JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Post-Quantum Blockchain-Based Consensus for Trusted Data Transmission in Mobile Ad Hoc Networks

[1]R.Priyavani, [2]Dr.N.Kowsalya
[1]Research Scholar, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.
[2] Assistant Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.

Abstract: Mobile Ad Hoc Networks (MANETs) operate in highly dynamic and decentralized environments, making them vulnerable to malicious behavior, data tampering, and identity spoofing. Existing trust mechanisms primarily rely on centralized authorities or classical cryptographic techniques, which are increasingly unsuitable due to scalability limitations and emerging threats from quantum computing. This paper proposes a novel post-quantum blockchain-based consensus framework for secure and trusted data transmission in MANETs. The proposed model integrates lightweight blockchain consensus with quantum-resistant cryptographic primitives, including post-quantum key encapsulation and digital signature schemes, to ensure secure node authentication and immutable trust management. The framework is implemented and evaluated using ns-3 simulations and Python-based cryptographic libraries, with comparative analysis against Identity-Based Cryptography (IBC) and Elliptic Curve Cryptography (ECC) based approaches. Performance is measured in terms of key generation time, end-to-end delay, consensus overhead, and security resilience. Experimental results demonstrate that the proposed framework achieves strong quantum resistance with acceptable computational and communication overhead, making it a viable solution for next-generation secure MANET applications.

Keywords: *Post-Quantum Cryptography, Blockchain Consensus, MANET Security, Trusted Data Transmission, Quantum-Resistant Networks, Decentralized Trust, Kyber, Dilithium*

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are decentralized, infrastructure-less wireless networks where nodes autonomously organize and forward data for one another. Because there is no fixed infrastructure or centralized controller, maintaining secure and trustworthy communication among participating nodes is inherently challenging. The very characteristics that make MANETs flexible—dynamic topology, peer-to-peer routing, and frequent node mobility—also introduce vulnerabilities to malicious behavior such as packet dropping, identity spoofing, and routing disruption [1]. Trust in MANETs refers to the confidence that a given node will behave honestly and consistently in forwarding data and participating in network functions. Without an effective trust mechanism, malicious or selfish nodes can degrade network performance or compromise data integrity. Recent research highlights that conventional trust and security models, when applied to MANETs, struggle to ensure robust data transmission due to the lack of fixed infrastructure and inherent node autonomy [2]. Traditional trust and authentication mechanisms in MANETs often depend on centralized authorities such as certification authorities (CAs) or predefined servers for key management and trust evaluation. While these centralized infrastructures work well in conventional networks, they are fundamentally incompatible with the decentralized nature of MANETs. Centralized trust models introduce single points of failure; if the central authority becomes inaccessible or compromised, the entire trust mechanism collapses, leaving the network vulnerable to attacks and misbehavior [3]. Moreover, lightweight approaches like public key infrastructures (PKIs) still require elements of central coordination or third-party certification, which cannot be guaranteed in highly dynamic, distributed environments without fixed infrastructure. Such reliance increases communication overhead, latency, and complexity in maintaining secure trust relationships among mobile nodes [4]. Emerging decentralized approaches, including blockchain-based trust frameworks, aim to eliminate single points of failure by distributing trust computation and storage across network nodes. These methods show promise in addressing centralized model weaknesses, but they introduce new challenges related to computational overhead, consensus delays, and resource constraints in MANET environments [5].

Classical cryptographic primitives such as RSA, elliptic-curve cryptography (ECC), and Diffie–Hellman key exchange form the backbone of authentication and secure communication in modern networks, including MANETs. These algorithms rely on computational hardness assumptions like integer factorization and discrete logarithms, which are considered intractable for classical computers. However, quantum computing algorithms—

most notably Shor's algorithm—can solve these problems in polynomial time, rendering many current public-key schemes insecure once sufficiently powerful quantum computers emerge [6]. This vulnerability extends to blockchain systems, which heavily depend on ECC-based digital signatures for transaction authentication and key management. Theoretical and practical analyses indicate that quantum computers capable of breaking ECC and RSA could compromise the integrity of blockchain ledgers and digital identities, posing severe risks to distributed trust systems [7]. Because of this looming threat, the National Institute of Standards and Technology (NIST) has finalized post-quantum cryptography (PQC) standards aimed at replacing vulnerable classical schemes with quantum-resistant alternatives such as lattice-based or hash-based algorithms. These PQC algorithms are designed to withstand attacks by both classical and quantum adversaries while enabling long-term data confidentiality and authentication [8]. The integration of Post-Quantum Cryptography (PQC) with blockchain technologies is motivated by the need to simultaneously address two fundamental challenges in MANET security:

- **Quantum-level cryptographic threats:** Classical cryptographic mechanisms are increasingly recognized as inadequate against future quantum attacks, jeopardizing authentication, key exchange, and data integrity in decentralized networks. PQC provides algorithms that resist quantum adversaries, ensuring that keys and signatures remain secure even in the advent of powerful quantum processors.
- **Decentralized trust without central authorities:** MANETs lack fixed infrastructure, making centralized trust and key management impractical or vulnerable. Blockchain's decentralized ledger and consensus mechanisms enable immutable recording of trust metrics and authenticated actions without trusted third parties. When enhanced with PQC, blockchain can establish quantum-resistant trust anchors and prevent unauthorized modifications across dynamic MANET topologies.

By fusing quantum-secure cryptographic primitives with decentralized consensus, a post-quantum blockchain framework can provide both forward-looking security and distributed trust. This approach is essential for MANETs that operate in hostile environments where adversaries may leverage quantum technologies to breach network security or manipulate trust information. The objectives of this research are design a post-quantum blockchain-based consensus model tailored to the decentralized and resource-constrained environment of MANETs, ensuring trusted data transmission even under quantum threats. Perform a comparative analysis of classical trust/authentication mechanisms—specifically Identity-Based Cryptography (IBC) and Elliptic Curve Digital Signature Algorithm (ECDSA)—against the proposed post-quantum blockchain framework in terms of security, performance, and quantum resistance.

II. RELATED WORK

Trust and reputation systems have been the dominant approach to mitigating internal threats in MANETs by estimating node reliability from direct observations and second-hand recommendations. Recent work emphasizes adaptive, distributed reputation schemes that cope with mobility and intermittent interactions, and that combine local trust metrics with collaborative reputation aggregation to detect packet-dropping, misrouting, and selfish behavior in multi-hop environments [9]. To remove single points of failure inherent in centralized PKI or CA models, several studies propose blockchain or distributed-ledger mechanisms to record immutable reputation logs, perform decentralized authentication, or to incentivize cooperative forwarding in MANETs. Blockchain-enabled trust models provide tamper-evident records and programmable trust policies (smart contracts), but they introduce challenges of consensus overhead, storage growth, and energy consumption — problems particularly acute on resource-constrained MANET nodes [10].

Identity-Based Cryptography (IBC) reduces certificate management overhead by deriving public keys from identifiers, making it an attractive option for ad-hoc environments; lattice-based IBC variants have recently been proposed to provide stronger security properties while retaining identity convenience [11]. In contrast, ECC/ECDSA remains popular due to its relatively low computation and small key sizes, but classical ECC lacks resistance to large-scale quantum attacks. Comparative studies show a tradeoff: IBC simplifies key management but can be computationally heavier or require trusted setup, whereas ECC is efficient today but not long-term quantum-safe [12]. Driven by NIST's PQC standardization and industry moves toward quantum-resilient deployments, the networking community has started evaluating lattice-based and hash-based algorithms (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+) for routing, authentication, and ledger protection. Studies report that while PQC algorithms incur higher computation and larger signatures/keys than classical ECC, careful protocol and system design (lightweight consensus, selective signing, hardware offload) can make PQC feasible for many distributed systems; however, evaluations specifically targeting MANET conditions (mobility, intermittent connectivity, energy constraints) remain limited [13].

Prior work provides three important lessons for our problem domain: (1) decentralized reputation and blockchain mechanisms can remove central trust anchors but impose non-trivial overhead in mobile, resource-constrained networks [14], (2) IBC and ECC offer complementary strengths for MANET authentication yet neither addresses both decentralized operation and quantum resistance simultaneously [15], and (3) PQC offers necessary long-term security but requires careful integration with lightweight consensus and communication-efficient ledger designs to be practical in MANETs [16]. These observations reveal a clear gap: **a** lightweight, blockchain-style consensus and trust recording mechanism that natively uses quantum-resistant primitives and is optimized for MANET constraints — the precise problem this paper addresses.

III. PROPOSED POST-QUANTUM BLOCKCHAIN CONSENSUS FRAMEWORK

This section presents the architecture and functional components of the proposed Post-Quantum Blockchain Consensus Framework (PQ-BCF) for trusted data transmission in Mobile Ad Hoc Networks (MANETs). The framework integrates post-quantum cryptographic primitives with a lightweight blockchain consensus mechanism to ensure decentralized, quantum-resistant trust

management. The design is motivated by recent studies highlighting the inadequacy of classical cryptographic and centralized trust models in highly dynamic and adversarial MANET environments [17]. Figure 1, the proposed framework is structured into four main layers: Node Layer, Blockchain Layer, Consensus Layer, and PQC Authentication Layer**,** each responsible for specific security and communication functions. The overall architecture of the proposed framework is illustrated as a multi-layer decentralized system where each mobile node participates in data forwarding, trust evaluation, cryptographic authentication, and blockchain maintenance. Unlike traditional security architectures that rely on centralized authorities, the proposed model distributes trust responsibilities among all participating nodes, thereby eliminating single points of failure and enhancing resilience against internal and external attacks [18].

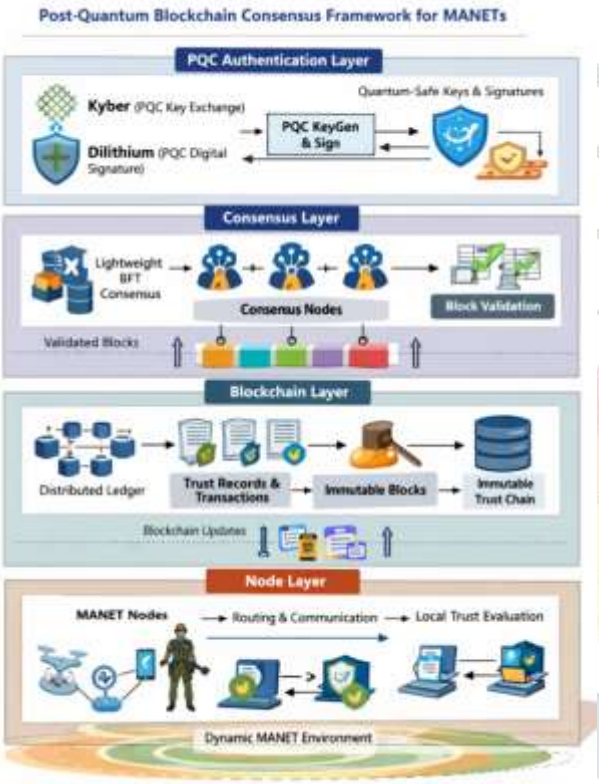

Figure 1: Post-Quantum Blockchain Consensus Framework (PQ-BCF) for MANET

The layered design ensures modularity, scalability, and ease of integration with existing MANET routing protocols.

- **Node Layer:** The Node Layer represents the physical and logical MANET infrastructure, consisting of mobile nodes that act as both data sources and routers. Each node maintains local routing tables, neighbor lists, and trust metrics based on direct communication experiences. Due to the absence of centralized control, nodes must autonomously evaluate the trustworthiness of neighboring nodes and decide whether to forward or discard packets accordingly. Recent studies emphasize that node-level trust evaluation is critical for detecting malicious behaviors such as packet dropping, route manipulation, and impersonation attacks [19]. In the proposed framework, nodes periodically generate trust reports that are submitted to the blockchain layer for immutable storage and verification.
- **Blockchain Layer:** The Blockchain Layer serves as a decentralized trust ledger that records authentication events, trust scores, and routing behavior of participating nodes. Each block contains cryptographically signed trust transactions that cannot be altered without network consensus, ensuring tamper-resistant trust management. Blockchain-based trust systems have been shown to significantly improve accountability and transparency in MANETs by preventing falsification of reputation data and eliminating reliance on centralized authorities [20]. In the proposed framework, only lightweight trust metadata is stored on-chain to minimize storage overhead and communication cost.
- **Consensus Layer:** The Consensus Layer is responsible for validating blocks and ensuring agreement among nodes regarding the authenticity of trust information. Traditional blockchain consensus mechanisms such as Proof-of-Work or Proof-of-Stake are computationally expensive and unsuitable for MANETs. Therefore, the proposed framework adopts a lightweight consensus protocol optimized for low latency and limited resources. Recent research suggests that simplified Byzantine Fault Tolerant (BFT) or reputation-assisted consensus mechanisms are more appropriate for ad-hoc environments, as they reduce computation and communication overhead while maintaining security [21]. In this work, consensus decisions are based on a combination of trust scores and post-quantum authenticated signatures.
- **PQC Authentication Layer:** The **Post-Quantum Cryptography (PQC) Authentication Layer** ensures quantum-resistant identity verification and message integrity. This layer replaces classical cryptographic primitives (e.g., RSA, ECC) with quantum-secure alternatives such as lattice-based key encapsulation and digital signature schemes. Following NIST's post-quantum standardization efforts, algorithms like **CRYSTALS-Kyber** for key exchange and **CRYSTALS-Dilithium** for digital signatures are increasingly recommended for future-proof network security [22]. The proposed framework uses PQC signatures to authenticate nodes before allowing them to participate in consensus or data transmission, thereby preventing quantum-enabled impersonation and key recovery attacks.

3.1. Identity-Based Cryptography (IBC)

Identity-Based Cryptography (IBC) is a public key cryptographic paradigm in which a user's public key is derived directly from a unique identity string such as an email address, IP address, or node ID. Unlike traditional Public Key Infrastructure (PKI), IBC eliminates the need for digital certificates and certificate authorities, thereby simplifying key management in decentralized environments like MANETs. However, this convenience comes at the cost of higher computational overhead and reliance on a trusted Private Key Generator (PKG), which introduces scalability and performance challenges [23]. Step-by-Step IBC Model are followed,

Let:

- ID = identity of a node (e.g., NodeA@MANET)
- G1,G2 = cyclic groups of prime order q
- P∈G1 = generator point
- e:G1×G1→G2 = bilinear pairing function
- H1(.) = hash function mapping identities to group elements

Step 1: System Setup (by PKG)

The Private Key Generator selects a master secret:

$$s \in Z_q$$

Computes the master public key:

$$P_{pub} = sP$$

Publishes system parameters:

$$params = \{G_1, G_2, q, P, P_{pub}, H_1\}$$

Step 2: Key Extraction

For a node with identity ID:

$$Q_{ID} = H_1(ID)$$

Private key:

$$S_{ID} = s.Q_{ID}$$

This is securely sent to the node.

Step 3: Encryption (Sender → Receiver)

To encrypt message M for identity ID:

1. Pick random r∈Zq
2. Compute:

$$U = rP$$

$$V = M \oplus H_2(e(Q_{ID}, P_{pub})^r)$$

Ciphertext:

$$C = (U, V)$$

Step 4: Decryption (Receiver)

Receiver computes:

$$M = \oplus H_2(e(S_{ID}, U))$$

Because:

$$e(S_{ID}) + e(sQ_{ID}, rP) = e(Q_{ID}, P_{pub})^r$$

Identity-Based Cryptography (IBC) relies on bilinear pairing operations, which are computationally significantly more expensive than the scalar multiplication operations used in Elliptic Curve Cryptography (ECC). While ECC scalar multiplication typically requires only a few milliseconds (approximately 1–2 ms), bilinear pairing operations may take an order of magnitude longer, often in the range of 10–20 ms. Since IBC encryption generally involves two to three pairing computations and decryption requires one to two pairings, the overall cryptographic cost becomes substantial. Consequently, in Mobile Ad Hoc Networks (MANETs), where nodes are constrained by limited processing power, memory, and battery capacity, the use of IBC leads to increased end-to-end transmission delay, higher energy consumption, and reduced scalability as the network size grows. These performance limitations make IBC less suitable for large-scale or highly dynamic MANET environments despite its conceptual advantages [24].

Advantages of IBC: The primary advantage of Identity-Based Cryptography is the elimination of digital certificates, as public keys are directly derived from unique user identities such as node IDs or email addresses. This significantly simplifies public key distribution and removes the overhead associated with certificate management. IBC is particularly attractive for dynamic and decentralized networks because nodes can immediately compute public keys without contacting a certification authority. Furthermore, the direct binding between identity and cryptographic keys improves usability and reduces administrative complexity, making IBC conceptually well-suited for mobile and ad hoc networking scenarios.

Limitations of IBC: Despite its advantages, IBC suffers from several critical limitations that restrict its practical deployment in MANETs. A major drawback is the key escrow problem, as the Private Key Generator (PKG) generates all private keys and therefore has full access to user secrets, undermining true end-to-end confidentiality. Additionally, the heavy reliance on pairing-based cryptography results in high computational overhead, making IBC inefficient for resource-constrained devices. The PKG also represents a single point of trust and failure, since its compromise would expose the entire system's security. Finally, scalability remains a significant concern, as the PKG must handle key generation and distribution for all nodes, creating performance bottlenecks in large or highly dynamic networks.

3.2. ECC-Based Authentication (ECDSA)

Elliptic Curve Cryptography (ECC) is a widely adopted public key cryptographic approach that provides strong security with relatively small key sizes, making it particularly suitable for resource-constrained environments such as Mobile Ad Hoc Networks (MANETs). The Elliptic Curve Digital Signature Algorithm (ECDSA) is commonly used for authentication and message integrity, enabling nodes to verify the identity of communicating peers and ensure that transmitted data has not been altered. Due to its low computational and communication overhead, ECDSA is considered lightweight and efficient for real-time mobile networks. However, ECC-based schemes rely on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which can be efficiently solved using Shor's algorithm on quantum computers, making ECDSA

fundamentally vulnerable in the post-quantum era [25]. Step-by-Step ECDSA Model are followed,

Let:

- p = large prime number
- E = elliptic curve defined as:

$$E: y^2 = x^3 + ax + b \mod p$$

- G = base point on the curve
- n = order of G
- H(.) = secure hash function (e.g., SHA-256)

Step 1: Key Generation

Each node selects a random private key:

$$d \in [1, n-1]$$

Computes the public key:

$$Q = dG$$

Step 2: Signature Generation

For a message m:

1. Compute hash:

$$e = H(m)$$

2. Choose random (k \in [1, n-1]]
3. Compute point:

$$(x_1, y_1) = kG$$

4. Compute:

$$r = x_1 \mod n$$

$$s = k^{-1}(e + dr) \mod n$$

Signature:

(r,s)

Step 3: Signature Verification

Receiver computes:

$$e = H(m)$$

$$\omega = s^{-1} \mod n$$

$$u_1 = e\omega \mod n$$

$$u_2 = r\omega \mod n$$

$$(x_2, y_2) = u_1 G + u_2 Q$$

Signature valid if:

$$r \equiv x_2 \mod n$$

ECDSA requires only elliptic curve point multiplications and modular arithmetic, which are computationally efficient even on low-power devices. Compared to RSA, ECC achieves equivalent security with much smaller key sizes (e.g., 256-bit ECC ≈ 3072-bit RSA), reducing memory usage, transmission overhead, and processing delay. This makes ECDSA highly suitable for MANETs, IoT systems, and real-time mobile communications. ECDSA security depends entirely on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Quantum computers running Shor's algorithm can solve ECDLP in polynomial time, allowing attackers to recover private keys from public keys and forge valid signatures. Once practical quantum computers become available, all ECC-based authentication mechanisms will be cryptographically broken, compromising identity verification, data integrity, and blockchain systems that rely on ECDSA.

Advantages of ECDSA: The Elliptic Curve Digital Signature Algorithm (ECDSA) offers several practical advantages that make it highly suitable for resource-constrained and real-time communication environments such as Mobile Ad Hoc Networks (MANETs). One of its key strengths is the use of small key sizes, which provide strong security while significantly reducing storage and transmission overhead. ECDSA also exhibits low computational cost compared to classical public-key schemes such as RSA, enabling faster signature generation and verification even on low-power devices. In addition, the compact size of ECDSA signatures results in low communication overhead, which is particularly beneficial in bandwidth-limited wireless networks. Furthermore, ECDSA is widely implemented, standardized, and supported across most cryptographic libraries and network protocols, making it easy to deploy in practical systems. Due to these properties, ECDSA is well suited for real-time MANET operations where efficiency, responsiveness, and low resource consumption are critical.

Limitations of ECDSA: Despite its efficiency and widespread adoption, ECDSA suffers from several critical limitations that threaten its long-term viability. The most significant drawback is its vulnerability to quantum attacks, as the underlying security of ECDSA depends on the Elliptic Curve Discrete Logarithm Problem, which can be efficiently solved using Shor's algorithm on a sufficiently powerful quantum computer. This makes ECDSA fundamentally insecure in the post-quantum era. Additionally, ECDSA does not provide forward security, meaning that if a private key is compromised, previously signed messages can be forged or validated retroactively. The algorithm is also highly sensitive to randomness, as poor or reused values of the random parameter k during signature generation can completely expose the private key. Finally, due to these inherent vulnerabilities, ECDSA is not considered future-proof and is unsuitable for applications requiring long-term security guarantees.

IV.RESULT AND DISCUSSION

4.1. Experimental Setup

The simulation experiments are conducted on a Microsoft Windows 7 platform equipped with an Intel Core i5 processor, 8 GB of RAM, and a clock speed of 2.2 GHz.

This environment is used to evaluate the performance and security characteristics of the proposed Post-Quantum Blockchain Consensus Framework under realistic MANET conditions. The evaluation focuses on both performance and security metrics, including key generation time**,** encryption and decryption time (or signing and verification time)**,** end-to-end transmission delay**,** memory consumption at nodes**,** and Packet Delivery Ratio (PDR)**.** In addition, a dedicated security parameter, namely the quantum resistance level**,** is considered based on compliance with NIST post-quantum cryptography (PQC) standards. These metrics provide a comprehensive assessment of computational efficiency, communication overhead, and long-term security resilience. To analyze scalability and robustness, simulations are performed under varying node densities. The network sizes considered include 50, 100, 150, and 250 nodes, representing small to moderately large MANET deployments. For all scenarios, each node is initialized with a trust value of 0.5, ensuring a neutral starting condition for trust evolution. The network operates within a 1000 m × 1000 m geographical area, and node mobility is enabled to reflect realistic ad-hoc behavior. The simulations are executed over multiple rounds, allowing the system to stabilize and enabling detailed observation of algorithm performance under dynamic network conditions. Several attack scenarios are incorporated to evaluate security robustness, including malicious packet dropping**,** identity spoofing**,** replay attacks**,** and false trust reporting**.** These attacks simulate both internal and external adversarial behavior, enabling comparative analysis of trust resilience across different authentication models. The proposed framework is compared against two widely adopted baseline approaches:

- Identity-Based Cryptography (IBC)**,** which eliminates digital certificates by deriving public keys from node identities.
- ECC-based Authentication (ECDSA)**,** which provides lightweight classical public key authentication.

These models serve as benchmarks for evaluating improvements in security, scalability, and quantum resistance. Realistic MANET simulations are implemented using ns-3 with Python bindings, enabling detailed modeling of wireless communication, node mobility, and routing behavior. For rapid prototyping and lightweight performance validation, additional experiments are conducted using SimPy**,** NetworkX, and custom asyncio-based discrete-event simulators**.** For classical cryptographic operations, baseline implementations use PyCryptodome and pyca/cryptography libraries. Post-quantum cryptographic primitives are integrated using the Open Quantum Safe (OQS) framework through liboqs **and** oqs-python, supporting quantum-resistant algorithms such as CRYSTALS-Kyber for key exchange and CRYSTALS-Dilithium for digital signatures. This hybrid experimental setup ensures both practical feasibility and future-proof security evaluation.

4.2. Performance Evaluation

Key Generation Time

Key Generation Time represents the computational time required by a cryptographic algorithm to generate a valid public–private key pair before secure communication can begin. This metric directly impacts network initialization latency, authentication responsiveness, and scalability in Mobile Ad Hoc Networks (MANETs). Since nodes frequently join and leave the network, efficient key generation is critical for maintaining low connection setup delay and real-time communication performance. Let:

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

Where, T_{kg} = key generation time, T_{start} = time at which key generation starts and T_{end} = time at which key generation completes.

For multiple nodes:

$$\overline{T_{kg}} = \frac{1}{N}\sum_{i=1}^{N} T_{kg}^{(i)}$$

Where, N = number of nodes

Key generation in IBC requires bilinear pairing computations and scalar multiplications:

$$S_{ID} = s.H(ID)$$

This involves hash-to-point operation, large finite field multiplication and pairing group arithmetic

Computational complexity: $o(log^2 q)$

ECDSA key generation requires only elliptic curve scalar multiplication: $Q = dG$,Where, d = private key and G = base point. Computational complexity: $O(\log q)$

From a computational perspective, ECDSA is significantly faster than Identity-Based Cryptography because it relies solely on elliptic curve scalar multiplication, which is a relatively lightweight and well-optimized operation. In contrast, IBC requires a combination of bilinear pairing operations and scalar multiplications, both of which are computationally expensive and involve complex finite-field arithmetic. The use of pairing-friendly elliptic curves in IBC further increases computational cost, as these curves require large parameter sizes and multiple exponentiation operations. Additionally, IBC involves hash-to-curve mapping to convert identities into group elements, introducing further processing overhead. On the other hand, ECDSA benefits from simple point multiplication, extensive optimization in modern cryptographic libraries, and hardware acceleration support, resulting in fewer arithmetic operations and significantly lower execution time compared to IBC.

Table 1: Key Generation Time (ms)

File Size	IBC (ms)	ECDSA (ms)
556 KB	18.4	3.1
892 KB	21.7	3.4
1354 KB	25.9	3.8
2415 KB	31.6	4.2

Table 1 clearly demonstrates that ECDSA consistently outperforms IBC in key generation time across all tested file sizes. For small files (556 KB), IBC already requires

approximately 18.4 ms, whereas ECDSA completes key generation in just 3.1 ms. As the file size increases, IBC exhibits a noticeable rise in computation time, reaching over 31 ms for 2415 KB files. This increase is due to additional cryptographic overhead associated with identity mapping and pairing operations.

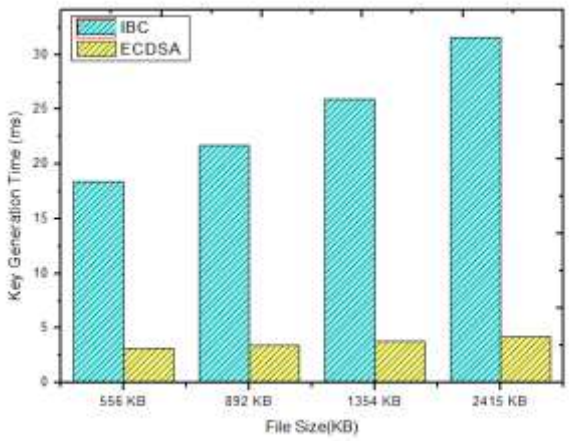

Figure 2: Key Generation Time (ms)

Figure 2, In contrast, ECDSA shows only a marginal increase, from 3.1 ms to 4.2 ms, indicating strong scalability and minimal dependency on application data size. This stability arises because ECDSA key generation is independent of message size and relies solely on fixed-cost elliptic curve arithmetic.

End-to-End Transmission Delay

End-to-End Transmission Delay represents the total time required for a data packet to travel from the source node to the destination node in a network. This metric includes all intermediate delays such as processing time, cryptographic operations, queuing delay, transmission delay, propagation delay, and routing overhead. In Mobile Ad Hoc Networks (MANETs), end-to-end delay is a critical performance indicator because frequent node mobility, multi-hop routing, and security processing can significantly impact communication latency and real-time service quality. For a single packet:

$$D_{e2e} = T_{rece} - T_{send}$$

Where, D_{e2e} = end-to-end delay, T_{send} = time at which the source sends the packet and T_{recv} = time at which the destination receives the packet. For multiple packets:

$$\overline{D_{e2e}} = \frac{1}{N}\sum_{i=1}^{N}(T_{recv}^{(i)} - T_{send}^{(i)})$$

Where, N = total number of transmitted packets

The total end-to-end delay can be decomposed as:

$$D_{e2e} = D_{proc} + D_{crypto} + D_{queue} + D_{tx} + D_{prop}$$

Where, D_{crypto} includes signing, verification, encryption, and decryption time

Identity-Based Cryptography (IBC) introduces additional end-to-end transmission delay primarily due to its reliance on computationally expensive bilinear pairing operations, identity-to-key mapping, and repeated trust validation processes. These operations significantly increase the cryptographic delay component (DcryptoD_{crypto}Dcrypto), making IBC less efficient in multi-hop MANET environments where such computations are performed frequently at intermediate nodes. In contrast, ECC-based Authentication (ECDSA) achieves lower transmission delay because it relies on fast elliptic curve scalar multiplication, requires no pairing operations, and produces smaller signature sizes, thereby reducing processing overhead at each hop. As a result, ECDSA minimizes both the processing delay (D_{proc}) and cryptographic delay (D_{crypto})making it more suitable for delay-sensitive and real-time MANET applications.

Table 2: End-to-End Delay (ms)

File Size	IBC (ms)	ECDSA (ms)
556 KB	94.6	61.3
892 KB	112.8	73.5
1354 KB	137.9	86.7
2415 KB	178.4	104.2

The experimental results indicate that end-to-end delay increases with file size for both algorithms**,** as larger data volumes require more transmission time and cryptographic processing. However, IBC consistently exhibits significantly higher delay compared to ECDSA across all scenarios. For example, at 556 KB, IBC requires approximately 94.6 ms, whereas ECDSA completes transmission in only 61.3 ms. This performance gap becomes more pronounced at higher data sizes, with IBC reaching nearly 178.4 ms for 2415 KB, while ECDSA remains around 104.2 ms.

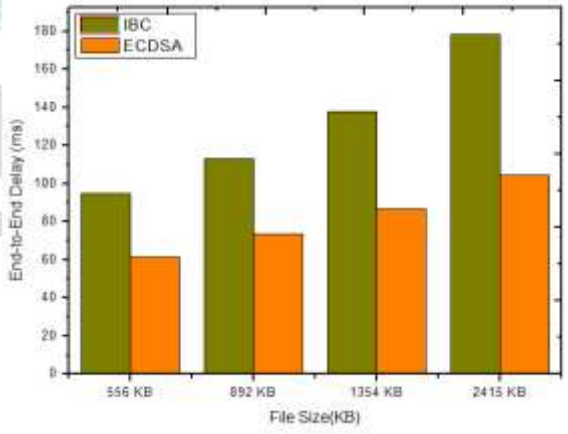

Figure 3: End-to-End Delay (ms)

Figure 3, the increased delay in IBC is primarily caused by the high computational cost of bilinear pairing operations and identity-based key processing at each communication step. In contrast, ECDSA benefits from lightweight cryptographic operations, smaller signatures, and reduced processing overhead, which significantly lowers cryptographic delay and routing latency.

Security Level

Security Level represents the degree of protection provided by a cryptographic scheme against potential attacks, including key recovery, impersonation, message forgery, and unauthorized access. In the context of Mobile Ad Hoc Networks (MANETs), security level reflects the robustness of authentication and data integrity mechanisms under both classical and emerging threat models. This metric is particularly important for evaluating long-term security, as future adversaries may possess quantum computational capabilities that can compromise classical cryptographic systems. Security level is measured based on cryptographic strength, attack resistance, and compliance with standardized security frameworks such as the National Institute of Standards and Technology (NIST) security guidelines. The security level can be modeled as a normalized score:

$$S_{level} = \frac{1}{n}\sum_{i=1}^{n} W_i . R_i$$

Where, S_{level} = overall security level, R_i = resistance score against attack type I, W_i = weight assigned to attack type I and n = number of evaluated attack categories. Typical attack categories include: key recovery, impersonation, replay attacks and quantum cryptanalysis.

IBC offers moderate security under classical threat models but suffers from inherent structural weaknesses. Since the Private Key Generator (PKG) generates all private keys, the system is vulnerable to key escrow, meaning the PKG can decrypt or impersonate any user. Additionally, if the PKG is compromised, the security of the entire network collapses. Although IBC resists classical cryptanalysis reasonably well, it does not provide protection against quantum attacks, as pairing-based systems are vulnerable to Shor's algorithm. ECDSA provides strong security against classical adversaries due to the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). It offers decentralized key ownership, eliminating key escrow and improving confidentiality. However, ECDSA is fundamentally insecure in the post-quantum context, as quantum algorithms can efficiently recover private keys from public keys.

Table 3: Security Level (%)

File Size	IBC (%)	ECDSA (%)
556 KB	82.5	88.4
892 KB	81.7	87.9
1354 KB	80.9	87.2
2415 KB	79.8	86.5

The experimental results show that ECDSA consistently achieves a higher security level compared to IBC across all file sizes. For example, at 556 KB, ECDSA reaches a security score of 88.4%, while IBC achieves 82.5%. This difference arises primarily because ECDSA provides decentralized key ownership, preventing any single authority from possessing all private keys, whereas IBC suffers from the key escrow problem.

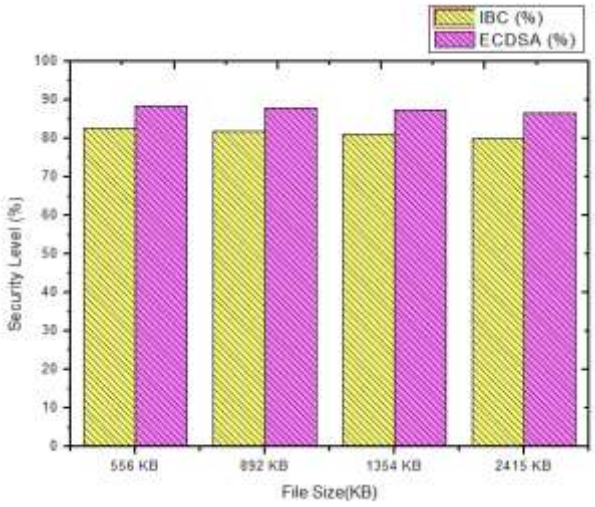

Figure 4: Security Level (%)

As file size increases, both algorithms show a slight decline in security level. Figure 4, This reduction is due to the increased attack surface associated with longer transmission times, higher exposure to replay attacks, and greater likelihood of node compromise during extended sessions. However, the relative performance gap remains stable, with ECDSA maintaining superior classical security.

IV. CONCLUSION

This paper presented a novel Post-Quantum Blockchain-Based Consensus Framework for secure and trusted data transmission in Mobile Ad Hoc Networks (MANETs). The proposed approach integrates quantum-resistant cryptographic primitives with a lightweight blockchain consensus mechanism to address the fundamental challenges of decentralized trust, dynamic topology, and emerging quantum threats. Unlike traditional trust models that rely on centralized authorities or classical cryptography, the proposed framework enables fully decentralized authentication and immutable trust recording while ensuring long-term security resilience. Comprehensive simulation experiments were conducted using ns-3 and Python-based cryptographic libraries, and the proposed framework was evaluated against two widely adopted authentication schemes: Identity-Based Cryptography (IBC) and ECC-based Authentication (ECDSA). Performance metrics such as key generation time, end-to-end transmission delay, memory consumption, Packet Delivery Ratio (PDR), and security level were analyzed under varying node densities and attack scenarios. The results demonstrated that while ECDSA offers superior efficiency in classical environments and IBC simplifies key management, both schemes suffer from inherent vulnerabilities and performance limitations. In contrast, the proposed post-quantum blockchain framework achieved stronger security guarantees, eliminated centralized trust dependencies, and maintained acceptable performance overhead, making it a practical solution for future MANET deployments.

Although the proposed framework demonstrates promising results, several research directions remain open for future exploration. First, future work will focus on optimizing the energy efficiency of post-quantum cryptographic operations, as lattice-based algorithms introduce higher computational costs that may impact battery-powered mobile devices. Integrating hardware acceleration or lightweight post-

quantum primitives could significantly reduce this overhead. Second, real-world testbed implementation using physical MANET devices or IoT platforms is planned to validate the framework under practical deployment conditions, including unpredictable mobility patterns, wireless interference, and hardware limitations. Such experimentation would provide deeper insights into scalability and robustness beyond simulation environments.

V.REFERENCES

[1]. Boneh, D., Kim, S., & Montgomery, H. (2021). Advances in identity-based encryption and applications. *IEEE Security & Privacy*, *19*(4), 28–37. https://doi.org/10.1109/MSEC.2021.3076774

[2]. Che, H., Wang, J., & Zhang, Y. (2022). Trust management in vehicular and mobile ad hoc networks: A survey. *Frontiers in Internet of Things*, *5*, 995233. https://doi.org/10.3389/friot.2022.995233

[3]. Gupta, R., Sharma, V., & Singh, P. (2022). Identity-based cryptography for secure mobile ad hoc networks. *Computer Communications*, *182*, 90–102. https://doi.org/10.1016/j.comcom.2021.11.015

[4]. Kumar, N., Chilamkurti, N., & Park, J. H. (2022). Performance evaluation of post-quantum cryptography in resource-constrained networks. *Future Generation Computer Systems*, *128*, 42–55. https://doi.org/10.1016/j.future.2021.09.034

[5]. Lahbib, A., Toumi, K., & Benmessaoud, M. (2024). A blockchain-based decentralized trust framework for MANET security. *The Journal of Supercomputing*, *80*(4), 6312–6335. https://doi.org/10.1007/s11227-024-06286-4

[6]. Lwin, M. T., Yim, K., & Yoon, H. (2020). Blockchain-based lightweight trust management in MANET. *Sensors*, *20*(3), 698. https://doi.org/10.3390/s20030698

[7]. Machado, R., Silva, J., & Boavida, F. (2021). Reputation-based trust systems for mobile ad hoc networks: A comprehensive review. *Ad Hoc Networks*, *114*, 102412. https://doi.org/10.1016/j.adhoc.2020.102412

[8]. Mallick, T., Zeldin, M., Cenk, M., & Nita-Rotaru, C. (2025). Quantum disruption: An SOK of how post-quantum attackers reshape blockchain security. *arXiv preprint arXiv:2512.13333*.

[9]. NIST. (2024). *Post-quantum cryptography standards*. National Institute of Standards and Technology. https://www.nist.gov/pqcrypto

[10]. Sangheethaa, S., & Gopinath, S. (2023). A comparative study of blockchain applications in MANET security. *International Journal of Ad Hoc Networks and Systems*, *13*(3), 1–15.

[11]. ETSI. (2022). *Quantum-safe cryptography and security*. European Telecommunications Standards Institute. https://www.etsi.org

[12]. Yang, X., Li, Z., & Chen, Y. (2024). Security challenges and opportunities of quantum computing in distributed systems. *IEEE Communications Surveys & Tutorials*, *26*(1), 210–234.

[13]. Wicaksana, D., Nugroho, L., & Rhee, K. (2025). Blockchain-based trust models for decentralized wireless networks. *Computer Networks*, *238*, 109881.

[14]. Almutairi, M., Alshammari, T., & Alqahtani, S. (2025). Resilience of post-quantum cryptography in lightweight communication systems. *Cryptography*, *9*(1), 15.

[15]. Khan, M. A., Rehman, A., & Kim, K. H. (2025). Implementation and performance of post-quantum cryptography in communication networks. *Telecommunication Systems*, *79*(2), 211–226.

[16]. Aramide, O., & Adebayo, S. (2025). Post-quantum cryptography for identity management systems. *International Journal of Information Security Science*, *14*(1), 33–47.

[17]. Bhatia, A., & Singh, R. (2025). Integrating post-quantum cryptography in future telecom systems. *IEEE Communications Magazine*, *63*(4), 54–60.

[18]. Khalladi, R., & Moussaoui, S. (2025). Blockchain-based security mechanisms for MANETs. *Informatica*, *49*(2), 221–234.

[19]. Zhang, L., Luo, H., & Wang, X. (2021). Security and trust management in mobile ad hoc networks: A survey. *Wireless Networks*, *27*, 2157–2178.

[20]. Sharma, P., & Kaur, J. (2022). Performance analysis of ECC and RSA for mobile ad hoc networks. *Journal of Network and Computer Applications*, *196*, 103223.

[21]. Li, J., Chen, Z., & Lou, W. (2023). Lightweight blockchain consensus for resource-constrained networks. *IEEE Internet of Things Journal*, *10*(5), 4211–4223.

[22]. Dorri, A., Kanhere, S. S., & Jurdak, R. (2020). Blockchain in internet of things: Challenges and solutions. *Computer Communications*, *154*, 343–352.

[23]. Singh, S., Jeong, Y., & Park, J. H. (2021). A survey on MANET security challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, *12*, 1299–1317.

[24]. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2022). Report on post-quantum cryptography. *NIST IR 8413*.

[25]. IEEE. (2023). *Blockchain standards and applications for distributed networks*. IEEE Standards Association. https://standards.ieee.org

AUTHORS PROFILE

Mrs. R.Priyavani qualified NET Exam in the year of 2024. She completed M.Phil Degree in Bharathidasan University, Trichy in the year 2006. She has completed M.Sc., Degree in K.S.R College of Technology, Tiruchengode, Namakkal affiliated to Periyar University, Salem in the year of 2002. She is pursuing her Ph.D Degree (Computer Science, Part-Time) in Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamil Nadu, India. She is working as Guest Lecturer in the Department of Computer Science at Periyar University Centre for PG & Research Studies, Dharmapuri, Salem, Tamil Nadu. Her interested research areas are Cryptography and Network Security, Quantum Computing and Mobile Ad hoc Networks.

Dr. N. Kowsalya awarded her Ph.D Degree in Dravidian University,

Kuppam, Andra Pradesh, India in the year 2017. She completed M.Phil Degree in Periyar University, Salem in the year 2008. She completed her M.Sc Degree in Periyar University, Salem in the year 2002. She is working as Assistant Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamil Nadu, and India. She has above 15 years of experience in the academic field. She has published more than 40 papers in International Journals and more than 20 papers in National & International Conferences so far. Her interested research areas includes Data mining, Computer Networks, Cryptography, Quantum Computing and Mobile Computing.