Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Wireless Sensor Network security enhancement using quantum key distribution of Elliptic Curve Cryptography

[1]M. Kavitha, [2]Dr. Y. Kalpana

[1]*Research scholar, VELS Institute of Science, Technology & Advanced studies (VISTAS) (Deemed to the university Esta-u/s 3 of the UGC Act, 1956) velan Nagar, P.V. Vaithiyalingam Road, Pallavaram -600117,Chennai, Chengalpattu District, Tamilnadu, India. E-mail: Kavithamp83@gmail.com Orcid id: https://orcid.org/0009-0008-8024-6620*

[2]*Research Supervisor, VELS Institute of Science, Technology & Advanced studies (VISTAS) (Deemed to the university Esta-u/s 3 of the UGC Act, 1956) velan Nagar, P.V. Vaithiyalingam Road, Pallavaram -600117,Chennai, Chengalpattu District, Tamilnadu, India. E-mail: ykalpanaravi@gmail.com Orcid id: https://orcid.org/0000-0001-8080-4575*

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

Wireless sensor networks (WSNs) are quiet dynamic technology made up of discrete multi-function sensor nodes that interconnect wireless for short distances. WSNs have distinct traits as well as limitations that impede the development of efficient attack detection and prevention methods. Security in WSN is a more difficult task because of the processing limits of sensor nodes as well as the nature of wireless communications. The widespread WSNs usage has given development to several forms of threats. To guard against threats, appropriate security measures must be implemented. Cryptography, specifically encryption, plays a pivotal role in protecting data from unauthorized access. However, not all encryption methods are equally effective, as some exhibit vulnerabilities. Elliptic Curve Cryptography (ECC) is the most efficient option because of its reduced key size. Comprehensive safety despite lower key sizes leads to area as well as power efficient crypto systems. With recent technological advancements, traditional encryption no longer appears to be a safe solution for security and privacy of data. Quantum cryptography uses quantum physics processes to provide safe data transmission among sender and recipient. However, quantum cryptography comprises a revolution over network security field. Therefore, this research focuses on Quantum Key Distribution (QKD) with ECC for effective authentication, key management and energy conservation. Thus, the proposed QKD-ECC method is implemented and evaluated with traditional ECC and other cryptography method for better WSN security and privacy of data transmission.

Keywords: Network security, Wireless sensor networks, Elliptic Curve Cryptography, Quantum Key Distribution, Authentication.

INTRODUCTION

Sensor Nodes are located in a specific region to monitor environmental or physical factors in real-world like pressure, temperature, location, sound and motion [1]. It's commonly employed in military applications. In general, the surroundings is hostile or in a catastrophe zone. Efficiency and cybersecurity are critical components of this network architecture. This is owing to the unique characteristics of sensor nodes, which contrary to traditional local network components get restricted by battery life as well as capacity for resources like storage, elaboration and bandwidth. Consequently, novel Medium Access Control (MAC) protocols have considered into account the restrictions of each particular sensor over network are necessary [2, 3]. The existence of malicious nodes for sensor network causes a variety of security issues [4]. Trust can be described as the belief that a certain thing is sufficiently dependable not to cause damage or interfere with the seamless real-time application operations. It is critical in daily life and also when utilizing sensitive data [5]. Trust models comprise the techniques used to obtain trust data and determine the reliability of each node. The world's technology has developed rapidly, it has become dependent on open network systems. So the information transmitted between network users has become faster and required to utilize many different technologies namely authentication factors and cryptography through security. Moreover, the network channel used to protect the transmitted data for authenticated users as well as protected data

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

transmitted through online channels. Hence, the significant portion of WSNs must function constantly as well as consistent with no interruption. Thus, the security in WSNs is very challenging to implement.

Most of the research challenge in WSN involves self-management, energy, as well as hardware and software complexions, MAC layer issues, collecting and transmitting of data, decentralized management, deployment, multimedia communication, real-time operations and synchronization [3]. Because of the essential properties of SNs, security is an essential and critical concern. This research concentrates on security attacks in WSNs. SN s require minimal encryption for accomplishing security with high level. Every sensor ought to find a balance among cost, safety level and performance. There have been several threats and attacks to WSN including data loss, communication delay, service slowdown resulted to delays, and Denial of Service (DoS) [7, 8]. This insists the three major security properties to be considered are integrity, authentication and confidentiality. However, achieving all of these targets at once is quite challenging. In certain instances, developers forfeit security by implementing economical approaches that lack sufficient processes such as key distribution. A WSN necessitates more adaptable ways to distribute keys around the network. There can be two sorts of approaches namely with respect to the usage of asymmetric or symmetric cryptography, as well as advanced cryptography like ECC, RSA. These are well-known to use resources which are efficiently than the conventional public key method.

The ECC is a form of encryption that includes over the public key cryptography category. Its operation relies on algebraic elliptic curves structure formed within finite fields. Numerous studies propose the application of ECC in the Internet of Things (IoTs) industry including make the MQTT protocol more robust by reducing manipulation of data, eavesdropping, as well as replaying attacks [9,10]. The ECC algorithm emerged after RSA because of advances in processing capacity as well as complicated factorization techniques. As a result of these improvements, larger key sizes are used, making the ciphering or deciphering process as well as key generation method with more resource-intensive. It works as similar as traditional key that has ability to generate only weak random numbers, which are easily accessed by third parties. In addition, the power of the CPU as well as these keys is subject to novel attack pattern because they must be reprogrammed whenever novel methods of attack are employed. If the quantum computers eventually develop into potential and have ability to readily decrypt data stored in classical keys, rendering current classical encryption techniques insecure. To keep in advance, the usage of huge Asymmetric keys is required to store and distribute safely in symmetric keys. Thus, these all factors cause researchers to reconsider the cryptographic keys security. Quantum cryptography includes QKD protocols to secure private communications as well as algorithm of quantum to both symmetric as well as public key cryptography. There are certain quantum based technologies, such as quantum key distribution, are currently being developed and deployed. One distinguishing aspect of these kinds of systems has their capacity to identify all illegal monitoring of the private key, either deliberate or unintentional, using the concept of quantum mechanics. In particular, any kind of interference caused by the source or detector of quantum could breach the no-cloning of quantum theorem that prompts to alarm for alerting the attack from intruder [11]. QKD solves the challenges associated with cryptographic keys by utilizing quantum physics to transport data from one point to another. The QKD employs its own quantum channel for transmitting data from transmitter to receiver and even requires a public Communication link for performing post-processing. It includes a gateway that estimates the data quantity lost during acquisition. This research focuses on quantum mechanism with ECC method for enhancing the sensor node security in authentication for data transmission. Hence, the proposed QKD-ECC method has improved authentication in data transmission in WSN.

LITERATURE REVIEW

The advancement in quantum cryptography sector is considered in the literature review for concentrating QKD, cryptography with post-quantum and QKD integration towards optical networks. It gets endorsed to be typically quicker than triple DES is illustrated by Gaur et al. Moreover, the ECC encryption technique comprises of elliptic curve in which set of points get satisfy the mathematical equation. In ECC, the curve point has generated by multiply the curve point using other integer. The challenges might be handled by determining the latest point on the curve [12].

Dirks et al. investigated the practical viability of a Geostationary Earth Orbit QKD (GEOQKD) technique that utilizes the untrusted as well as trusted mode BBM92 protocols for accomplishing a maximum tolerable loss

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

as 41dB per channel using key rates 1.1bit/s with untrusted as well as 300bit/s in trusted mode. This study discusses about the design of realistic space segment as well as its architecture which allows the GEOQKD method for operating both trusted and untrusted settings with high targeting accuracy levels [13]. Williams et al. proposed a QKD algorithm have accomplished secured communication by encoding time-bins with correlated photon pairs. The protocol has been evaluated in a real-world environment for evidence that it could synchronize time as well as identify eavesdroppers [14]. Schimpf et al. have presented a work on employing a blinking-free polarization with entangled photon source pairs in accordance with GaAs QD to QKD. The paper considers the issue of entangled deterioration at higher temperatures as well as recommends operating the source for minimum 20 K as well as using a pulsed two-photon stimulation method for maintaining faithfulness for the Bell state [15]. Amer et al. have discussed about the quantum repeater performance in QKD grid networks with a limited trusted nodes. Moreover, t he analysis have finds limitations for such networks, especially in terms of successful probability in BSM as well as decoherence rate, and also recommends the usage of trustworthy nodes despite the optimal repeater technique [16]. Ding et al. have suggested a novel approach for optimizing the actual QKD method parameter based on the Random Forest (RF) technique. The suggested method is probably used in typical QKD networks as well as helps with the advancement of quantum communication methods [17].

The document "State-of-the-Art Survey of Quantum Cryptography" discusses the quantum cryptography significance in ensuring unconditional security in the transmission of confidential information in the era of quantum computing. It reviews various protocols such as QKD, direct communication of quantum secure, post-quantum cryptography and secure multiparty communication. The challenges of quantum communication, experimental work in quantum cryptography, and the shift to quantum cryptography from classical techniques are also highlighted. The document includes discussions on device-independent QKD, continuous-variable quantum cryptography, as well as various cryptographic protocols. The development of quantum-resistant cryptographic algorithms is highlighted as a crucial area of research [18]. "Secure Communication Through Quantum Channels: A Study of Quantum Communication and Quantum Cryptography" provides an outline of the recent research over quantum communication as well as quantum cryptography, exploring fundamental principles like QKD, digital signatures and teleportation. It reviews various implementations of physical quantum communication methods, their applications in secure transactions and military communications, and compares their security with traditional encryption techniques. The benefits about cryptography and quantum communication namely resistance to quantum computer threats, and unconditional security are highlighted [19].

Device-independent QKD (DI-QKD) has eliminates the normal dependency on hardware integrity as an evident in protocols such as BB84. This is due to the continually exists the possibility that gadgets will be corrupted or defective. DI-QKD seeks to give assurances of safety have independent in all defects present over devices employed. DI-QKD is a cryptographic technique that exclusively based on the data-theoretic or entanglement assisted characteristics of quantum devices. It has been explored promptly as a means of simplifying security assessments and decreasing dependency on preconceptions about quantum hardware development. Along with QKD, there are certain recommendations for investigating whether additional quantum resources like quantum communication and entanglement and has ability to improve both quantum cryptography as well as broader cryptographic features [20].

Algorithmic sequences of quantum cryptography have provided precise and comprehensive responds to the difficulties that encounters the industries and businesses. To address numerous unresolved security issues, Artificial Intelligence (AI), Deep Learning (DL) and Machine Learning (ML) based methods have been merged with quantum cryptography. These combinations of hybrid computational methods are necessary for generating self-tuning intelligent techniques that deliver optimal privacy and security for all data types. The find out has developed challenges that get the most essential international substances classification among the resulting quantum cryptography questions which challenges the sectors like banking, software, defense, stock market and finance industries through combining quantum cryptography with AI, DL and ML. Researchers and industrial experts have concentrated on developing certain scenarios is discussed in this study for data synchronization with cloud servers for various sectors like banking, engineering, finance, and medicine . The suggested approach is applied to several tenants like single, multi and cloud servers as well as database servers. This framework is

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

intended for four firms with 245 users, and also includes integration consistency concepts that are executed via salting approaches. In this experimental scenario, plain-text sizes are consider with range from 24 to 8248 for examining safe keys, generation of data distribution key, encryption process, and decryption process time transformations. Encryption time for key generation ranges from 2.323 ms to 8.727 ms at level 1 of quantum as well as 0.036 ms to 1.849 ms at level 2 of quantum. The encryption time for key generation varies from 2.153 ms to 19.480 ms at level 1 of quantum as well as 0.053 ms to 3.351 ms at level 2 of quantum [21].

RESEARCH GAP

The research gap highlights limitations in existing ECC-based approaches for WSNs particularly with respect to high computational delays, inefficient power consumption, poor bandwidth optimization, and network congestion. There are several researches are adequately addressing these ineffectiveness, avoidance of WSNs vulnerable for encryption attacking and not able to meet practical performance demands. This research seeks to bridge these gaps by introducing an enhanced authentication by QKD scheme with ECC. It integrates quantum mechanism with ECC as hybrid asymmetric cryptography may generate high secure, efficient solution tailored to WSNs.

RESEARCH METHODOLOGY

The research methodology introduced design and implementation of an enhanced authentication scheme by combining ECC with the concept of Elliptical Curve Triangulation (ECT) with QKD as public channel protocol for WSNs. Initially, a comprehensive analysis of traditional ECC techniques is utilized for identifying key inadequacy with respect to delay, network congestion, power consumption, and bandwidth usage. Moreover, the development of proposed scheme concentrates to minimize computational overhead as well as improving energy efficiency. However, there are current parametrization of Elliptic Curve (EC) is involved based on area of triangle formulae. Hence, every non-singular EC allows for such parametrization and it is utilized in this experimental research with quantum mechanism. There are two process of securing data transmission are encryption and decryption but in this experimental research, hybrid mechanism of ECC and quantum cryptography mechanism is involved. The overall cryptography workflow of proposed QKD-ECC method for WSN is shown in figure 1.

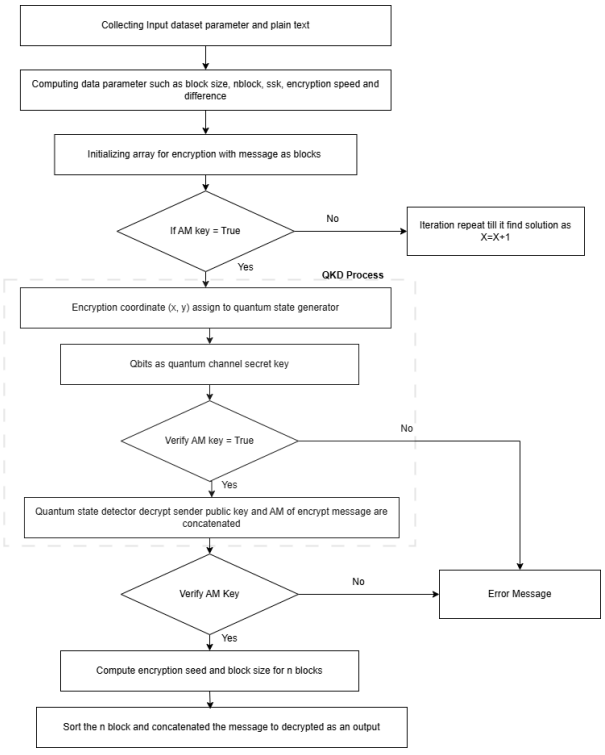

Figure 1 Workflow of hybrid cryptography method (QKD-ECC)

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

These combinations of hybrid computational methods are necessary for generating self-tuning intelligent techniques that deliver optimal privacy and security for all data types. The find out has developed challenges that get the most essential international substances classification among the resulting quantum cryptography questions which challenges the sectors like banking, software, defense, stock market and finance industries through combining quantum cryptography with AI, DL and ML. The proposed approach is a functional quantum encryption method that relies on flawless encryption techniques as well as truly arbitrary quantum keys. However, QKD is employed for particular contexts, such as local key distribution. Therefore, the evolution of QKD technology as well as cryptographic method persists with the objective of obtaining complete security, as demonstrated by rigorous security assessments as well as verification techniques. To improve cybersecurity, a hybrid strategy integrating classical as well as quantum cryptographic key exchange mechanisms is viewed as a viable alternative. At first, this study explains the QKD idea and the quantum mechanism in ETC enabling more secure cryptography in WSN.

QKD Principle

Quantum cryptography is frequently associated with just a few of specific protocols in the broader cryptography sector. Because of its crucial function in secure decoding, QKD is typically connected with encryption that is symmetrical techniques. In general, the quantum key obtained using QKD may be used as a session key in cryptosystems with symmetric like AES. The encrypted character of the quantum key over QKD improves the symmetric cryptosystem security by shielding it from potential quantum attackers. QKD technological advances are regarded as the foundation of quantum cryptography as well as quantum cybersecurity technology. QKD uses quantum mechanical features to facilitate the production of keys for secure communication among legitimate parties. This procedure makes redundant quantum assets such as preparation of quantum channel and measuring equipment (typically using polarization) and detectors on both Alice's as well as Bob's appliances. QKD necessitates certain fundamental presumptions concerning the devices utilized by the communication parties. There are two keys assumptions get critical.

1. The equipment utilized to generate and measure quantum states needs to be reliable. This is a fundamental need for any systems that interact with quantum channels with long-distance inclusive of techniques like scaling methods of quantum network as well as quantum teleportation and repeaters.
2. Detection of photon measurements have been utilized in BB84 protocol with cautious implementation are required that necessitate the robust artificial randomness security sources. Several proposals for the generation of random number with respect to quantum states have influence an essential possibility to enhance the security over context.

The procedure of QKD is as follows

- Key Generation processs: The cryptographic key is initiated in the process of key generation.
- Quantum Key process: Generating the raw quantum key process is basically assisted using the quantum mechanics principles.
- Key Refinement: The raw quantum key has been refined for ensuring its security that has involved both privacy amplification and error correction.
- Applying Authentication Mechanism: Implementation of authentication mechanisms has ensured that communication is valid and flawless.
- Security Measure: Due to highly sensitive of the refined key, an additional security layer has been applied for securing the context.
- Symmetric Key derivation: The ultimate symmetric key has obtained from the refine quantum key and it gets utilized to encrypt.
- Final Encryption: Data encryption that is based on symmetric keys is traditional. The technique establishes a secure channel of communication.

The QKD protocol consists of several steps beginning with the qubits generation as well as progressing to their evaluation and comparison from legitimate users. The procedure additionally incorporates error detection in data reconciliation, which results in the secret key generation. The quantum mechanism principle serve as the foundation for QKD, making it intrinsically secure toward threats from dominant quantum computers. While

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

traditional methods like RSA are prone to quantum computing attacks, QKD maintains secured in these settings. QKD allows two valid users to safely exchange keys. Usually, both parties employ a communication channel and pre-shared authentication key for ensuring the basic security in transmission of each quantum packet. This procedure have produces a raw quantum cryptography key. This key is enhanced through additional traditional processing to generate a single that is data-theoretically secure. The QKD security has stems from its capacity for recognizing and reacting to eavesdrop initiatives as the quantum particles state changes if interfered with assuring that solely authorized users may generate the ultimate secure key.

Elliptic Curve Triangulation

The non singular elliptic curve that allowed for certain parametrization with rational point is illustrated in equation 3.1.

$$y^2 = x(x - r1)(x - r2) \tag{3.1}$$

Area S of triangle include side "a, b, c" considered in the elliptic curve is illustrated in equation 3.2.

$$S = \sqrt{sp(sp - a)(sp - b)(sp - c)} \tag{3.2}$$

The semi-perimeter sp is represented as formulae in equation 3.3

$$sp = \frac{a+b+c}{2} \tag{3.3}$$

Figure 2 illustrate the parameter T that introduced and illustrated in equation 3.4

$$T = \frac{sp-a}{sp} \tag{3.4}$$

Simplify by dividing S^2 by sp^2 in elliptic curve is represented in equation 3.5

$$y^2 = x[x^2 + Ax + B] = x(x - r1)(x - r2) \tag{3.5}$$

We have for coordinates (x, y) of a point on elliptic curve shown in equation 3.6

$$\begin{cases} x = tbc = \frac{p-a}{p}bc \\ y = \frac{S_{abc}}{p^2} \end{cases} \tag{3.6}$$

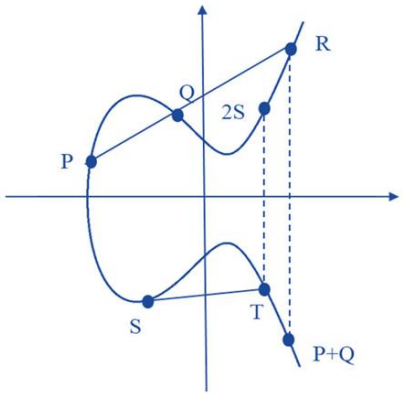

Figure 2 Elliptic curve Triangulation

Elliptic curve roots, coefficients and triangle sides are related through is represented in .equation 3.7

$$\begin{cases} r1r2 = B = (a - b)(a - c) \\ r1 + r2 = -A = 2bc - a(b + c) \end{cases} \tag{3.7}$$

This represents the triangle rational sides and area S whereas the rational points on the curve with coordinates (x, y) are available in equation 3.6. Let we initiate the triangle with rational sides by expressing side b and c functions

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of curve coefficients A and B that keep side a of triangle (a,b,c) as free parameter. Based on the first equation from equation 3.7 assist in determining root and curve coefficients derived is shown in equation 3.8.

$$\begin{cases} b = \frac{A-ac}{a-2c} \\ b + c = \frac{A-2c^2}{a-2c} \end{cases} \quad (3.8)$$

Moreover, second equation of equation 3.7 is used to find the equation for c is shown in equation 3.9.

$$ac^2 + c\big(A - 2(a^2 - B)\big) - a(A + B) = 0 \quad (3.9)$$

For discriminant D, the equation 3.10 is formulated as

$$D = (A + 2B)^2 + (2a)^2(1 - 2A - 3B) \quad (3.10)$$

Hence, the side C formulated is shown in equation 3.11

$$C = \frac{2a^2-2B-A\pm\sqrt{D}}{2a} = f\big(a, D(A,B)\big) \quad (3.11)$$

Similarly, the side b is formulated as shown in equation 3.12

$$b = \frac{A-ac}{a-2c} = g\big(a, D(A,B)\big) \quad (3.12)$$

Thus, the term A and B is expressed with respect to triangle side (a, b, c) and obtain the following for the discriminant D is shown in equation 3.13

$$D = 4a^3(b + c) - 8a^4 + 7a^2(b^2 + c^2) - 20a^2bc + 4a^2 - 12a(b + c) + 16bc \quad (3.13)$$

Given side a is rational and D is a square of integer or rational number, sides c and b will be rational too, thereby giving us triangle △(a,b,c) with rational sides.

Algorithm of QKD-ECC method

- Key generation and raw quantum key
- Implementing AM
- Verifying AM

Enhanced authentication of encryption process

Key generation with quantum key

Entity P is linked to a specific elliptic curve set of domain parameters as *D = (a, b, n, D, G, l, FR),* where *E* (F_{qf}) denotes the elliptic curve *E* in the quantum finite field F_{qf} with prime order *l.* Point P then follows these steps.

Step 1: Selection of value to *d in the* range [1, n−1].
Step 2: Computing S=dP_k,

Where,

P_k= private key

S = public key

Improved Nonce Management

- Use a secure random number generator to ensure the nonce *k* is unique and unpredictable for each signing operation.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Consider using a deterministic approach (like RFC 6979) where k is generated based on the private key and the message hash:

Compute $k = HMAC_K(H(m)) \bmod n$, where K is derived from the private key.

Key generation of AM in encryption process

The domain parameters Q, entity P *and* message m are defined as Q= *(FR, a, b, n, D, G, q)*
Steps required to be considered for entity P

Step 1: Selection of k value from the range [1, $n-1$].
Step 2: Computing $K_P = (X_1, Y_1)$, $g = X_1 \bmod n$. When $g = 0$, return to Step 1.
Step 3: Calculae $k^{-1} \bmod n$.
Step 4: Computing $s = k^{-1}(Q(m) + dg) \bmod n$; when h=0, return to Step 1.

The integer pair (g, h) generates the authentication for the message m.

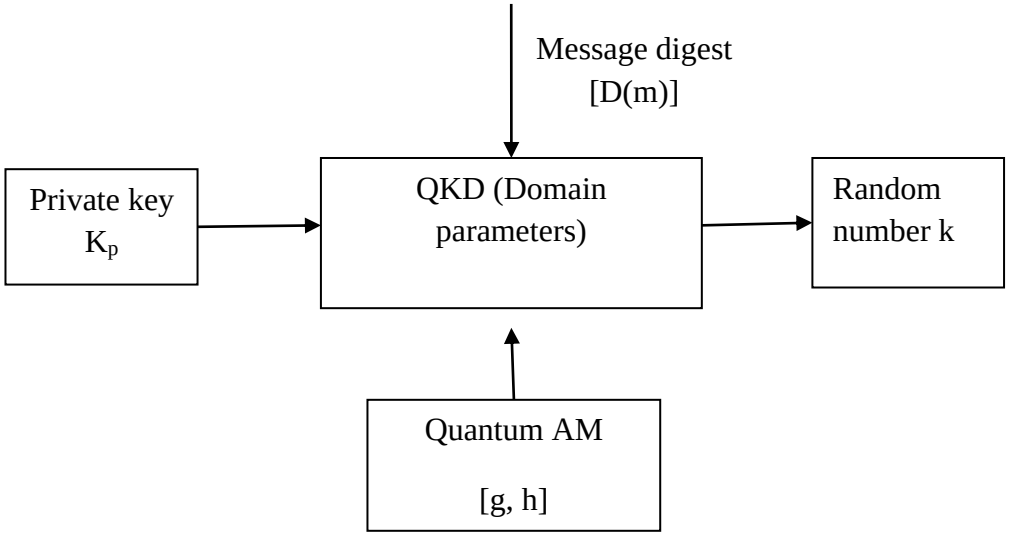

Figure 3 Generation of Quantum AM

Quantum AM of decryption process

Verifying AM key (g, h) for message (m) using entity P 's signature, entity R will utilize the public key S as well as domain parameters D = *(FR, b, a, h, n, G)*. The verification process is as follows:

Step 1: Ensure that the values g, h are within the range [1, $n-1$].

Step 2: Compute $\omega = h^{-1} \bmod n$, $D(m)$.

Step 3: Calculate $u_1 = D(m).\omega \bmod n$.

Step 4: Calculate $u_1 = g \,.\, \omega \bmod n$.

Step 5: Determine the point $(X_0, Y_0) = u_1 P_k + u_2 S$ and compute $v = X_0, \bmod n$.

If $v = g$, authentication key get accepted as valid.

1. Given multiple signatures $\sigma_i = (g_i, h_i)$ messages m_i:
   - Compute:

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

$$\omega_i = h_i^{-1} mod\ n$$

$$u_{1i} = D(m_i)\ \omega_i mod\ n$$

$$u_{2i} = g_i \omega_i mod\ n$$

2. Compute the aggregated elliptic curve point:

$$V = \sum_{i=1}^{m} (u_{1i} G + u_{2i} S)$$

3. Verify by checking:

$$r' = x_V \bmod n$$

If $g' = g_i$ for all authentication key and get valid.

Multi-Signature Schemes

- Implement a multi-signature scheme where a message must be signed by t out of n participants.
- The aggregate signature can be constructed as:

$$h = \sum_{j=1}^{t} h_j \bmod n$$

- Each participant computes their own signature, and a final verification can check if:

$$g' = x_V \bmod n$$

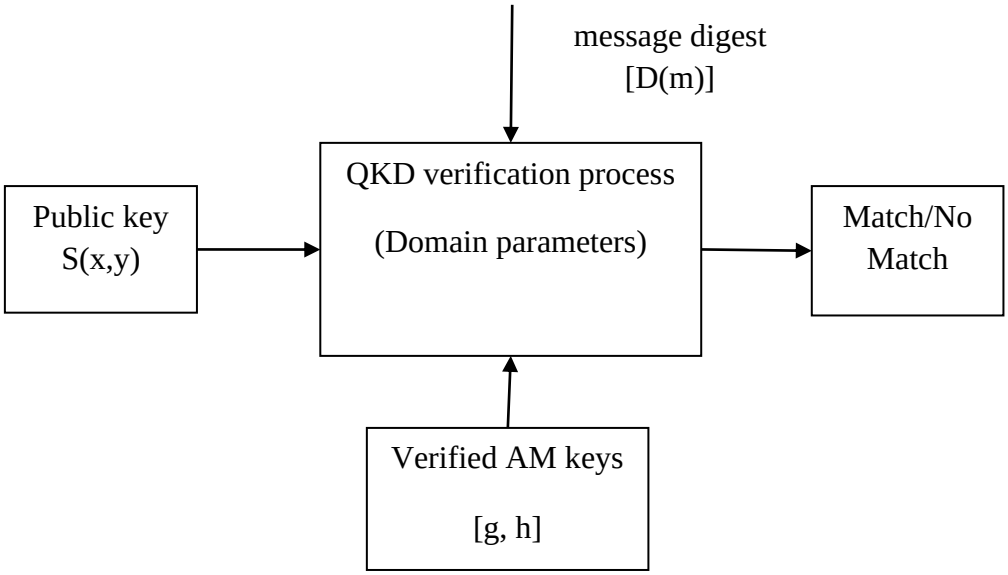

Figure 4 Enhanced authentication Digital Signature Verification

Result and Discussion

The NS3 network simulator was used to evaluate the EAECC technique within IEEE 802.15.4 Zigbee networks, focusing on key metrics: encryption and decryption time, throughput, and energy consumption. The results confirmed EAECC's performance advantage over RSA and Sengupta's technique, particularly in throughput and congestion management. EAECC optimizes both security and efficiency, with strong throughput and minimal encryption and decryption time consumption that making it a suitable choice for secure and high-performance communication in IEEE 802.15.4 networks.

Throughput Performance

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

QKD-ECC has consistently achieved higher throughput than RSA and EAECC method that calculated as the data size divided by the total time for encryption and decryption. This improvement was evident across various data sizes (115 to 1150 bytes), highlighting QKD-ECC ability has efficiently handle larger data packets without sacrificing speed.

$$\text{Total throughput} = \frac{\text{Data size (bytes)}}{\text{Time taken for encryption and decryption process (S)}}$$

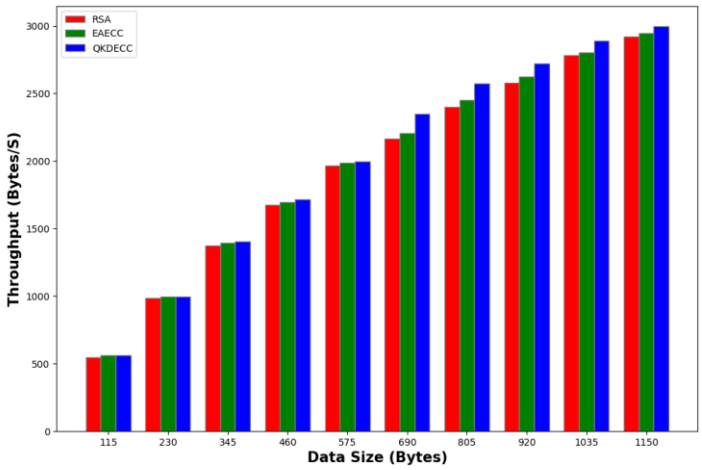

Figure 5 Throughput comparison of QKD-ECC with other cryptography technique

Figure 5 shows a comparison of throughput (in bytes per second) for proposed QKD-ECC with other cryptography technique such as EAECC and RSA across different data sizes. QKD-ECC consistently outperforms than other two methods, particularly as data size grows indicating higher efficiency in data transmission with very minimum loss of packets.

Encryption and Decryption performance

QKD-ECC demonstrated lower encryption and decryption times compared to the other techniques. This reduction translates into lower computational demand which is crucial for power-constrained networks like Zigbee, and ensures the network's overall efficiency.

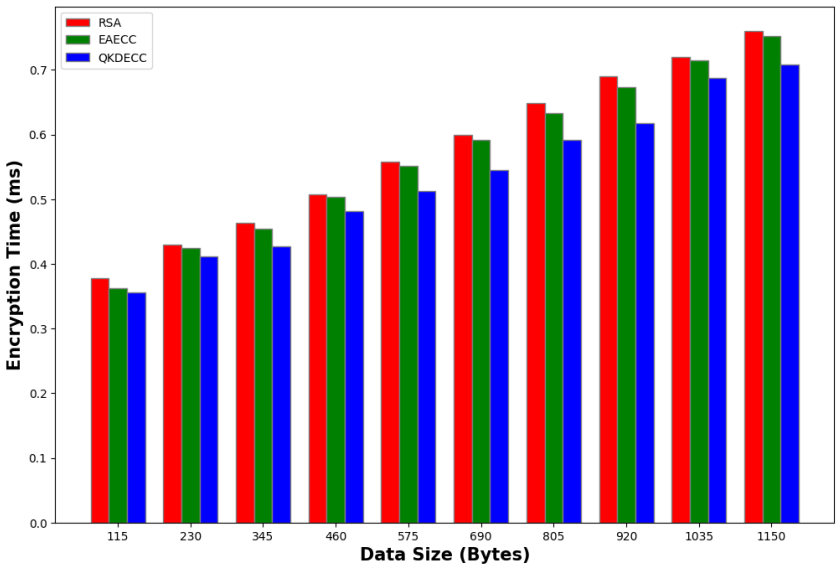

Figure 6 Encryption time comparison of QKD-ECC other cryptography techniques

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 6 illustrates the encryption time of proposed QKD-ECC with existing EAECC and RSA in which encryption time consumed for all data sizes are very low in QKD-ECC while compared to other existing EAECC and RSA. Hence, the safer data transmission is done with less time consumption.

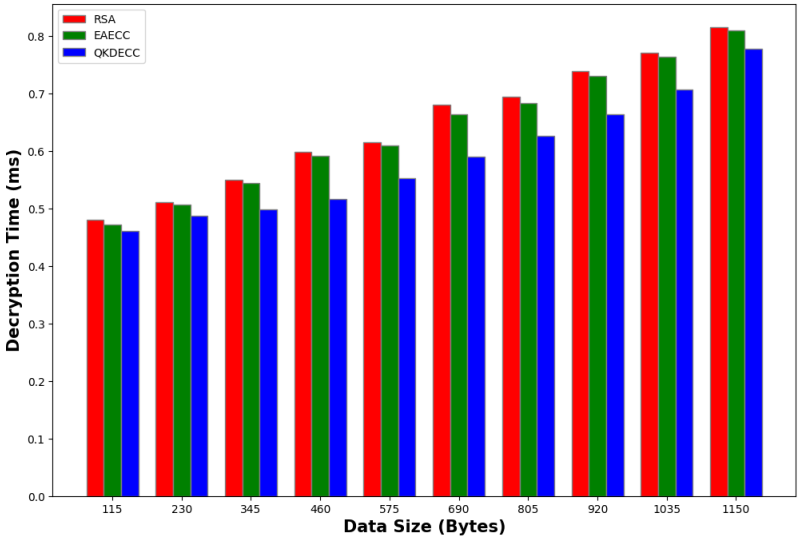

Figure 7 Decryption time comparison of QKD-ECC other cryptography techniques

Figure 7 illustrates the decryption time of proposed QKDECC with existing EAECC and RSA in which decryption time consumed for all data sizes are very low in QKD-ECC while compared to other existing EAECC and RSA. Hence, the safer data transmission is done with less time consumption.

CONCLUSION

This experimental research has undergone through the notable advancements achieved using raw quantum key secure with ECC whereas the proposed QKD-ECC method utilizes improvement in throughput, encryption and decryption time effectively in WSNs. The result of QKD-ECC method determines that data transmission is more with throughput while compare to other cryptography method as well as encryption and decryption time is less while compare to other cryptography method such as EAECC and RSA. Thus, the robust solutions are not only bolsters security but also meets the operational demands of resource constrained environments. Moreover, the future work has focused on integrating ML techniques and classifiers to further enhance model performance. Leveraging data-driven approaches allows for the optimization of security mechanisms, adaptive management of network resources, and improvement of overall efficiency in WSN deployments.

REFERENCE

[1] Cao, C., Tang, Y., Huang, D., Gan, W., & Zhang, C. (2021). IIBE: an improved identity-based encryption algorithm for WSN security. Security and Communication Networks, 2021.

[2] Afroz, F.; Braun, R. Energy-efficient MAC protocols for wireless sensor networks: A survey. Int. J. Sens. Netw. 2020, 32, 150–173.

[3] Samara, G. Wireless Sensor Network MAC Energy-efficiency Protocols: A Survey. In Proceedings of the 2020 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28–30 November 2020; pp. 1–5.

[4] Singh, S., & Saini, H. S. (2021). Learning-based security technique for selective forwarding attack in clustered WSN. Wireless Personal Communications, 118(1), 789-814.

[5] Mehmood, G., Khan, M. Z., Waheed, A., Zareei, M., & Mohamed, E. M. (2020). A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks. IEEE Access, 8, 131397-131413.

[6] Qichen, W. (2022, April). Research progress on wireless sensor network (WSN) security technology. In Journal of Physics: Conference Series (Vol. 2256, No. 1, p. 012043). IOP Publishing.

Research Article

[7] Azzedin, F.; Albinali, H. Security in Internet of Things: RPL Attacks Taxonomy. In Proceedings of the 5th International Conference on Future Networks & Distributed Systems, Dubai, United Arab Emirates, 15–16 December 2021; pp. 820–825.

[8] Khanam, S.; Ahmedy, I.B.; Idris, M.Y.I.; Jaward, M.H.; Sabri, A.Q.B.M. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access 2020, 8, 219709–219743. [CrossRef]

[9] De Rango, F.; Potrino, G.; Tropea, M.; Fazio, P. Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. Pervasive Mob. Comput. 2020, 61, 101105.

[10] De Rango, F.; Tropea, M.; Fazio, P. Mitigating DoS attacks in IoT EDGE Layer to preserve QoS topics and nodes' energy. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer CommunicationsWorkshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6-9 July 2020; pp. 842–847.

[11] Lusnig, L., Sagingalieva, A., Surmach, M., Protasevich, T., Michiu, O., McLoughlin, J., & Cavalli, F. (2024). Hybrid quantum image classification and federated learning for hepatic steatosis diagnosis. Retrieved from NCBI.

[12] J.D. Gaur, A.K. Singh, N.P. Singh, March). Comparative study on different encryption and decryption algorithm, in: 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, 2021, pp. 903–908.

[13] B. Dirks, I. Ferrario, A. Le Pera, D. V. Finocchiaro, M. Desmons, D. de Lange, H. de Man, A. J. Meskers, J. Morits, N. M. Neumann, et al., "Geoqkd: quantum key distribution from a geostationary satellite," in International Conference on Space Optics—ICSO 2020, vol. 11852, pp. 222–236, SPIE, 2021.

[14] J. Williams, M. Suchara, T. Zhong, H. Qiao, R. Ket- timuthu, and R. Fukumori, "Implementation of quantum key distribution and quantum clock synchroniza- tion via time bin encoding," in Quantum Computing, Communication, and Simulation, vol. 11699, pp. 16– 25, SPIE, 2021.

[15] C. Schimpf, S. Manna, S. F. Covre da Silva, M. Aigner, and A. Rastelli, "Entanglement-based quantum key distribution with a blinking-free quantum dot operated at a temperature up to 20 k," Advanced Photonics, vol. 3, no. 6, pp. 065001–065001, 2021.

[16] O. Amer, W. O. Krawec, and B. Wang, "Efficient routing for quantum key distribution networks," in 2020 IEEE International Conference on Quantum Computing and Engineering (QCE), pp. 137–147, IEEE, 2020.

[17] H.-J. Ding, J.-Y. Liu, C.-M. Zhang, and Q. Wang, "Predicting optimal parameters with random forest for quantum key distribution," Quantum Information Processing, vol. 19, pp. 1–8, 2020.

[18] Kumar, A., Garhwal, S. State-of-the-Art Survey of Quantum Cryptography. Arch Computat Methods Eng 28, 3831–3868 (2021). https://doi.org/10.1007/s11831-021-09561-2

[19] Ukidve, S., Yadav, R., Manshahia, M.S., Chaudhary, M.P. (2023). Secure Communication Through Quantum Channels: A Study of Quantum Cryptography. In: Vasant, P., et al. Intelligent Computing and Optimization. ICO 2023. Lecture Notes in Networks and Systems, vol 853. Springer, Cham. https://doi.org/10.1007/978-3-031-50327-6_31

[20] Shamshad, S., Riaz, F., Riaz, R., Rizvi, S.S., & Abdulla, S. (2022). An enhanced architecture to resolve public-key cryptographic issues in the Internet of Things (IoT), employing quantum computing supremacy. Retrieved from NCBI.

[21] Santosh Kumar Henge1, Gitanjali Jayaraman2, M Sreedevi3, R Rajakumar3, Mamoon Rashid4,*, Sultan S. Alshamrani5, Mrim M. Alnfiai5 and Ahmed Saeed AlGhamdi, Secure keys data distribution based user-storage-transit server authentication process model using mathematical post-quantum cryptography methodology, NHM, 18(3): 1313–1334, 2023.