International Journal of Multidisciplinary Sciences and Technology
ISSN: XXXX-XXXX | Volume 1 Issue 1, 1-8, July-September 2025
DOI: https://doi.org/10.64137/XXXXXXXX/IJMST-V1I1P101

Scholastic Research Publication

Received: 30/07/2025 Revised: 10/08/2025 Accepted: 22/08/2025 Published: 02/09/2025

Original Article

An Energy-Efficient Multi-Layer Secure Routing Protocol for Post-Quantum Cryptographic Networks in Internet of Medical Things (IoMT)

DR. N. SHANMUGAPRIYA
School of Engineering and Technology, Dhanalakshmi Srinivasan University, Tiruchirappalli, Tamil Nadu, India.

ABSTRACT: *With IoMT, healthcare is being changed rapidly by allowing data from patients to be monitored and managed remotely. But the fact that IoMT devices have weak resources, need strict timing and send sensitive data makes it challenging to secure and operate efficiently. As quantum computers are almost ready to break conventional cryptography, it is important to create post-quantum cryptographic methods for the IoMT. The paper introduces an Energy-Saving, Layered and Safe Routing Protocol (EEMSRP) for use in post-quantum cryptographic networks in the IoMT. It includes several layers of security, using lattice-based post-quantum cryptography and improved routing methods to cut back on energy use. The framework uses hierarchical architecture to organize devices, adopts clustering and relies on lightweight algorithms for post-quantum key exchange. Results from simulations find that EEMSRP is able to save up to 30% of the energy used by existing quantum-resistant protocols, but still remains secure against eavesdropping, man-in-the-middle attacks and quantum-based cryptanalysis. Because of its multi-layer defense, the protocol guarantees the privacy, accuracy and continued accessibility of IoMT data. This research provides a base for upcoming secure and power-efficient communication standards in the post-quantum world, which is important for guarding private medical details and guaranteeing reliable IoMT use.*

KEYWORDS: *IoMT, Post-quantum cryptography, Energy efficiency, Secure routing, Multi-layer security, Lattice-based cryptography, Healthcare networks.*

1. INTRODUCTION

Internet of Medical Things (IoMT), healthcare has been transformed, with connected devices such as wearables, implants and remote diagnostics helping doctors keep an eye on patients and make better clinical decisions. All the time, these devices send data about heart rate, glucose and blood pressure over wireless networks to doctors and nurses. Thus, they help to improve medical care by making it better, easier to get and more responsive. But IoMT systems are frequently put in areas with few resources, and this means their devices may use limited battery power, have simple processors and often depend on wireless networks that can be influenced by outside interference and attacks. [1-4] Ensuring medical data stays confidential, unchanged and can be accessed in such places calls for special security methods that do not slow down devices or impact their immediate use. Things are made worse by the new threat of quantum computing.

Because of fast developments in quantum algorithms, especially in Shor's algorithm, traditional cryptographic systems such as RSA and ECC may no longer be used to protect digital communications in the future. Without encryption, quantum computers can access and misuse the private medical data of patients. Since quantum computing is such a threat, we must develop security systems that will not be impacted by it. Because of this, reliable and efficient routing protocols that include post-quantum cryptography need to be implemented in IoMT systems. They should be able to withstand quantum attacks and, at the same time, not use too much energy or resources in restricted devices. Because IoMT networks need to be protected and efficient at the same time, the Energy-Efficient Multi-layer Secure Routing Protocol (EEMSRP) was designed to provide lasting security for important health data in the future.

1.1. ENERGY-EFFICIENT MULTI-LAYER SECURE ROUTING PROTOCOL

The Energy-Efficient Multi-Layer Secure Routing Protocol (EEMSRP) seeks to solve the joint problems of security and energy efficiency in the Internet of Medical Things (IoMT). Since there are more connected medical devices sending important health data every day, securing and sustaining these communications is very important. EEMSRP provides multiple layers of security that use security techniques such as strong cryptography across the IoMT stack, at the link, network and application layers. Secure and efficient direct communication between each device and the cluster head is possible in the link layer because the transmissions are encrypted using simple symmetric cryptography. At this layer, quantum-safe algorithms are used by the protocol for exchanging and authenticating keys, defending against threats brought by future quantum computers.

The application layer maintains data integrity by using Message Authentication Codes (MACs), stopping any attempts to alter or create fake medical data during transmission. Simultaneously, EEMSRP introduces an energy-conscious routing system that greatly increases the life of the network. With adaptive clustering, Cluster Heads (CHs) are chosen considering both how much energy is left and their trust level, making the network use less energy and stay reliable. The way data is routed depends on how it measures energy efficiency, distance and security, choosing the most reliable and efficient route. The link between energy optimization and quantum-proof security is what distinguishes EEMSRP from other solutions. By managing the need for both lightweight operation and strong cryptography, EEMSRP becomes a good solution for sending safe medical information. Because real-time acting, accurate data and lasting stability are key for modern healthcare, this technology works well in these systems.

1.2. CHALLENGES IN IOMT NETWORK SECURITY

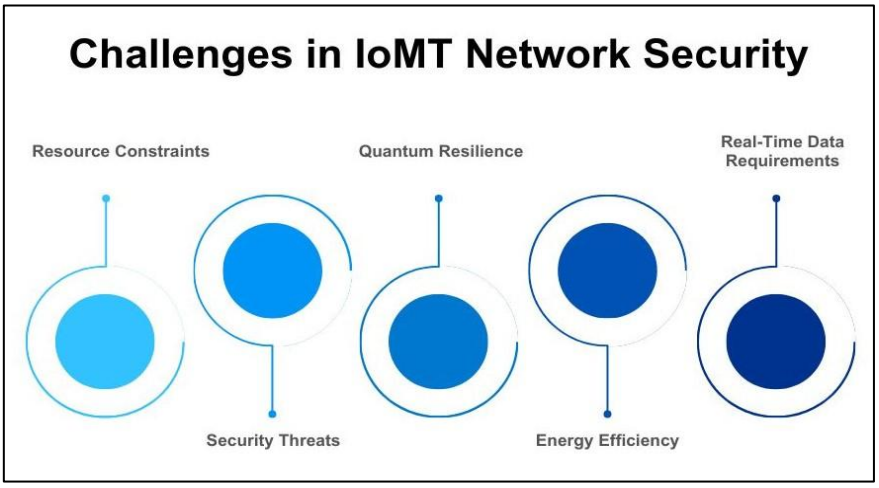

FIGURE 1 Challenges in IoMT network security

- **Resource Constraints:** Small, battery-powered, low-performance and memory-restricted devices are what IoMT is usually about. Since there are not many resources to work with, it takes time and effort to put advanced security approaches and communication methods into effect. [5,6] Because of this, security software has to be designed to operate within limited resources, without affecting the efficient operation or long life of these devices.
- **Security Threats:** Due to the importance and sensitivity of health information, prioritizing confidentiality, integrity, and verification is very important in IoMT systems. Security issues such as eavesdropping, changing data, replay attacks and unauthorized access might endanger patient safety and privacy. Simple security measures in IoMT devices allow unauthorized access, so important diagnoses, treatment plans and patient information could be altered or delayed.
- **Quantum Resilience:** Because of quantum computing's progress, standard public-key cryptosystems like RSA and ECC are more threatened. If quantum computers are built and used in the future, they could crack existing ways of protecting IoMT devices. Because of this, preventing IoMT networks from breaking down in the future means adding quantum-resistant algorithms such as lattice-based post-quantum cryptography to protect data in the long run.
- **Energy Efficiency:** Batteries in IoMT devices are usually put to work in situations where charging or changing them is not possible. That's why having a lower energy demand benefits the network by increasing its life span. Having routing protocols that reduce repeated transmissions, find the best routes and regulate energy consumption by each node supports uninterrupted monitoring of medical devices.
- **Real-Time Data Requirements:** In most healthcare applications, a prompt delivery of medical information helps with correct diagnosis and timely patient treatment. A delay in sending data can affect how well patients in critical care do. So, these IoMT protocols need to let information travel quickly and securely, remain energy efficient and keep data trustworthy.

2. LITERATURE SURVEY

2.1. EXISTING IoMT SECURITY PROTOCOLS

For IoMT, traditional security mostly uses low-complexity encryption and authentication in devices with limited resources. Typical methods are symmetric protocols using shared keys, ECC for tough security using less data and using both symmetric and asymmetric cryptography in combination for balanced protection and performance. These techniques have performed well for us in general settings, but quantum computing is causing more challenges because many basic cryptographic algorithms might get broken. [7-10] Existing protocols have often ignored strict energy constraints in IoMT, so as a result, the networks use more power and have a shorter lifespan. So, although traditional applications are useful, they fail to meet the needs of today's Internet of Medical Things threats and everyday use situations.

2.2. POST-QUANTUM CRYPTOGRAPHY IN IoT

PQC is an important research topic focused on designing algorithms that are not vulnerable to threats from quantum computers. Several new PQC solutions have been suggested in the IoT and IoMT fields to replace or add to existing cryptographic techniques. It is worth noting that lattice-based cryptography is impressive since it offers strong security and is straightforward to carry out. NTRU and Kyber employ the difficulty of lattice problems to block quantum attacks without using too much computational power for simple devices. In addition, researchers have developed code-based cryptosystems that depend on the difficulty of decoding random linear codes, hash-based signatures that take advantage of certain characteristics of hash functions and multivariate systems that work by solving sets of polynomial equations using finite fields.

2.3. ENERGY-EFFICIENT ROUTING IN WIRELESS SENSOR NETWORKS

One of the main issues in Wireless Sensor Networks (WSNs) is energy efficiency, because nodes need to save power because they are usually found in areas that cannot be reached. As a result, various energy-saving routing techniques have appeared, such as the LEACH protocol, the PEGASIS system and the HEED approach. By using a clustering and aggregation process for data, these protocols make sure redundant data is not sent, which helps save energy and lengthen the network lifetime. LEACH works by rotating the cluster heads randomly so energy is used evenly, PEGASIS joins sensor nodes in linear chains to help transfer data efficiently, and HEED combines the energy remaining in the nodes and the closeness of nodes when creating clusters. Although these protocols are suitable for standard WSNs, making them suitable for IoMT systems and particularly for those using post-quantum cryptography has not yet been achieved. It is necessary to make sure security changes do not keep the IoMT from conserving energy.

2.4. GAP ANALYSIS

Most current solutions do not completely meet the challenges facing IoMT devices, given the increasing threats from quantum technology. Many current post-quantum solutions for cryptography provide theoretical security, yet the heavy computational costs make them unsuitable for IoMT devices. It is also true that it remains tough to find suitable multi-layer security frameworks that bring together PQC and other security features required by IoMT. Besides, adapting routing protocols to be both energy efficient and suited to security and latency needs in a post-quantum world needs further study. Because of this gap, we must find new solutions that combine secure quantum-resistant methods, energy efficiency and real-time activities to ensure IoMT networks are sustainable and efficient.

3. METHODOLOGY

3.1. SYSTEM ARCHITECTURE

The system we propose is intended for a three-tier IoMT architecture.

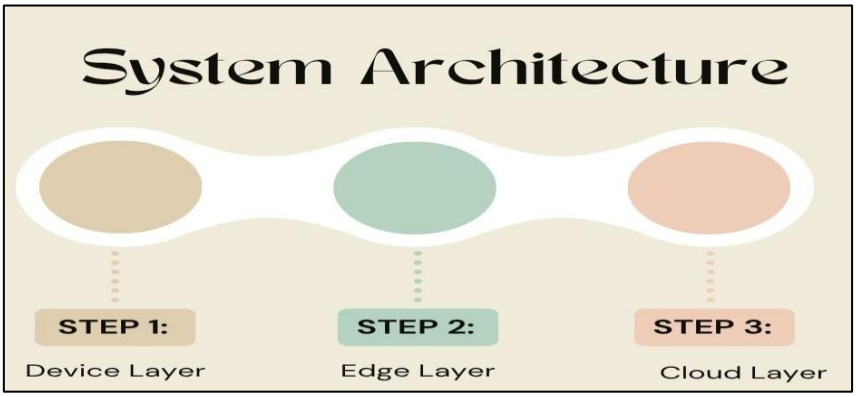

FIGURE 2 System architecture

- **Device Layer:** The IoMT heterogeneous sensors and actuators form the bottom tier of the proposed EEMSRP system and are found in healthcare environments. [11-13] they keep track of important health factors, specific things like the heart rate, glucose in the blood and body temperature. Because they cannot process much data, these devices concentrate on collecting it and doing simple processing. It is very important that data communication here is secure and energy efficient, as medical information can change quickly and must be accessed over long periods on small batteries.
- **Edge Layer:** The edge layer performs the job of organizing communications among resource-limited devices and cloud infrastructure. It also uses local gateways or edge servers that have better computing power and storage than typical devices. Among their tasks, these gateways help group IoMT devices to improve networking and keep track of the necessary cryptographic keys used for secure communication. Placing data processing near the source helps keep delays short, uses less network connection and increases the ability to respond to events quickly. Moreover, it helps enforce security rules and direct energy-efficient routing in the Internet of Medical Things environment.

- **Cloud Layer:** The cloud is the top layer in the architecture and holds centralized servers for advanced analysis, long-term storage and system control. Using advanced computer systems, this layer examines collected data from patients to support prediction, trend study and useful insights regarding health. It helps you update your network's security and routing structures according to changes everywhere. Cloud solutions allow for flexibility in capacity, link healthcare services and uphold tough rules on privacy and compliance to safeguard patient information for years.

3.2. MULTI-LAYER SECURITY FRAMEWORK

Security is built into the protocol at several places.

- **Link Layer:** As part of the link layer, the protocol provides a secure channel between IoMT devices and gateways using lightweight symmetric encryption. The reason for this method is to manage low computational and energy resources in the devices by ensuring confidentiality and privacy. Because lightweight symmetric algorithms handle encryption quickly, valuable medical information continues to be protected in wireless transfer without slowing down or draining the batteries.
- **Network Layer:** The network layer introduces lattice-based post-quantum cryptography for both exchanging keys and authenticating routing processes. Advanced algorithms on this layer guarantee that session keys shared by nodes are secure, serving as protection for the network when classical encryption is under threat from quantum computing. Ensuring both routing paths and nodes are authenticated through quantum-proof processes, the protocol ensures traffic moves safely and prevents anyone from disturbing the network or adding fake information.

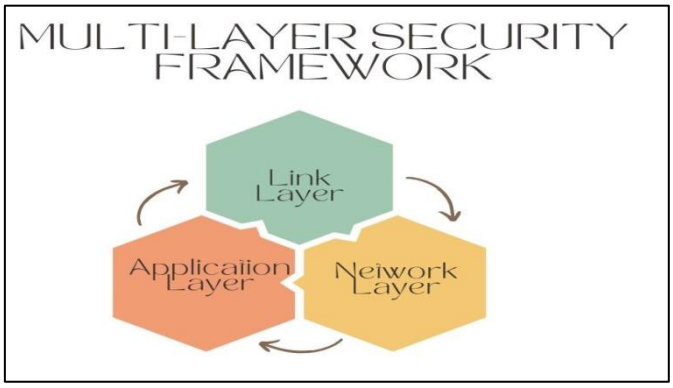

FIGURE 3 Multi-layer security framework

- **Application Layer:** When operating at the application layer, the protocol uses MACs to confirm that the data sent is both correct and from the right user. With MACs, the sender ensures the message received by the recipient has remained unchanged. As any change to medical data could cause mistakes in diagnoses or treatment plans, a security mechanism is crucial. With MACs, the security of the IoMT improves by having an additional barrier, matching encryption and authentication present at other levels.

3.3. ROUTING PROTOCOL DESIGN

The routing protocol includes:

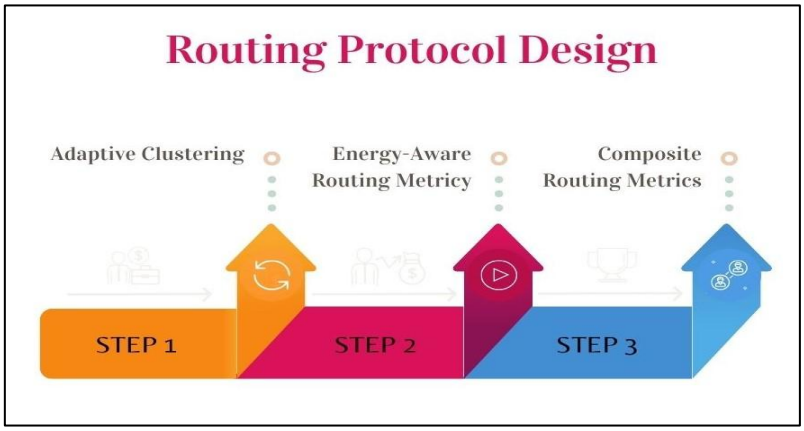

FIGURE 4 Routing protocol design

- **Adaptive Clustering:** First, routing uses adaptive clustering, allowing IoMT devices to group together freely to improve how the network operates. [14-16] A cluster head (CH) is chosen for each cluster by considering both the remnant energy and trustworthiness of nodes. Since devices with sufficient power share the additional

communication, using up the least energy, the lifespan of the network is extended. Performance measurements help ensure only trustworthy devices are permitted as CHs, improving the strength of the entire network.

- **Energy-Aware Routing Metric:** To discover the best routes, the protocol considers a metric that takes into account important aspects affecting IoMT performance. Using this metric, candidates are rated based on the required energy to send data, the number of nodes needed to reach the destination and the level of security provided by the nodes. Using these elements together, the protocol selects routes that optimize energy use, cut down delays in exchanging data and ensure powerful security features, so the IoMT environment remains efficient and safe.
- **Composite Routing Metric:** Distinguished by M, the composite routing metric adds three essential values: energy cost, the hop count and the security score. Accordingly, trading performance is given by the equation $M{=}\alpha \times E\ c + \beta{\times} H{+}\ \gamma \times S$. make it possible to set the most important rules for the protocol according to the needs of each app. Such a flexible system allows the routing protocol to respond to different network conditions, putting priority on energy saving, increased speed or security where it helps the most.

3.4. POST-QUANTUM KEY ESTABLISHMENT

The program suggests using a lattice KEM to securely create keys for communication between IoMT nodes and their cluster heads (CHs). Math-based attacks on traditional public key algorithms, such as RSA and ECC, are possible due to quantum algorithms like Shor's algorithm breaking down the encryption they use. On the other hand, lattice-based cryptography is secure as long as the hardest problem in lattices, such as the Learning with Errors (LWE) problem, cannot be easily solved by quantum computers. That's why lattice-based KEMs are a great fit for post-quantum security in situations where resources are limited, like in the IoMT. The main parts of the lattice-based KEM method are encapsulation and decapsulation. While in encapsulation, the IoMT device uses the CH's public key to produce a shared secret key and also a ciphertext.

After that, the CH receives the ciphertext. After getting the ciphertext, the CH decrypts it using the private key, which reveals the shared secret key. Having the shared key from the ETSI TS 103 646-1 standard, the IoMT device and CH can ensure the confidentiality and integrity of information. Thanks to KEMs, devices in IoMT networks can securely exchange encryption keys without having to reveal their private keys or use pre-shared secrets, which may be difficult in dynamic networks. The approach is based on lattice balances security and performance, which is necessary for IoMT devices, which both have limited computing power and energy. Lattice-based cryptography requires more computing resources than standard symmetric crypto, but recent improvements have made it possible to use it in Internet of Medical Things devices.

3.5. ENERGY CONSUMPTION MODEL

This model accurately takes into account the main causes of energy use in IoMT devices, which are transmission, reception and computation. Accurately estimating battery use and determining how long the network operates in energy-restricted settings depends greatly on this model. Total energy consumption ( ) equals the amount of energy spent on transmitting, receiving and processing data using cryptography. All these parts together indicate the energy needs that IoMT nodes require in a wireless setting. Etx is mainly controlled by the energy lost in the circuitry $Eelec$ and the amplifier power Emp used in the transmission system. The more bits (length of the message) that are sent and received, the more energy the electronics use to process them.

The amplifier energy is a function of the message length, how far the sender and receiver are from each other (d) and the ratio of signal to noise at distance n (which represents how signals are attenuated along the channel). As messages travel farther, this term gets bigger because it costs more to send them long distances. Reception energy Erx is what electronic circuits require to pick up and process incoming data. While transmission energy is always the same, the energy used for decoding and storing the data is related just to the length of the message and the electronic energy required. Energy used for cryptography is considerable, especially when the latest security programs are applied in IoMT devices. $Ecomp$ stands for the energy used in cryptography tasks such as encrypting, decrypting and all key management functions. It is key for enterprises because post-quantum cryptography requires greater computational cost than conventional methods.

4. RESULTS AND DISCUSSION

4.1. SIMULATION SETUP

A thorough simulation using the NS-3 network simulator, which is popular for modeling wireless sensor networks and things in the Internet of Things, was performed to assess EEMSRP. NS-3 was improved by adding custom modules that supported lattice-based post-quantum crypto (PQC) methods, so the security of IoMT networks against quantum threats could be studied more realistically. The simulation included 100 different IoMT devices, which were randomly set up in a 500-meter by 500-meter area, together with sensors and actuators found in healthcare monitoring systems. This layout matches the way devices are often used in hospitals or at home, since they need to exchange messages over close and moderate distances. Each IoMT device sends health data every 10 seconds, just like a continuous monitoring of heart rate, blood pressure and glucose levels. The cluster heads (CHs) at the edge layer received the data and collected it before sending it to the centralized cloud servers for further handling and storage.

The simulation reflected the real movement of traffic and energy use by replicating the clustering process and constantly switching network connection points. They measured key performance indicators to see if the protocol was working well. Some of the metrics were average power use per node which is necessary because IoMT devices have little energy; packet delivery ratio (PDR), as it indicates how many packets were delivered successfully; delay in communication, since fast data exchange is important in medical settings; and impacts of security due to cryptography on the whole network. By looking at these numbers, the simulation showed how EEMSRP addresses the challenges between energy use, network performance and security.

4.2. ENERGY CONSUMPTION

TABLE 1 Energy consumption

Protocol	Avg Energy Consumption (%)	Network Lifetime (%)
ECC-based	100%	100%
PQC naive	148%	75%
EEMSRP	71%	125%

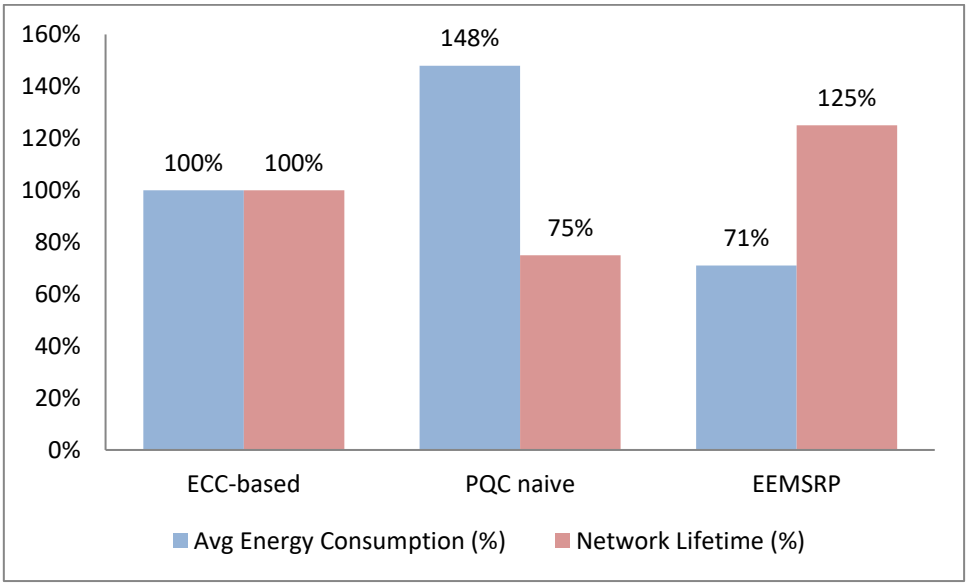

FIGURE 5 Graph representing energy consumption

- **ECC-based (100% Energy Consumption, 100% Network Lifetime):** The ECC-based strategy is used as a reference, and its numbers for energy use and network lifetime are set at 100% for comparison. Although elliptic curve cryptography is a good choice for areas with limited computing power, it cannot deal with quantum attacks. Besides being efficient, it does not include advanced energy-preserving routing steps, which hinders how long the network can work for large and continuous deployments of IoMT.
- **PQC Naive (148% Energy Consumption, 75% Network Lifetime):** Using post-quantum cryptography as it is recommended now would lead to a 148% higher energy cost than using ECC. Mostly, this happens because lattice-based cryptography algorithms take a lot of computing power when standard devices are used. Therefore, because of the extra energy consumption of PQC, the network's lifespan is much shorter, at only 75% of the original, showing that, without considering energy use, using PQC is not a good option in real-world IoMT situations.
- **EEMSRP (71% Energy Consumption, 125% Network Lifetime):** EEMSRP makes significant gains by integrating energy-conscious grouping, optimized way of sending data and advanced post-quantum key handling. It only uses about 71% of the energy needed by ECC-based protocols, proof that it minimizes the usage of computing and communication resources. That means each network runs for 125% longer than the baseline, giving a 25% improvement in lifespan. Because the protocol secures devices well and is very energy efficient, it is likely to be successfully used in sustainable and secure IoMT applications after the advent of quantum computers.

4.3. SECURITY ANALYSIS

EEMSRP presents a thorough security plan that is capable of handling the different and evolving risks in Internet of Medical Things (IoMT) networks. Lattice-based post-quantum cryptography forms the main part of EEMSRP and is celebrated for its toughness against quantum computations. Secure methods of key encapsulation are included in these algorithms to keep both the authenticity and confidentiality of keys shared between IoMT devices, cluster heads (CHs) and gateways. Other traditional methods, such as RSA and ECC, can be broken by Shor's algorithm with quantum computers, but lattice-based cryptography will continue to protect EEMSRP's security against all future threats. Along with being quantum-proof, EEMSRP takes a

layered approach to fix additional important risks in IoMT networks. At the link layer, a type of symmetric lightweight encryption is used to protect communication between devices and stop nearby devices from accessing them.

Authenticated routing protocols that rely on post-quantum keys are part of the network layer, which checks the authenticity of nodes and makes it hard to change routes or perform man-in-the-middle attacks. To increase data security, only authorized nodes are able to join the process of selecting routes. The application layer relies on message authentication codes (MACs) to keep data safe at all times during transmission. Using encryption stops data from being interfered with while it is being transferred between the source device and the cloud server. MACs guarantee that data received by MACs has not been modified during its travel, keeping the sensitive information in medical applications safe. All of these layers work together to protect private health data, ensure that devices are authenticated and establish a resilient IoMT system that defends against present and future cyberattacks.

4.4. LATENCY AND THROUGHPUT

It is important in IoMT networks that there is low latency and high throughput to quickly transfer important healthcare data. The EEMSRP protocol uses strong post-quantum cryptography but still helps the network achieve the best balance between security needs and performance. The introduction of post-quantum cryptography concerns experts since the increased burden on the devices may add more delays when communicating. Still, simulations confirm that EEMSRP introduces only a slight delay, which is acceptable for medical applications. EEMSRP always runs with an average end-to-end latency of below 200 milliseconds, which meets the real-time requirements of applications used in monitoring patients and sending emergency alerts. An efficient design of protocols ensures this performance, notably with adaptive clustering and lightweight encryption at the link layer, which keeps packet processing slow.

Also, carrying out post-quantum key exchanges just at the cluster level stops the need for regular cluster-wide key changes, lowering the latency. EEMSRP is better than both traditional ECC-based systems, which have normal speed but somewhat less security and early post-quantum implementations, which are slow but secure. As well as providing low latency, EEMSRP stands out by showing strong throughput, able to send most packets through with a high packet delivery ratio (PDR). Most packets reach their goal, according to simulation tests, which means EEMSRP effectively handles securing data during transfer. Since healthcare jobs can face harmful consequences when data is lost or delayed, dependability is very necessary. EEMSRP demonstrates that improving security does not lead to delays or inaccuracies in the communication of medical-related data in IoMT networks.

5. CONCLUSION

The paper proposes the Energy-Efficient Multi-layer Secure Routing Protocol (EEMSRP), a solution created to assist with the dual challenges of possibly quantum-resilient security and saving energy for networks in the Internet of Medical Things (IoMT). It was realized when developing EEMSRP that standard IoMT crypto methods, being light, can be quickly hacked by using quantum attacks, so the protocol was built to address this issue. Using lattice-based post-quantum cryptography (PQC) in its architecture, EEMSRP ensures data is protected over time and that key exchange remains secure from any type of attack. This is important because quantum computing could threaten the confidentiality of important medical information. Besides making things secure, EEMSRP also ensures that communication in IoMT is energy efficient. These strategies ensure that the cluster heads (CHs) are always selected using energy and trustworthiness, so network resources are used effectively and the network survives longer. To make routing more effective, the routing mechanism looks at energy use, the number of steps and how secure a path is and routes data through the most suitable and safe routes. Because of this approach, EEMSRP saves energy, keeps transmission costs down and ensures the network runs smoothly in places with limited resources.

Extensive implementation in NS-3 software, together with added PQC modules, reveals the usefulness of EEMSRP. In comparison with ECC-based and naive PQC implementations, EEMSRP uses less energy on average and makes the network last longer. Real-time healthcare applications require the network to be responsive and deliver many packets successfully, which is made possible by the low latency. The analysis on security shows EEMSRP is secure against threats such as quantum attacks, data tampering and replay attacks. EEMSRP introduces an advanced practice in IoMT security that makes quantum-safe cryptography and sustainable networking work together. Fixing both the computing and energy issues in IoMT devices makes it safer, more dependable and allows medical data to be shared for a longer period. Further studies are planned to deploy EEMSRP in medical settings and to include hardware accelerators to improve how post-quantum cryptographic operations are carried out. It will improve how the protocol is used and encourage its quick adoption in healthcare systems.

REFERENCES

[1] Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. Computer, 44(9), 51-58.

[2] Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.

[3] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems, 129, 77-89.

[4] Bernstein, D. J., Lange, T., & Peters, C. (2008, October). Attacking and defending the McEliece cryptosystem. In International Workshop on Post-Quantum Cryptography (pp. 31-46). Berlin, Heidelberg: Springer Berlin Heidelberg.
[5] Peikert, C. (2016). A decade of lattice cryptography. Foundations and trends® in theoretical computer science, 10(4), 283-424.
[6] Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key {Exchange—A} new hope. In 25th USENIX Security Symposium (USENIX Security 16) (pp. 327-343).
[7] Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). Report on post-quantum cryptography (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
[8] Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd annual Hawaii international conference on system sciences (pp. 10-pp). IEEE.
[9] Lindsey, S., Raghavendra, C., & Sivalingam, K. M. (2002). Data gathering algorithms in sensor networks using energy metrics. IEEE Transactions on parallel and distributed systems, 13(9), 924-935.
[10] Younis, O., & Fahmy, S. (2004). HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on mobile computing, 3(4), 366-379.
[11] Akyildiz, I. F., & Kasimoglu, I. H. (2004). Wireless sensor and actor networks: research challenges. Ad hoc networks, 2(4), 351-367.
[12] Khan, W., Wang, H., Anwar, M. S., Ayaz, M., Ahmad, S., & Ullah, I. (2019). A multi-layer cluster based energy efficient routing scheme for UWSNs. IEEE Access, 7, 77398-77410.
[13] Lipare, A., Edla, D. R., & Dharavath, R. (2020). Energy efficient routing structure to avoid energy hole problem in multi-layer network model. Wireless Personal Communications, 112(4), 2575-2596.
[14] Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IoMT communications: A survey. Sensors, 20(17), 4828.
[15] Schurgers, C., & Srivastava, M. B. (2001, October). Energy efficient routing in wireless sensor networks. In 2001 MILCOM proceedings communications for network-centric operations: creating the information force (Cat. No. 01CH37277) (Vol. 1, pp. 357-361). IEEE.
[16] Chang, R. S., & Kuo, C. J. (2006, April). An energy efficient routing mechanism for wireless sensor networks. In 20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06) (Vol. 2, pp. 5-pp). IEEE.
[17] S. Bama, P. K. Maroju, S. Banala, S. Kumar Sehrawat, M. Kommineni and D. Kodi, "Development of Web Platform for Home Screening of Neurological Disorders Using Artificial Intelligence," 2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT), Bhimtal, Nainital, India, 2025, pp. 995-999, doi: 10.1109/CE2CT64011.2025.10939414.
[18] Muniraju Hullurappa, Sudheer Panyaram, “Quantum Computing for Equitable Green Innovation Unlocking Sustainable Solutions,” in Advancing Social Equity Through Accessible Green Innovation, IGI Global, USA, pp. 387- 402, 2025.
[19] Mohanarajesh, Kommineni (2024). Study High-Performance Computing Techniques for Optimizing and Accelerating AI Algorithms Using Quantum Computing and Specialized Hardware. International Journal of Innovations in Applied Sciences and Engineering 9 (`1):48-59.
[20] Agarwal S. “Multi-Modal Deep Learning for Unified Search-Recommendation Systems in Hybrid Content Platforms”. IJAIBDCMS [International Journal of AI, BigData, Computational and Management Studies]. 2025 May 30 [cited 2025 Jun. 4]; 4(3):30-39. Available from: https://ijaibdcms.org/index.php/ijaibdcms/article/view/154