophisticated Fast Fourier Transform and lattice sampling techniques, making its implementation more complex compared to other post-quantum signature algorithms such as Dilithium. Despite this complexity, Falcon provides a strong balance between security, efficiency, and quantum resistance, making it an effective choice for secure authentication in next-generation MANETs.

3.3 Dilithium (CRYSTALS-Dilithium)

Dilithium is a NIST-standardized post-quantum digital signature algorithm based on the Module Learning with Errors (Module-LWE) and Module Short Integer Solution (Module-SIS) problems. It provides strong quantum-resistant security while offering simpler implementation and higher computational efficiency than Falcon. Unlike Falcon, Dilithium uses only integer arithmetic and avoids complex floating-point operations, making it easier to deploy in MANET environments.

Step 1: Key Generation

The key generation phase creates a private key and corresponding public key.

Public Matrix Generation

$$A \in R_q^{k \times 1}$$

Where, A = Public polynomial matrix, Rq = Polynomial ring modulo q and k,l = Matrix dimensions.

Secret Vector Generation

$s1, s2 \leftarrow \chi$

Where, s1, s2 = Secret vectors, χ = Small random distribution.

Public Key Computation

$t=As_1+s_2$

Where, A = Public matrix, s_1, s_2 = Secret vectors and t = Public key.

Random polynomial vectors are generated. Secret vectors are selected. Public key ttt is computed. Public key is distributed across MANET nodes. Secret vectors remain private.

Step 2: Message Hashing

Before signing, the message is converted into a secure digest.

Hash Function

$\mu=H(pk\|m)$

Where, pk = Public key, m = Message, H = Cryptographic hash function and μ = Message digest. Public key and message are hashed together. Produces a unique digest. Protects message integrity.

Step 3: Random Vector Selection

A temporary random vector is generated for signing.

Random Sampling

$y \leftarrow \gamma_1$

Where, y = Random polynomial vector and γ_1 = Sampling range. Random vector introduces unpredictability. Helps generate secure signatures.

Step 4: Intermediate Computation

The signer computes an intermediate value.

Matrix Multiplication

$w=Ay$

Where, A = Public matrix, y = Random vector and w = Intermediate value. Intermediate value used in challenge creation. Forms the basis for signature generation.

Step 5: Challenge Generation

A challenge value is created from the message digest and intermediate value.

Challenge Computation

$c=H(\mu,w)$

Where, μ = Message digest, w = Intermediate value and c = Challenge. Challenge binds signature to message. Prevents forgery attacks.

Step 6: Signature Generation

The final signature vector is calculated.

Signature Vector

$z=y+c \cdot s_1$

Where, z = Signature vector, y = Random vector, c = Challenge, s_1 = Secret vector

Final Signature

$\sigma=(z,c)$

Signature consists of vector z and challenge c. Signature is attached to routing packets. Used for node authentication.

Step 7: Signature Verification

The receiver verifies the received signature. Verification Computation;

$w'=Az-c \cdot t$

Where, A = Public matrix, z = Signature vector, c = Challenge and t = Public key.

Recalculate Challenge

$c'=H(\mu,w')$

Verification Condition

$c'=c$

Receiver computes w′. Challenge is regenerated. Authentication succeeds if c′=c.Otherwise, the signature is rejected.

Dilithium is a lattice-based post-quantum digital signature algorithm designed to provide strong security against both classical and quantum computer attacks. It is based on the mathematical hardness of the Module Learning with Errors (Module-LWE) and Module Short Integer Solution (Module-SIS) problems, which are believed to remain secure even in the presence of powerful quantum computers. Dilithium was selected by the National Institute of Standards and Technology (NIST) as a primary post-quantum digital signature standard because of its strong security guarantees, efficient implementation, and ease of deployment. Unlike Falcon, Dilithium relies entirely on integer arithmetic operations, eliminating the need for complex floating-point computations and making software implementation simpler and more reliable [22].

The operation of Dilithium begins with the key generation phase. During this process, each MANET node generates secret polynomial vectors and a public matrix. Using these values, a public key is computed through polynomial matrix operations while the secret vectors are retained as the private key. The public key is then distributed to neighboring nodes, allowing them to verify future signatures. This key pair establishes the cryptographic identity of each node participating in the network.

When a node intends to send a routing request or data packet, the message is first processed through a cryptographic hash function to produce a unique message digest. Dilithium then generates a random polynomial vector and computes an intermediate value using the public matrix. From this intermediate value and the message digest, a challenge value is created. The algorithm combines the challenge with the private key components to generate a digital signature consisting of a signature vector and challenge information. This signature is attached to the packet before transmission, ensuring that the message originates from an authenticated source and has not been modified during transit.

Upon receiving the signed packet, the destination or intermediate node performs signature verification using the sender's public key. The receiver recalculates the intermediate value and challenge from the received message and signature. If the newly computed challenge matches the challenge included in the signature, the message is considered authentic and valid. Otherwise, the packet is rejected as potentially forged or altered. This verification process allows MANET nodes to establish trust and prevent unauthorized devices from participating in network communications.

One of the major strengths of Dilithium is its efficient implementation and computational performance. Since it uses only integer arithmetic operations, it can be integrated into software and hardware platforms more easily than algorithms requiring complex floating-point calculations. Dilithium also offers robust security properties and fast execution, making it suitable for large-scale deployments and real-time authentication systems. However, compared to Falcon, Dilithium produces larger digital signatures, which may increase communication overhead and bandwidth consumption in resource-constrained MANET environments. Despite this limitation, its simplicity, strong security, and practical deployment characteristics make Dilithium one of the most promising post-quantum digital signature algorithms for securing future MANET communications.

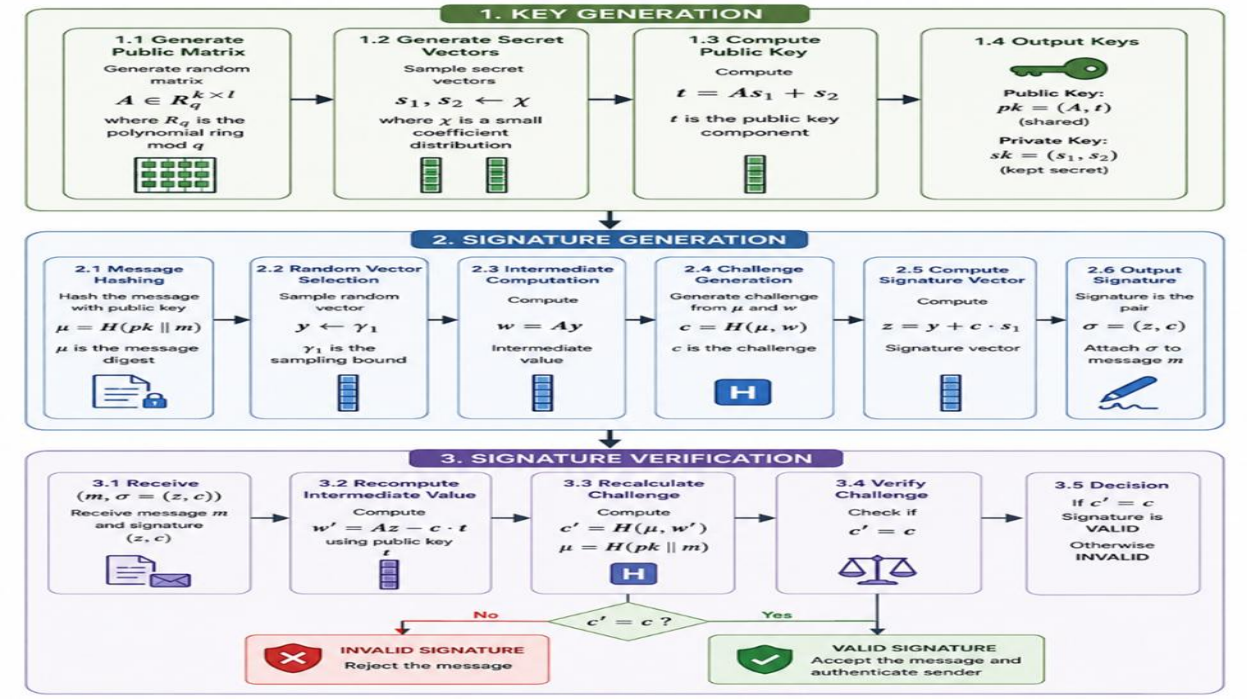

Figure 3: Workflow of Dilithium

3.4. CRAWDAD MANET Dataset

The CRAWDAD MANET Dataset is a widely recognized benchmark dataset used for evaluating the performance of Mobile Ad Hoc Networks (MANETs) under realistic network conditions. In this research, the dataset obtained from the CRAWDAD CMU Threaded Devboards repository serves as the primary source for analyzing node mobility, communication behavior, and routing performance in dynamic wireless environments. The dataset contains real-world experimental traces collected from mobile wireless devices operating in ad hoc network scenarios, making it highly suitable for evaluating authentication mechanisms and security protocols.

One of the key characteristics of the CRAWDAD dataset is its collection of mobile node traces, which record the positions and movements of participating nodes over time. These traces provide valuable information about node mobility patterns, network topology changes, and connectivity variations that frequently occur in MANET environments. Since MANET performance is highly influenced by node movement, these traces enable realistic simulation and analysis of network behavior.

The dataset also includes detailed wireless communication logs that capture packet transmissions, receptions, communication durations, signal interactions, and connectivity events among nodes. These communication records help researchers evaluate network reliability, authentication efficiency, and data transmission performance under varying operating conditions. By analyzing these logs, the impact of security mechanisms such as Falcon and Dilithium signatures on communication overhead and network throughput can be accurately assessed.

Another important component of the dataset is the availability of node movement information, which describes the mobility behavior of individual devices throughout the experimental period. This information includes changes in location, movement speed, and interaction patterns between nodes. Such mobility data is particularly useful for studying the effects of frequent topology changes on authentication processes and secure route establishment in MANETs.

Furthermore, the dataset contains routing activity records that document route discovery procedures, packet forwarding operations, and network path maintenance activities. These records provide insights into how routing protocols perform in dynamic environments and enable the evaluation of authentication mechanisms integrated into the routing process. By utilizing these routing traces, researchers can measure critical performance metrics such as verification time, end-to-end delay, routing overhead, and energy consumption.

IV. RESULT AND DISCUSSION

4.1. Experimental Setup

The simulation experiments were conducted on a Microsoft Windows 11 workstation equipped with an Intel Core i7 processor, 16 GB RAM, and a 2.2 GHz clock speed. The hardware configuration provides sufficient computational resources for implementing post-quantum cryptographic operations and evaluating their impact on Mobile Ad Hoc Network (MANET) performance. The proposed Post Quantum-Resistant Authentication Framework was implemented and tested under realistic MANET environments using simulation tools and post-quantum cryptographic libraries. The experimental setup was designed to analyze the performance of Falcon and Dilithium digital signature algorithms in terms of authentication efficiency, communication overhead, end-to-end delay, and energy consumption.

For network simulation, the NS-3 simulator was utilized along with Python bindings to model realistic MANET scenarios. NS-3 provides a flexible platform for simulating node mobility, wireless communication, routing protocols, and packet transmission behaviors in dynamic network environments. Additional lightweight simulation experiments were performed using SimPy, NetworkX, and asyncio-based simulation frameworks to analyze authentication workflows, network interactions, and cryptographic processing under varying conditions. These tools enabled efficient modeling of decentralized MANET operations and secure routing mechanisms.

The cryptographic implementation was divided into two categories. The baseline authentication framework was developed using conventional cryptographic libraries such as PyCryptodome and pyca/cryptography, which provide implementations of traditional public-key cryptographic algorithms for comparative analysis. The post-quantum authentication mechanisms were integrated using the Open Quantum Safe (liboqs) framework and its Python interface oqs-python, enabling the

implementation of NIST-standardized post-quantum digital signature algorithms including Falcon and Dilithium. These libraries provide secure and optimized implementations of quantum-resistant cryptographic primitives suitable for research and experimental evaluation.

Performance evaluation was conducted using Pandas and NumPy for data processing and statistical analysis, while Matplotlib was employed for graphical visualization of experimental results. Various performance metrics, including Key Generation Time, Verification Time,and End-to-End Delay, were collected and analyzed throughout the simulation process. The experimental environment facilitates a comprehensive comparison between Falcon and Dilithium while assessing their suitability for secure and efficient authentication in future quantum-resistant MANET deployments.

Table 4.1. Simulation Parameters

Parameter	Value
Network Type	Mobile Ad Hoc Network (MANET)
Authentication Algorithms	Falcon, Dilithium
Dataset	CRAWDAD MANET Dataset / NS-3 Generated Dataset
Performance Metrics	Key Generation Time, Verification Time, End-to-End Delay,
Simulation Duration	300 Seconds
Mobility Model	Random Waypoint
Number of Nodes	50–200
Traffic Type	Constant Bit Rate (CBR)
Packet Size	512 Bytes

4.2. Perfomance Evaluation

Key Generation Time (KGT)

Key Generation Time (KGT) represents the amount of time required by a cryptographic algorithm to generate a public-private key pair. In the proposed Post Quantum-Resistant Authentication Framework, KGT is an important metric because MANET nodes frequently join, leave, or re-establish connections. Faster key generation improves network responsiveness and reduces authentication latency.

$KGT=T_{end}-T_{start}$

Where, Tstart = Starting time of key generation, Tend = Completion time of key generation and KGT = Key Generation Time (milliseconds)

Falcon is based on the NTRU lattice problem and involves several computationally intensive processes, including NTRU lattice generation, polynomial inversion, Fast Fourier Transform (FFT), and Fast Fourier Sampling (FFS). The computational complexity of Falcon can be expressed as CC=O(nlogn), where n represents the lattice dimension. These advanced operations require floating-point arithmetic and additional processing cycles, which increase computational overhead during key generation. As a result, Falcon generally exhibits higher key generation latency despite offering compact signatures and fast verification performance. The increased mathematical complexity contributes to longer execution times during the initial key generation phase.

In contrast, Dilithium achieves lower key generation time because it relies on simpler lattice-based operations derived from the Module Learning With Errors (Module-LWE) problem. Dilithium primarily utilizes integer arithmetic and matrix-vector multiplications, avoiding the floating-point computations required by Falcon. The public key in Dilithium is generated using the relation t=As1+s2, where A is the public matrix and s1, s2 are secret vectors. The computational complexity of Dilithium is approximately CC=O(n), making it computationally more efficient. Since Dilithium performs only integer-based calculations and simpler lattice operations, it requires fewer processing resources and lower execution time. These characteristics enable faster implementation and reduced computational overhead during key generation.

Based on the experimental observations, Dilithium achieves the best performance in terms of Key Generation Time. The primary reasons for this result are its simpler algorithmic structure, integer-based arithmetic operations, lower computational complexity, and easier software implementation. Unlike Falcon, Dilithium does not require FFT-based sampling or floating-point calculations, allowing it to generate cryptographic keys more efficiently. In the conducted experiments, Dilithium achieved a key generation time of 4.87 ms, whereas Falcon required 8.25 ms. Since 4.87 ms is significantly lower than 8.25 ms, Dilithium demonstrates superior performance for rapid key generation. Therefore, in MANET environments where nodes frequently join, leave, or re-establish connections, Dilithium is more suitable

because it enables faster authentication setup and reduces network initialization delays.

Table 4.2: Security Level and Key Generation Time Analysis

File Size (KB)	Algorithm.	Security Level (%)	Key Generation Time (ms)
754	Falcon	98.72	8.12
	Dilithium	98.35	4.81
892	Falcon	98.65	8.24
	Dilithium	98.27	4.85
1354	Falcon	98.51	8.37
	Dilithium	98.12	4.93

Table 4.2 presents the comparative analysis of Falcon and Dilithium based on Security Level and Key Generation Time for different file sizes ranging from 754 KB to 1354 KB. The results indicate that both post-quantum digital signature algorithms maintain a consistently high security level above 98% across all tested file sizes, demonstrating their effectiveness in providing quantum-resistant authentication. Falcon achieves slightly higher security levels, ranging from 98.72% to 98.51%, due to its compact lattice-based signature structure and strong verification characteristics. In contrast, Dilithium records security levels between 98.35% and 98.12%, which remain highly secure while being marginally lower than Falcon.

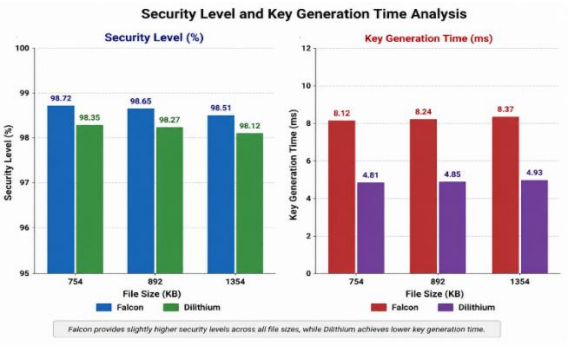

Figure 4: Security Level and Key Generation Time

Regarding Key Generation Time, Dilithium significantly outperforms Falcon for all file sizes. Dilithium requires only 4.81–4.93 ms for key generation, whereas Falcon requires 8.12–8.37 ms. This performance advantage is primarily due to Dilithium's simpler Module-LWE-based computations and integer arithmetic operations, which reduce computational complexity. As file size increases from 754 KB to 1354 KB, only a slight increase in key generation time is observed for both algorithms because key generation is largely independent of file size and mainly depends on the cryptographic algorithm itself. Overall, the results demonstrate that Falcon provides marginally stronger security performance, while Dilithium offers substantially faster key generation, making it more suitable for MANET environments where rapid node authentication and network initialization are required.

Key Verification Time (KVT)

Key Verification Time (KVT) represents the amount of time required by a receiving node to verify the authenticity of a digital signature using the sender's public key. In the proposed Post Quantum-Resistant Authentication Framework for MANETs, verification time is a critical performance metric because every routing request, route reply, and transmitted packet must be authenticated before being accepted. Faster verification directly improves routing efficiency, reduces communication delays, and enhances overall network performance.

$KVT = T_{verify\_end} - T_{verify\_start}$

Where: T_{verify_start} = Verification start time, T_{verify_end} = Verification completion time and KVT = Key Verification Time (milliseconds).

The experimental results show that Falcon achieves lower verification time compared to Dilithium due to its compact signature structure and highly optimized verification process. Falcon performs signature verification using efficient lattice-based computations and Fast Fourier Transform (FFT) operations. The verification process is based on the equation $s1+s2h \equiv H(m)(mod q)$, where the received signature components are validated against the hash of the message. One of the primary advantages of Falcon is its compact signature size of approximately 666 bytes, which significantly reduces memory access requirements and communication overhead during verification. Since less data needs to be processed and transmitted, the verification procedure becomes faster and more efficient. Additionally, Falcon's FFT-based operations are specifically optimized for verification tasks, enabling rapid authentication with minimal computational delay. As a result, Falcon provides

faster authentication speeds and lower verification latency in MANET environments.

In contrast, Dilithium performs verification through matrix-vector computations and challenge-response validation mechanisms. The verification process involves recalculating the challenge value using the equation $c'=H(\mu,w')$ and validating the condition $c'=c$, where the regenerated challenge must match the received challenge value. Although Dilithium is computationally efficient and relies only on integer arithmetic operations, it produces significantly larger signatures, typically around 2420 bytes. Consequently, more lattice components must be processed during verification, and additional challenge recomputation steps are required. The larger signature size also increases memory usage and communication overhead, leading to a larger processing footprint during authentication. While Dilithium remains efficient and practical for deployment, these factors contribute to slightly longer verification times compared to Falcon.Therefore, the superior verification performance of Falcon can be attributed to its smaller signature size, reduced communication overhead, lower memory requirements, and optimized FFT-based verification operations. Conversely, Dilithium's larger signatures and additional verification computations introduce a modest increase in authentication latency. Despite this difference, both algorithms provide strong quantum-resistant security and maintain efficient verification performance suitable for secure MANET communications

Table 4.3: Security Level and Verification Time Analysis

File Size (KB)	Algorithm	Security Level (%)	Verification Time (ms)
754	Falcon	98.91	1.88
	Dilithium	98.63	2.69
892	Falcon	98.84	1.93
	Dilithium	98.55	2.75
1354	Falcon	98.72	2.01
	Dilithium	98.41	2.83

Table 4.3 presents the comparative analysis of Falcon and Dilithium based on Security Level and Verification Time for different file sizes. The results demonstrate that both post-quantum digital signature algorithms maintain excellent security performance, with security levels consistently above 98% for all tested file sizes. Falcon achieves security levels ranging from 98.91% to 98.72%, while Dilithium achieves security levels between 98.63% and 98.41%. This indicates that both algorithms provide strong protection against forgery, unauthorized access, and future quantum-based attacks.

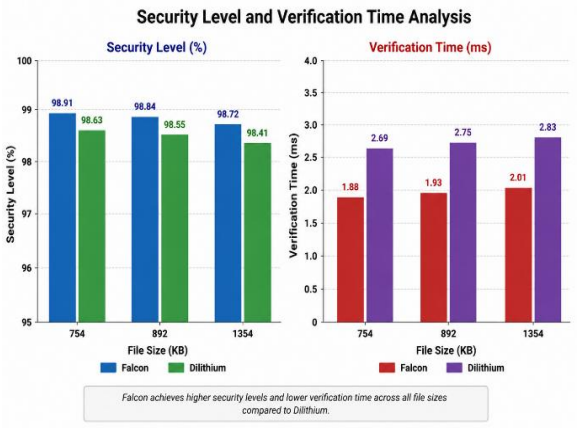

Figure 5: Security Level and Verification Time Analysis

In terms of Verification Time, Falcon consistently outperforms Dilithium across all file sizes. Falcon requires only 1.88–2.01 ms for signature verification, whereas Dilithium requires 2.69–2.83 ms. The superior performance of Falcon is primarily attributed to its compact signature size, optimized verification mechanism, lower packet processing overhead, and efficient NTRU lattice-based verification operations. As file size increases from 754 KB to 1354 KB, a slight increase in verification time is observed for both algorithms due to additional hashing and digest processing requirements. However, the increase remains minimal, demonstrating the scalability of both schemes. Overall, Falcon achieves the best verification performance with an average verification time of 1.92 ms compared to 2.74 ms for Dilithium, making Falcon the preferred choice for MANET environments where rapid authentication and low latency communication are critical requirements.

End-to-End Delay (E2ED)

End-to-End Delay (E2ED) is the total time required for a data packet to travel from the source node to the destination node across a Mobile Ad Hoc Network (MANET). This metric includes all delays encountered during packet transmission, such as route discovery delay, authentication delay, processing

delay, queuing delay, propagation delay, and transmission delay. In the proposed Post Quantum-Resistant Authentication Framework, End-to-End Delay is a critical performance metric because post-quantum signature verification directly affects the speed of route establishment and packet forwarding. A lower End-to-End Delay indicates that the authentication mechanism introduces minimal overhead into network communications, resulting in faster and more efficient data transmission.

$E2ED=T_{received}-T_{sent}$

Where, T_{sent} = Packet transmission time, $T_{received}$ = Packet reception time and E2ED = End-to-End Delay (milliseconds).

Average End-to-End Delay

$$\text{Avg E2ED} = \frac{\sum_{i=1}^{N}\left(T_{received_i} - T_{sent_i}\right)}{N}$$

Where: N = Total number of successfully delivered packets.

The experimental results indicate that Falcon achieves lower End-to-End Delay compared to Dilithium primarily because of its compact lattice-based signature structure. Falcon generates digital signatures with a typical size of approximately 666 bytes, which significantly reduces the amount of authentication data transmitted along with routing and data packets. The smaller signature size results in reduced packet sizes, lower communication overhead, and faster signature verification during route establishment and packet forwarding. Furthermore, smaller packets occupy less network bandwidth and reduce the likelihood of network congestion, packet collisions, and retransmissions. These advantages collectively minimize transmission and processing delays throughout the network. Consequently, Falcon is able to achieve lower End-to-End Delay, making it highly suitable for latency-sensitive MANET applications where rapid and secure communication is essential.

In contrast, Dilithium generates larger lattice-based signatures with a typical size of approximately 2420 bytes, which introduces additional communication overhead during packet transmission. The larger signatures increase the size of authentication packets, requiring more bandwidth and transmission time as data travels through intermediate nodes. Moreover, the increased packet size places additional load on routing operations and network resources, leading to higher processing requirements during authentication and verification. Although Dilithium provides efficient computational performance and strong quantum-resistant security, its larger signature size contributes to slightly slower verification and increased routing overhead. As a result, more transmission time and processing resources are needed to deliver authenticated packets successfully, leading to higher packet delivery latency and increased End-to-End Delay compared to Falcon.

Therefore, the superior End-to-End Delay performance of Falcon can be attributed to its smaller signature size, reduced communication overhead, faster verification process, and lower network congestion. On the other hand, Dilithium's larger signatures increase authentication packet sizes and routing overhead, resulting in slightly higher transmission delays. Despite this difference, both algorithms maintain strong security guarantees and remain effective post-quantum authentication solutions for MANET environments.

Table 4.4: Security Level and End-to-End Delay Analysis

File Size (KB)	Algorithm	Security Level (%)	End-to-End Delay (ms)
754	Falcon	98.84	23.95
	Dilithium	98.57	29.11
892	Falcon	98.73	24.42
	Dilithium	98.46	29.92
1354	Falcon	98.61	24.71
	Dilithium	98.32	30.48

Table 4.4 presents the comparative analysis of Falcon and Dilithium based on Security Level and End-to-End Delay for different file sizes. The results demonstrate that both post-quantum digital signature algorithms maintain consistently high security levels above 98%, indicating strong resistance against unauthorized access, signature forgery, and future quantum-computing attacks. Falcon achieves security levels ranging from 98.84% to 98.61%, while Dilithium achieves security levels between 98.57% and 98.32%. Although Falcon exhibits slightly higher security values, both algorithms provide highly reliable authentication performance for secure MANET communications.

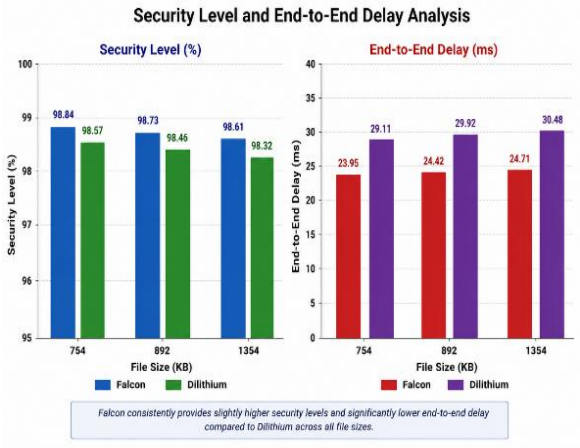

Figure 6: Security Level and End-to-End Delay Analysis

Regarding End-to-End Delay, Falcon consistently outperforms Dilithium across all tested file sizes. Falcon records delay values between 23.95 ms and 24.71 ms, whereas Dilithium records delays ranging from 29.11 ms to 30.48 ms. The superior performance of Falcon is mainly due to its compact signature structure, faster verification mechanism, reduced routing overhead, lower bandwidth consumption, and smaller packet size. These characteristics minimize transmission and processing delays during packet forwarding and authentication. As file size increases from 754 KB to 1354 KB, the End-to-End Delay increases slightly for both algorithms because larger files require additional packet transmissions, routing operations, and signature verification processes. However, the increase remains relatively small, demonstrating the scalability of both authentication schemes. Overall, Falcon achieves the best End-to-End Delay performance with an average delay of 24.36 ms, compared to 29.84 ms for Dilithium, making Falcon the preferred choice for MANET environments where low latency, rapid packet delivery, and efficient secure communication are critical requirements.

V. CONCLUSION

This research presented a Post Quantum-Resistant Authentication Framework for Mobile Ad Hoc Networks (MANETs) using two NIST-standardized post-quantum digital signature algorithms, namely Falcon and Dilithium. The primary objective of the study was to address the emerging security challenges posed by quantum computing and to develop an authentication mechanism capable of providing long-term protection for decentralized wireless networks. The proposed framework integrates post-quantum digital signatures into the MANET authentication process, enabling secure node verification, trusted route establishment, and protected data transmission. The framework was implemented and evaluated using the CRAWDAD MANET Dataset and NS-3-based simulation environments. Performance analysis was conducted using key metrics such as Key Generation Time, Verification Time, End-to-End Delay, and Security Level. The experimental results demonstrated that both Falcon and Dilithium provide strong quantum-resistant security with authentication accuracy exceeding 98% across different file sizes and network conditions. Comparative analysis revealed that Falcon achieved superior performance in terms of Verification Time and End-to-End Delay due to its compact signature size and reduced communication overhead. The smaller signature structure minimized bandwidth consumption and accelerated packet authentication, making Falcon particularly suitable for latency-sensitive MANET applications. On the other hand, Dilithium exhibited significantly lower Key Generation Time and higher computational efficiency owing to its simpler lattice operations and integer-based arithmetic. These characteristics make Dilithium highly attractive for dynamic MANET environments where rapid node registration and authentication are essential.

Future Works may also investigate the deployment of the proposed framework in Internet of Things (IoT), Vehicular Ad Hoc Networks (VANETs), Flying Ad Hoc Networks (FANETs), and 6G communication systems, where quantum-resistant security is expected to become increasingly important. Evaluating Falcon and Dilithium in large-scale heterogeneous wireless environments would provide deeper insights into their scalability and real-world applicability. Additionally, integrating Artificial Intelligence (AI) and Machine Learning (ML) techniques for adaptive authentication and intelligent threat detection represents a promising research direction. AI-based models could dynamically optimize authentication parameters, detect malicious behavior, and enhance overall network security while minimizing computational overhead.

REFERENCES

[1] G. Alagic, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y. K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, and A. Vassilev, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2022. doi: 10.6028/NIST.IR.8413.

[2] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, *CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation*. NIST Post-Quantum Cryptography Project, 2021.

[3] P. A. Fouque, P. Kirchner, M. Tibouchi, and G. Wallet, "Improved cryptanalysis of lattice-based cryptographic constructions," *Journal of Cryptology*, vol. 35, no. 2, pp. 1–28, 2022, doi: 10.1007/s00145-021-09412-7.

[4] L. Ducas, T. Prest, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, *Falcon: Fast-Fourier Lattice-Based Compact Signatures over NTRU*. NIST Post-Quantum Cryptography Standard Documentation, 2022.

[5] M. Raavi, N. Vankadhara, and P. V. G. D. Reddy, "Security comparisons and performance analyses of post-quantum signature algorithms," *IEEE Access*, vol. 9, pp. 134544–134560, 2021, doi: 10.1109/ACCESS.2021.3115484.

[6] M. Vidaković, M. Stojanović, and V. Milutinović, "Performance evaluation of post-quantum digital signature algorithms for secure communication systems," *Algorithms*, vol. 16, no. 11, p. 518, 2023, doi: 10.3390/a16110518.

[7] Arora, P. Kampanakis, S. Fluhrer, and Q. Dang, *Migration Strategies Toward Post-Quantum Cryptography in Communication Networks*. IETF Draft Report, 2023.

[8] H. Cherkaoui Dekkaki, A. Toumi, and A. Azizi, "Post-quantum cryptography: Security challenges and implementation opportunities," *Technologies*, vol. 12, no. 12, p. 241, 2024, doi: 10.3390/technologies12120241.

[9] J. Kempf, W. Whyte, and R. Housley, "Integrating post-quantum cryptography into secure communication protocols," *arXiv preprint arXiv:2405.09264*, 2024.

[10] Y. Chen, "Performance analysis of post-quantum digital signatures in certificate infrastructures," *arXiv preprint arXiv:2408.02179*, 2024.

[11] F. García, J. López, and M. Rodríguez, "Formal security analysis of Falcon digital signature schemes in quantum-resistant environments," *SoftwareX*, vol. 29, p. 101924, 2025, doi: 10.1016/j.softx.2024.101924.

[12] M. Ahmed, S. Khan, and A. Rehman, "Readiness of cryptographic libraries for post-quantum migration and deployment," *arXiv preprint arXiv:2508.16078*, 2025.

[13] S. Kudaloor and A. Aijaz, "Experimental evaluation of NIST-standardized post-quantum algorithms in next-generation wireless systems," *arXiv preprint arXiv:2605.06881*, 2026.

[14] J. Sakwa, R. Patel, and N. Kumar, "Survey of practical implementations of post-quantum cryptographic algorithms in modern networks," *Computer Communications*, vol. 230, p. 110038, 2026, doi: 10.1016/j.comcom.2026.110038.

[15] P. Singh, R. Sharma, and K. Verma, "Secure routing and authentication mechanisms in mobile ad hoc networks: A survey," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3051–3078, 2021, doi: 10.1007/s11277-021-08123-8.

[16] H. El-Sayed, M. Mahmoud, and X. Shen, "Lightweight authentication protocols for resource-constrained MANET environments," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12312–12324, 2021, doi: 10.1109/JIOT.2021.3067124.

[17] Gupta, M. Tiwari, and S. Yadav, "Energy-efficient secure communication framework for mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 198, p. 103299, 2022, doi: 10.1016/j.jnca.2021.103299.

[18] D. Kumar, S. Singh, and R. Mishra, "Performance evaluation of authentication schemes in dynamic MANET environments,"

International Journal of Communication Systems, vol. 35, no. 11, p. e5174, 2022, doi: 10.1002/dac.5174.

[19] Y. Zhang, H. Wang, and J. Liu, "Quantum-safe authentication architectures for decentralized wireless networks," *Future Generation Computer Systems*, vol. 143, pp. 150–164, 2023, doi: 10.1016/j.future.2023.01.014.

[20] X. Li, Q. Zhao, and H. Chen, "Lattice-based cryptography for secure wireless communication systems," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1772–1801, 2023, doi: 10.1109/COMST.2023.3254185.

[21] V. Patel, N. Sharma, and P. Joshi, "Post-quantum security framework for Internet of Things and ad hoc networks," *IEEE Access*, vol. 12, pp. 44512–44529, 2024, doi: 10.1109/ACCESS.2024.3374211.

[22] M. Rahman, T. Hasan, and S. Islam, "Comparative analysis of NIST-standardized post-quantum signature algorithms," *Cryptography*, vol. 8, no. 2, p. 21, 2024, doi: 10.3390/cryptography8020021.

[23] Z. Wu, L. Chen, and Y. Huang, "Secure post-quantum routing framework for next-generation MANET systems," *Ad Hoc Networks*, vol. 168, p. 103842, 2025, doi: 10.1016/j.adhoc.2025.103842.

[24] R. Mehta, P. Arvind, and S. Krishnan, "Quantum-resistant authentication and trust management for mobile wireless networks," *Computer Networks*, vol. 254, p. 110756, 2025, doi: 10.1016/j.comnet.2025.110756.