International Journal of Basic and Applied Sciences, 14 (4) (2025) 708-720

SPC

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/rp152h11
Research paper

Adaptive Routing and Security for Heterogeneous Networks Using Quantum Key Distribution and Bat Optimized Recurrent Neural Network

S. Nithya [1] *, Krishna Prakash Arunachalam [2], S. Kanimozhi [3], Asha Rani Borah [4]

[1] Assistant Professor, Department of Information Technology, PSNA College of Engineering and Technology, Kothandaraman nagar, Dindigul, India.
[2] Departamento de Ciencias de la Construcción, Facultad de Ciencias de la Construcción Ordenamiento Territorial, Universidad Tecnológica Metropolitana, Santiago, Chile.
[3] Assistant Professor, Department of Computer Science and Engineering, Chennai Institute of Technology, Chennai, India. Research Scholar, Dr. MGR Educational and Research Institute, Chennai, India.
[4] Professor, Department of Computer Science and Engineering, New Horizon College of Engineering, Bengaluru, India.
**Corresponding author E-mail: snithya@psnacet.edu.in*

Received: April 22, 2025, Accepted: June 22, 2025, Published: August 27, 2025

Abstract

In contemporary heterogeneous networks, the reliance on robust and secure communication protocols is increasingly critical due to the rising sophistication of intruding techniques and diverse attack vectors. The dynamic nature of routing in these networks, coupled with nodes of varying computational capabilities, poses a risk of routing attacks, which significantly compromise network security and performance. To address these challenges, this paper introduces an advanced framework combining Post-Quantum Cryptography (PQC) with Bat Optimization Algorithm (BOA) based Adaptive Quantum Routing RNN (AQR-RNN) to enhance security and routing efficiency. Quantum Key Distribution (QKD) is employed to secure communications, thus providing a robust defense against threats. Simultaneously, BOA- AQR-RNN is utilized to optimize routing efficiency, inspired by the echolocation capabilities of bats. This approach leverages AQR-RNN architectures to adaptively learn and predict routing paths, enhancing decision-making and optimization processes. The synergy between QKD and BOA- AQR-RNN approach not only strengthens the security framework of heterogeneous network routing protocols but also achieves superior Quality of Service (QoS) by dynamically optimizing routing strategies. The proposed methodology demonstrates significant potential for advancing secured communication in Internet of Things (IoT) environments and other complex network architectures.

Keywords: *Heterogeneous Network; Quantum Key Distribution; Optimization Algorithm; Network Security; Quality of Service.*

1. Introduction

The IoT consists of several heterogeneous devices that have enabled convenient and efficient communication between things separated in physically disconnected locations. Given the peculiarities established with IoT, it remains a challenge to ensure any trust and data security during transmission at the IoT level. In a present IoT system, data encryption is rather simply implemented in a method called lightweight cryptography to assure data security whilst in transmission. Lightweight cryptography poses such a risk for quantum computers, presenting several challenges with respect to privacy and security of the IoT. QKD offers long-term security while communicating. [1] QKD allows two parties communicating with symmetric private keys to exchange shared, private keys, where information-theoretic security is derived from fundamental principles of quantum mechanics. A pair of private keys is established for encrypting messages communicated between the communication associates, which occurs on classical channels. QKD protocols utilize quantum phenomena, i.e., no no-cloning property and quantum entanglement, to determine the possibility of a third-party eavesdropping. Once the peer nodes mutually establish shared secret keys, the information exchanged between peer nodes is encrypted with standard symmetric ciphers [2]. Because traditional routing protocols lack adaptability, like Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Low-Energy Adaptive Clustering Hierarchy (LEACH), frequently need to dynamically adjust to the complexity of heterogeneous networks [3, 4]. These limitations lead to inefficient energy use, higher end-to-end latency, and lower Quality of Service (QoS) as nodes show different rates of energy depletion or when network density rises. New developments in quantum cryptography, artificial intelligence, and bio-inspired optimization have provided the way to more effective and safe routing systems [5].

To improve energy efficiency and reduce congestion, a number of routing optimization techniques have been introduced, such as clustering-based methods, hybrid multipath transmission, and metaheuristic algorithms [6-7]. However, these approaches are computationally demanding or rely on predefined static policies, which makes them unsuitable for real-time, resource-constrained networks. Machine learning-based models, such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and reinforcement learning, have demonstrated promise in predicting network traffic and optimizing route selection. However, in complicated network topologies, these AI-driven methods frequently lack an effective global search mechanism, which results in less-than-ideal routing choices [8]. Furthermore, even though AI-based techniques increase flexibility, they do not automatically solve energy-related issues; extra optimization layers are needed to balance load distribution and reduce energy consumption [9].

Heterogeneous Wireless Sensor Network (HWSN) security is still an important concern, particularly in light of the advent of quantum computing, which offers traditional encryption methods like Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Advanced Encryption Standard (AES) in jeopardy. Quantum Key Distribution (QKD) must be incorporated for unbreakable cryptographic security because traditional encryption techniques based on mathematical complexity, like RSA and AES, are still susceptible to quantum computer attacks [10]. While AI-driven routing models have shown promise in adaptive learning and congestion prediction, they often lack integration with energy-efficient path selection mechanisms, leading to network inefficiencies in large-scale deployments [11]. To get beyond these limitations, a thorough strategy that combines bio-inspired optimization, AI-driven predictive routing, and quantum-resistant security measures in a synergistic manner is required [12]. In order to guarantee dependable, scalable, and impenetrable data transmission in HWSNs, this study suggests a unique QKD-assisted Bat Optimization Algorithm (BOA). Adaptive Quantum Routing RNN (AQR-RNN) architecture that integrates energy-efficient global search, predictive deep learning-based routing, and quantum-secure communication. The suggested framework improves network longevity, security, and adaptability by utilizing AI-based dynamic routing, bio-inspired energy efficiency strategies, and QKD-powered encryption. This makes it a feasible option for next-generation heterogeneous sensor networks.

1.1. Motivation

An increasing need for highly secure and effective data transmission in diverse networks is the motivation behind this study. Quantum-safe encryption algorithms must be used since current cryptography approaches are susceptible to advances in quantum computing. At the same time, traditional routing methods have trouble changing network conditions, which leads to energy usage and less-than-ideal path selection. In this study, this research integrates BOA- AQR-RNN for adaptive routing with QKD for secure key management to provide a strong communication architecture that guarantees low latency, high security, and energy efficiency.

1.2. Major contribution

A unique framework that combines AI-driven routing with QKD-based security methods in a synergistic manner is proposed in this research. The suggested method seeks to improve the security and efficiency of HWSNs by utilizing the unbreakable encryption offered by QKD and the predictive powers of AI. This will help to solve the dual challenges of data protection and energy conservation in the age of quantum computing.

1.2.1. Development of a hybrid routing framework

- A QKD-assisted Bat Optimization Algorithm (BOA)-Adaptive Quantum Routing RNN (AQR-RNN) architecture is proposed for heterogeneous networks that combines quantum-resistant security, bio-inspired optimization, and AI-based adaptive routing.

1.2.2. Energy-efficient path selection using BOA

- To ensure low energy consumption and a longer network lifetime, BOA is used to carry out global search-based energy-aware routing.

1.2.3. AI-driven adaptive routing with AQR-RNN

- AQR-RNNs are used for predictive routing adaptation, enabling traffic-optimized and congestion-aware path selection in real time.

1.2.4. Quantum key distribution (QKD) for secure communication

- Ensures unbreakable encryption against both conventional and quantum-based cyber-attacks by integrating QKD-based cryptographic security.
- Ensures feasible deployment in energy-constrained networks by integrating high-performance AI models with lightweight routing techniques to optimize computational overhead.

The organization of the research is as follows: Section 2 defines the recent related works with their limitations. Section 3 states the proposed methodology. Section 4 describes the result section, and Section 5 ends with a conclusion and future scope.

2. Related work

The development of intelligent, secure, and energy-efficient routing techniques has been the main focus of recent developments in heterogeneous networks. Numerous approaches have been put forward to improve routing speed by combining cryptographic security, optimization techniques, and machine learning. However, existing methods still suffer from computational overhead, limited adaptability, and security vulnerabilities, necessitating the need for a more robust solution. Optimizing energy in heterogeneous networks has been the focus of numerous studies.

Ahmed A. et al (2023) [13] have constructed an Adaptive Particle Swarm Optimization (PSO) method for encryption advances through Discrete-time Quantum Walks (DTQW). In cryptography, key generation methods apply a variety of chaotic systems, elements of quantum mechanics, and optimization techniques for encryption key generation. The "Quantum Secure" aspect is DTQW, which leads to quantum-like properties to establish unpredictability within the generated keys. However, the APSO method is computationally expensive, consequently limiting access to adequate processing resources, which in the case of run-time demands. APSO still suffers from premature convergence, contributing to optimum points, with the residual performance being the inferior solution. Thus, tuning the required parameters for performance effectiveness for differing optimization problems remains a challenge.

Tara Nawzad et al (2025) [14] have developed to refine lattice-based cryptographic keys, rather than the authors' objective of providing Genetic Algorithm (GA) key generation efficiencies to produce keys maintaining security against quantum attack patterns. This approach is computationally less demanding in terms of processing resources and memory, which is ideal for resource-constrained areas. However, despite the computational efficiency of GAs, it still possesses deterministic contributions to convergence behaviour that lead to predictable patterns, to be exploited by attackers. Thus, randomness within the GA is an extreme necessity to maintain appropriate cryptographic security.

In the study conducted by Tannu Sharma et al (2023) [15], the Privacy-Aware Post Quantum Secure method uses an Ant Colony Optimization (ACO) based Ad Hoc On-Demand Distance Vector (AODV) Routing protocol to enhance performance and to mitigate quantum threats using Ring Learning with Errors (RLWE)-based key exchange. Post-Quantum Secure ensures that each of the encryption algorithms is secure against quantum attacks when used in a subsequent computing environment. However, the authors acknowledge computational complexity, which leads to overhead in a large-scale network.

Muthusamy et al. (2024) [16] presented an Optimized Group-Centric Routing (OGCR) framework that groups sensor nodes dynamically according to their transmission patterns and energy reserves. Through load balancing among nodes, their approach effectively reduced energy usage and increased network lifespan. However, in high-density networks, this method demonstrated notable performance loss, resulting in higher transmission delays and network congestion when the number of active nodes above a certain threshold. Furthermore, the study failed to consider real-time flexibility when choosing the best clusters, which might result in less-than-ideal routing choices in dynamic environments.

In order to guarantee consistent energy distribution among sensor nodes, Bhanu and Santhosh (2024) [17] developed the Optimal Energy Conservation Routing (OECR) method, which integrated adaptive power regulation and load-balancing techniques. By successfully lowering premature energy depletion, the model extended the lifespan of the network. However, their approach faced challenges in high-traffic scenarios, where routing delays increased due to congestion and route re-computation. Additionally, the security mechanisms in OECR were limited to basic authentication, making the network vulnerable to eavesdropping and malicious attacks.

Ensuring secure routing in heterogeneous environments has been a major concern due to the increasing risks of cyber-attacks and unauthorized data interception. In order to prevent unwanted access, Nagaraju et al. (2022) [18] created a Secure Routing-Based Energy Optimization (SREO) model that included lightweight cryptographic authentication. Their findings showed enhanced secrecy and data integrity, which successfully decreased the chance of data leakage. However, the higher computational expense resulting from the security improvements rendered the framework unsuitable for IoT devices with limited resources. Furthermore, their strategy depended on static key management methods, which could be endangered by proficient attackers.

A Multi-Objective Optimized Multipath Transmission Algorithm (MOMTA-HN) presented by Qi et al. (2024) [19] to offer dependable and secure routing. By distributing data over several secure pathways, their technique used multipath transmission to reduce packet loss and increase energy efficiency. Despite its benefits, MOMTA-HN was ineffective at managing real-time topology alterations because it did not incorporate AI-based adaptive routing. The absence of a predictive learning mechanism meant that routing decisions were based on historical data rather than future network states, leading to suboptimal path selection.

Numerous research papers have investigated the application of machine learning approaches for routing optimization in light of the growing popularity of artificial intelligence-driven networking. Using deep learning methods, Thangavelu and Rajendran (2024) [20] developed an AI-Assisted Secure Routing (AISR) model that predicted the best routing routes by analyzing network conditions. Their method proved to be highly effective in reducing latency and increasing energy economy, which makes it a good fit for extremely dynamic networks. However, the security mechanisms in AISR were limited to machine learning-based anomaly detection, which lacked the robustness required for post-quantum cryptographic attacks. Furthermore, the absence of quantum-resistant encryption techniques posed a major challenge in future-proofing the security of the model. The comparison with state-of-the-art techniques is shown in Table 1.

Table 1: Comparison with State-of-the-Art Techniques

Reference	Technique Used	Key Contributions	Energy Efficiency	Limitations
Muthusamy et al. (2024)	Optimized Group-Centric Routing (OGCR)	Improves energy efficiency through dynamic clustering	Moderate	High delay in dense networks does not integrate security
Bhanu & Santhosh (2024)	Optimal Energy Conservation Routing (OECR)	Load balancing and adaptive power control reduce energy depletion	Moderate	Increased latency in high-traffic scenarios, and lacks advanced security
Nagaraju et al. (2022)	Secure Routing-based Energy Optimization (SREO)	Lightweight cryptographic authentication ensures secure transmission	High	Increased computational overhead, limited scalability
Qi et al. (2024)	Multi-Objective Optimized Multipath Transmission Algorithm (MOMTA-HN)	Secure multipath transmission reduces packet loss	High	Not adaptive to topology changes, no predictive analysis
Thangavelu & Rajendran (2024)	AI-Assisted Secure Routing (AISR)	Machine learning-based adaptive routing for dynamic networks	High	No quantum-resistant security, requires high processing power

Although many methods have been proposed to increase routing security and efficiency in HWSNs, few address energy optimization while allowing real-time adaptability and providing quantum threats. Most methods lack predictive learning capabilities, face scalability issues, or do not include quantum-resilient encryption methods. Because of these limitations, there is a strong motivation for a single, intelligent, adaptive, energy-efficient routing solution that is provably secure.

2.1. Research gaps

The quick development of heterogeneous networks has made it more difficult to maintain low energy consumption and good network performance while guaranteeing effective, safe, and adaptive routing. The dynamic nature of HWSNs, where node mobility, fluctuating energy restrictions, and unpredictable traffic loads greatly affect network performance, makes it difficult for traditional routing protocols like AODV and DSR. Additionally, current energy-efficient routing techniques, including group-centric and multipath transmission algorithms, improve path selection but do not include predictive routing or real-time flexibility, which results in significant latency and packet loss in rapidly changing environments. Additionally, security remains a critical concern, as conventional cryptographic techniques rely on computational hardness, making them vulnerable to emerging quantum attacks. For low-power sensor networks, current routing protocols are not feasible due to their large computational overhead or lack of strong security features. Even though some current research incorporates AI-driven routing schemes, it mostly concentrates on avoiding congestion and conserving energy without taking quantum-resistant encryption solutions into account.

Secure routing technologies, such as multipath secure transmission and lightweight cryptographic authentication, also enhance data integrity, but they are ineffective for large-scale IoT deployments because they are not scalable or adaptable in real-time. The absence of a unified framework that integrates energy efficiency, predictive routing, and quantum-resistant security highlights a major research gap in existing HWSN solutions. Hence, motivated by these considerations, a novel framework with a BOA, AQR-RNN, and QKD is developed to develop a secure, scalable, intelligent routing system. In order to overcome these challenges, AQR-RNN for adaptive, predictive routing decisions, BOA for global search-based energy-efficient path selection, and QKD for unbreakable encryption.By overcoming the drawbacks of conventional routing techniques and protecting the network from cyber and quantum-based threats, this innovative technology guarantees secure, energy-efficient, and dynamically adaptable routing. Also, the proposed framework is designed to enhance network lifespan, minimize latency, and optimize security, making it an ideal solution for next-generation HWSNs in critical applications. The next section details the methodology and architecture of this integrated framework.

3. Proposed methodology

Heterogeneous networks face significant challenges for routing because of dynamic topology, energy constraints, and the varied computational capacities of sensor nodes. The inability of traditional routing algorithms, such as AODV, LEACH, and DSR, to dynamically adjust to shifting network conditions frequently results in higher latency, packet loss, and energy usage. This work addresses these issues by integrating a BOA-based AQR-RNN to dynamically optimize routing paths by ensuring adaptability to topological changes, reducing end-to-end latency, minimizing energy consumption, and improving network lifetime. The overall framework of the proposed work is shown in Figure 1.

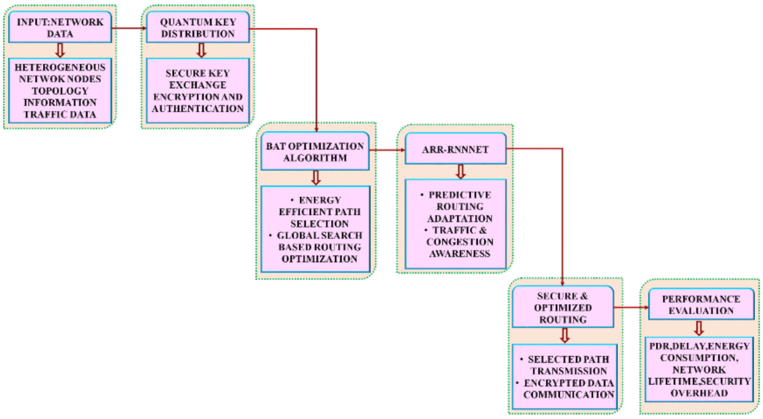
INPUT:NETWORK DATA
HETEROGENEOUS NETWOK NODES TOPOLOGY INFORMATION TRAFFIC DATA
QUANTUM KEY DISTRIBUTION
SECURE KEY EXCHANGE ENCRYPTION AND AUTHENTICATION
BAT OPTIMIZATION ALGORITHM
• ENERGY EFFICIENT PATH SELECTION
• GLOBAL SEARCH BASED ROUTING OPTIMIZATION
ARR-RNNNET
• PREDICTIVE ROUTING ADAPTATION
• TRAFFIC & CONGESTION AWARENESS
SECURE & OPTIMIZED ROUTING
• SELECTED PATH TRANSMISSION
• ENCRYPTED DATA COMMUNICATION
PERFORMANCE EVALUATION
PDR,DELAY,ENERGY CONSUMPTION, NETWORK LIFETIME,SECURITY OVERHEAD

Fig. 1: Overall Framework of Proposed Work.

3.1. Secure key exchange using quantum key distribution (QKD)

The only cryptographic method that can be proven to be secure is QKD, which uses the basic ideas of quantum mechanics to create and share encryption keys. By taking advantage of the Heisenberg Uncertainty Principle and Quantum No-Cloning Theorem, QKD provides unconditional security in contrast to traditional cryptography techniques that depend on computational complexity, making eavesdropping detectable and avoidable. To create a tamper-proof cryptographic key for heterogeneous networks, the suggested QKD-assisted secure key exchange architecture combines error correction, privacy amplification, authentication methods, and quantum key generation based on the BB84 protocol. The production and transmission of quantum states, measurement and basis reconciliation, error correction and privacy amplification, authentication, and secure key storage are the four main stages of the QKD-based secure key exchange process.

3.1.1. Quantum state preparation and transmission

To establish secure communication with the destination node (D), the source node (S) first creates a random binary sequence, which can be expressed mathematically as follows:

$$K = \{k_1, k_2, \dots, k_n\} \tag{1}$$

One of two bases can be used to encode each bit k_i into a quantum state. Diagonal Basis (Hadamard Basis): $|0\rangle$, $|1\rangle$, and Rectilinear Basis (Standard Basis):

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2}$$

Before sending the sequence to destination node D over a quantum channel, the source node chooses a basis at random for each qubit. The transmitted quantum state Q can be expressed mathematically as follows:

$$Q = \{q_1, q_2, \dots, q_n\}, q_i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\} \tag{3}$$

where each qubit q_i corresponds to a classical bit k_i, encoded on a randomly selected basis.

3.1.2. Measurement and basis reconciliation

The destination node D uses randomly selected bases to carry out quantum measurements after receiving the quantum states. The results are only valid when the sender and the recipient utilize the same basis because quantum measurement is basis-dependent. Let, B_s be the basis sequence used by the sender S and B_d be the basis sequence used by the receiver D. The receiver publicly announces the basis choices B_d over a classical channel, and the sender S reveals which bases matched. The correctly measured bits form the raw key K_{raw} is defined below:
$K_{raw} = \{k_1, k_2, \ldots., k_m\}, m \leq n$ (4) where m is the number of correctly measured bits. The remaining bits (mismatched basis measurements) are discarded.

3.1.3. Error correction and privacy amplification

Quantum noise, channel flaws, and possible eavesdropping can all cause errors in the raw key. The Cascade algorithm, an interactive reconciliation technique, is used to fix such errors. The following provides the raw key's entropy: The entropy of the raw key is given by:

$$H\,(K_{raw}) = H\,(K_{final}) + H\,(E) \tag{5}$$

Here, $H\,(K_{final})$ specifies the final key entropy after error correction and H (E) defines the error-related entropy, which must be eliminated. The mathematical formulation of the quantum bit error rate (QBER) is stated below:

$$QBER = \frac{N_{error}}{N_{total}} \tag{6}$$

Here, the number of mismatched bits in key comparison is defined as N_{error} and the total number of exchanged bits is stated as N_{total}. If QBER exceeds a predefined threshold T_{th} the key is discarded, and retransmission is initiated. Strong universal hash functions are used in privacy amplification to eliminate any information leakage, and the following is their mathematical formulation:

$$K_{final} = H\,(K_{raw}) \tag{7}$$

$H\,(.)$ specifies the collision-resistant cryptographic hash function and the final quantum-secured key K_{final} is ready for encryption.

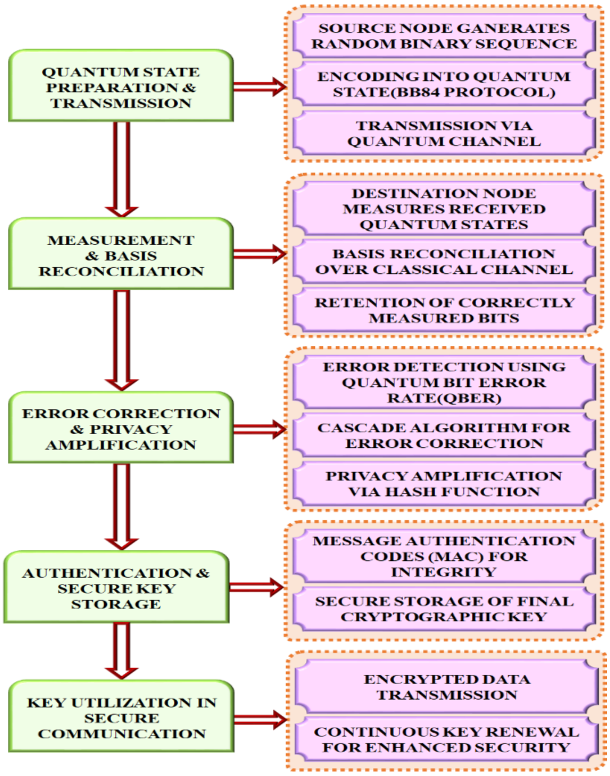
QUANTUM STATE PREPARATION & TRANSMISSION
SOURCE NODE GANERATES RANDOM BINARY SEQUENCE
ENCODING INTO QUANTUM STATE(BB84 PROTOCOL)
TRANSMISSION VIA QUANTUM CHANNEL
MEASUREMENT & BASIS RECONCILIATION
DESTINATION NODE MEASURES RECEIVED QUANTUM STATES
BASIS RECONCILIATION OVER CLASSICAL CHANNEL
RETENTION OF CORRECTLY MEASURED BITS
ERROR CORRECTION & PRIVACY AMPLIFICATION
ERROR DETECTION USING QUANTUM BIT ERROR RATE(QBER)
CASCADE ALGORITHM FOR ERROR CORRECTION
PRIVACY AMPLIFICATION VIA HASH FUNCTION
AUTHENTICATION & SECURE KEY STORAGE
MESSAGE AUTHENTICATION CODES (MAC) FOR INTEGRITY
SECURE STORAGE OF FINAL CRYPTOGRAPHIC KEY
KEY UTILIZATION IN SECURE COMMUNICATION
ENCRYPTED DATA TRANSMISSION
CONTINUOUS KEY RENEWAL FOR ENHANCED SECURITY

Fig. 2: Block Diagram of QKD.

3.1.4. Authentication and secure key storage

Message authentication codes (MACs) are used for authentication to prevent man-in-the-middle attacks. The following is a mathematical formulation of MACs:

$$MAC = H\,(K_{final}, \text{session ID}) \tag{8}$$

If authentication is unsuccessful, the procedure of exchanging keys is restarted. The last key is used for symmetric encryption and is safely stored in a trusted module:

$$C = AES\,(K_{final}, M) \tag{9}$$

Here, C defines the encrypted message and M specifies the original plaintext message. The block diagram of QKD is shown in Figure 2. For HWSNs, the QKD-based key exchange system guarantees provably secure symmetric key generation, guarding against replay attacks, quantum decryption, and eavesdropping. The framework ensures a tamper-proof, attack-resistant cryptographic model by combining error correction, privacy amplification, and authentication procedures, greatly boosting the security of next-generation sensor networks.

3.2. AQR-RNN-based bat optimization algorithm for routing

To choose the best energy-efficient, low-latency, and congestion-free way for data transmission, a bio-inspired metaheuristic optimization technique is used. A predictive routing system based on deep learning that adapts routing decisions dynamically based on real-time parameters by learning from past network patterns. This framework greatly improves the dependability, security, and lifespan of heterogeneous networks by guaranteeing quantum-safe security, real-time adaptability, and energy-efficient data transmission.

3.2.1. Problem formulation

Routing in heterogeneous networks requires path selection that is low-latency, energy-efficient, and congestion-aware, making it an NP-hard combinatorial optimization problem. The routing problem is represented as a multi-objective optimization assignment based on graphs. The HWSN is represented as a directed graph $G\ (N, L)$, Where, $N = \{N_1, N_2, \ldots, N_k\}$ defines the set of sensor nodes, $L = \{(i, j)\}$ defines the set of available communication links, (i, j) denotes the connection between nodes $N_i$and N_j respectively. The goal is to determine an optimal path $P*$ from source S to destination D that minimizes a multi-objective cost function, and its mathematical formulation is given below:

$$P^* = \arg\min \textstyle\sum_{(i,j)\in P} w_{ij}\ D_{ij} + \tau E_{total} - \gamma QKD_{ij} \tag{10}$$

Subject to
Energy constraint: $E_n \geq E_{min}, \forall N_n \in P$
Bandwidth constraint: $C_{ij} \geq B_n, \forall\ (i, j) \in P$
Packet loss minimization: $P_{ij} \leq P_{max}, \forall\ (i, j) \in P$
QKD security constraint: $QKD_{ij} \geq QKD_{min}, \forall\ (i, j) \in P$
D_{ij} specifies the transmission delay between nodes $N_i$and N_j, E_n specifies the residual energy of the node N_n.The total energy consumed along path P is stated as E_{total}. w_{ij} specifies the weight assigned to the link. τ and γ specifies the scaling factors for energy and security. The packet loss probability over the link is specified as P_{ij}. The quantum key distribution success rate over the link is stated as QKD_{ij}.

3.2.2. Initialization

The echolocation behavior of micro bats, which emit signals, assess echoes, and modify their movement in response to their surroundings, served as the model for the BOA. Each bat in BOA represents a candidate routing solution, defined as:

$$X_b = \{P_{b1}, P_{b2}, \ldots, P_{bm}\} \tag{11}$$

Here, each P_{bm} defines the possible routing path. Bats use the fitness evaluation of each path to dynamically alter their position, velocity, and frequency.

3.2.3. Fitness evaluation for path selection

The fitness function evaluates each path based on:

$$F\ (P) = \omega_1 D_{total} + \omega_2 E_{avg} - \omega_3 QKD_{ij} \tag{12}$$

The end-to-end delay is termed as D_{total}, energy consumption is specified as E_{avg} and quantum key distribution success probability is defined as QKD_{ij} respectively.

3.2.4. Velocity and position updation

The velocity and position of every bat are updated at each iteration t using the below equation.

$$V_b^{t+1} = V_b^t + (X_b^t - X^*)\ f_b \tag{13}$$

This equation updates the velocity V_b of an entity. The velocity is dependent upon the prior velocity V_b^t, as well as the difference between the present position $X_b^t$and the optimal global best path X^*, weighted by the frequency parameter f_b. The mathematical formulation of the position updation equation is given below:

$$X_b^{t+1} = X_b^t + V_b^{t+1} \tag{14}$$

In this equation, the previously determined position X_b^t is updated by adding the newly calculated velocity V_b^{t+1} to the previous position X_b^t. The mathematical formulation of frequency parameter adjusting exploration intensity is given below:

$$f_b = f_{min} + (f_{max} - f_{min}).\beta \tag{15}$$

The minimum and maximum allowed frequencies are stated as f_{min} and f_{max} respectively.

3.2.5. Loudness and pulse rate adjustment

Each bat adjusts its loudness A_b and pulse rate $r_b$dynamically, and its mathematical expressions are given below:

$$A_b^{t+1} = \alpha A_b^t \tag{16}$$

$$r_b^{t+1} = r_b^0 [1 - \exp(-\gamma t)] \tag{17}$$

α and γ specifies the constant term controlling the rate of exploration and exploitation. The updated pulse rate is termed asr_b^{t+1} and the loudness of the bat at iteration t is stated asA_b^t . By effectively balancing local and global search, this approach enhances the Bat Algorithm's optimization performance and guarantees that the best route is selected. Once the best routing path is selected, it is fed into the RNN-based predictive model for real-time adaptation. The best solution found by BOA is used to train the RNN for predictive routing.

3.3. Adaptive quantum routing RNN network (AQR-RNN)

The network architecture in heterogeneous networks is dynamic because of energy depletion, mobility, congestion, and node failures. The static decision-making or reactive methods used by traditional routing protocols frequently result in higher latency, higher energy consumption, and less-than-ideal Quality of Service (QoS). In order to overcome these obstacles, this study presents an AQR-RNN mechanism that adapts routing paths before performance deterioration happens by using past and current network conditions to forecast future network states. By continuously learning from past network conditions, the RNN-based routing model makes dynamic predictions about the optimal routing choice. The architecture of AQR-RNN is shown in figure 3). AQR-RNN is intended to forecast the most effective routing paths in real time based on evolving network states. The model includes three advanced components to ensure both accuracy and real-time responsiveness:

- Multi-Scale Dependency Retention Gate (MDRG);
- Multi-Scale Feature Alignment Unit (MFA-Unit); and
- Progressive Adaptive Sampling Mechanism (PASM).

These components enable AQR-RNN to retain long-term memory, integrate local and global network information, and adapt the learning process to the learning timeframes. They allow AQR-RNN to make intelligent, adaptive, low-latency, low-energy, and low-congestion routing decisions. Following is a short description of the components.

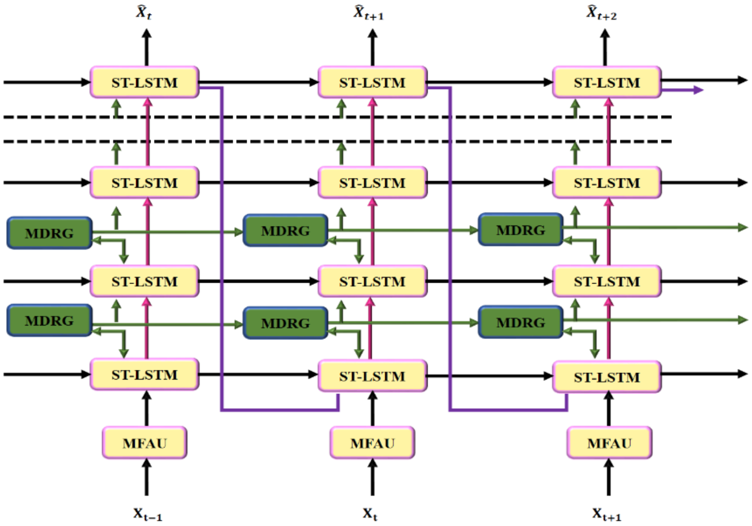

Fig. 3: Architecture of AQR-RNN.

3.3.1. Input feature representation

To predict optimal routing paths, the RNN model extracts a feature set representing real-time network parameters. The input feature vector S_t at timestep t is defined below:

$$S_t = [E_n, C_{ij}, D_{ij}, P_{ij}, QKD_{ij}] \tag{18}$$

The residual energy of the node ensures that the energy-efficient paths are selected is termed as E_n, the link capacity between nodes, preventing congestion-based failures, is specified as C_{ij}, D_{ij} defines the end-to-end transmission delay, ensures low-latency routing. The packet loss probability over the link, preventing high error rates, is specified as P_{ij} and QKD_{ij} specifies the QKD success rate, ensuring a secure communication path.

3.3.2. Multi-scale dependency retention gate (MDRG)

MDRG is a memory mechanism that allows the neural network to retain modes of interest in the traffic it encounters in the last few hours or days. Conventional models forget previous data quickly, but with MDRG, the model is able to "look back" and leverage both short and long-term behavior. This provides some ability to stabilize routing, even in environments where traffic or topology changes slowly over a longer period. Thus, retaining a few useful pieces of past knowledge in a routing context improves predictive performance and avoids the model having the same routing failure multiple times. Vanishing gradients hinder the capacity of recurrent architectures, such as LSTMs, to maintain long-range dependencies. When network circumstances change over time, this leads to ineffective routing predictions. Memory skipping is introduced by MDRG, which preserves information from previous traffic conditions by enabling the model to retrieve earlier time steps directly. MDR gates expedite learning and maintain long-term network conditions in routing. The MDRG unit permits direct updates from previous time steps, which speeds up training and enhances gradient flow. The hidden state h_t is updated using below equation.

$$Z_t^{l-1} = \text{MDRG}\,(\,H_t^{l-1}, Z_{t-1}^{l-1}\,) \tag{19}$$

$$H_t^l, C_t^l, M_t^l = \text{STLSTM}\,(Z_t^{l-1}, H_{t-1}^l, C_{t-1}^l, M_t^{l-1}) \tag{20}$$

The intermediate hidden state carrying long-term traffic dependencies is stated as Z_t, the updated hidden at time t is defined as H_t. The temporal and spatiotemporal memory states are defined as C_t and M_t respectively. The internal calculation of the MDRG unit with its candidate state computation (P_t), State Update Gate Computation(S_t) and final hidden state update (Z_t) is defined below:

$$P_t = \tanh\left(W_{px} * X_t + W_{pz} * Z_{t-1}\right) \tag{21}$$

$$S_t = \sigma\,(W_{sx} * X_t + W_{sz} * Z_{t-1}) \tag{22}$$

$$Z_t = S_t \circ P_t + (1 - S_t) \circ Z_{t-1} \tag{23}$$

The weight matrix for input and the weight matrix of the previous hidden state are specified as W_{px} and W_{pz} respectively. The element-wise multiplication is stated as $\circ$. In order to preserve some historical context while encoding new information from the input, this stage creates a preliminary hidden state candidate. By preventing vanishing gradients, the final hidden state method enables the network to effectively capture long-term dependencies. The design of MDRG is shown in Figure 4.

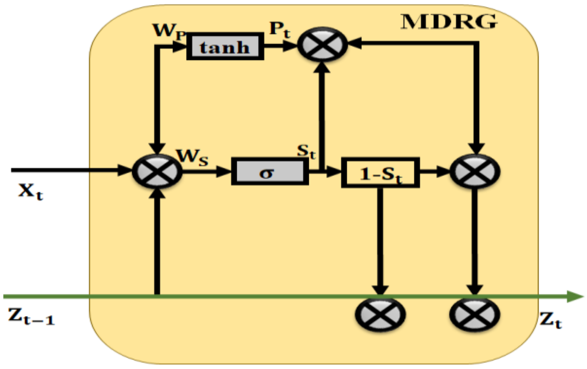

Fig. 4: Multi-Scale Dependency Retention Gate (MDRG).

3.3.3. Multi-scale feature alignment unit (MFA-Unit) for routing decisions

The MFA unit uses specific local node information (energy levels or link quality) and global network information (overall congestion, topology). The dual-purpose nature of the data allows routing decisions to be made that are optimal for a single node and optimal for the network. The MFA unit builds on the model's ability to make balanced decisions by aligning features from different levels of the network and creating smarter cooperative routing. By integrating local and global features, the MFA-Unit module guarantees that routing decisions are made with a comprehensive understanding of the network. The MFA unit improves adaptive decision-making for time-varying networks by choosing the best routes based on both local and global knowledge. The mathematical expression of the MFA unit is defined below:

$$X_t' = \sigma\,(\text{global}).\,\text{global} + \sigma\,(\text{local}).\,\text{local} \tag{24}$$

Both the local and global specify the global and local features. The design of MFAU is shown in Figure 5.

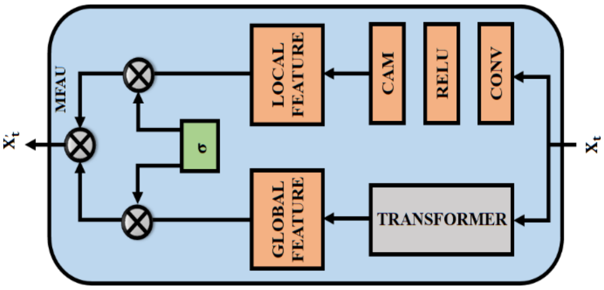

Fig. 5: Multi-Scale Feature Alignment Unit (MFA-Unit).

3.3.4. Progressive adaptive sampling mechanism (PASM)

PASM is a learning framework whereby the model is progressively taught to define its prediction based on less training data and more from its global experience. At the beginning of training, the model is taught using known (ground-truth) observations, although as training progresses, the model increasingly uses its output to improve. This process is very similar to real deployment, where the model is always making decisions without supervision. PASM decreases the variation (mismatch) between training and testing conditions, and therefore allows the model to perform smooth and reliable routing during live deployments. In traditional RNN training, inconsistencies arise between training and inference due to exposure bias. PASM mitigates this by:

$$P_{PASM} = \in_e + (\in_e - \in_s) \cdot \frac{1}{1 + e^{\frac{\beta_s - k}{\alpha_s}}} \tag{25}$$

The probability of using ground truth data during training is stated as P_{PASM} and the training iteration count is stated as k . The scaling factors are termed as α_s and β_s respectively.

3.3.5. Routing path prediction

The model predicts the optimal next-hop decision y_t and its mathematical expression is given below:

$$y_t = W_y h_t + b_y \tag{26}$$

Here, W_y transforms hidden states into routing decisions, and the optimal routing path is selected using below equation.

$$P_t^* = \arg\max y_t \tag{27}$$

The overall process of the proposed framework is shown in table 2).

Table 2: BOA-RNN-Based Secure Adaptive Routing for HWSNs

```
Input:
S (Source), D (Destination), G (V, E) (Network Graph)
Candidate Paths $P = \{p_1, p_2, \ldots, p_k\}$
QKD Threshold, Energy Threshold, Delay Threshold
Output
Optimal Routing Path $P^*$with Energy Efficiency, Low Latency, and Secure Transmission
Step 1: Quantum Key Distribution (QKD) for Secure Encryption
Generate and transmit quantum bits over the quantum channel.
The receiver measures and reconciles basis mismatches.
Compute Quantum Bit Error Rate (QBER).
If QBE $<$ QKDhreshold, generate a secure encryption key $K_{QKD}$
Step 2: BOA-Based Energy-Efficient Path Selection
Initialize bat population (paths) and set fitness function
$F(P) = \omega_1 D_{total} + \omega_2 E_{avg} - \omega_3 QKD_{ij}$
Update bat velocities and adjust path selection dynamically.
Select best path $P^*$ that minimises F (P)
Step 3: Adaptive Quantum Routing RNN Network (AQR-RNN)
Input network metrics $X_t = \{\text{Energy}, \text{Bandwidth}, \text{Delay}, \text{Packet loss}\}$
Predict next-hop routing decision using
$P_{AQR-RNN} = \text{Softmax}(W_o h_t)$
Compare $P_{AQR-RNNNet}$ with BOA-selected $P^*$ and select the best path.
Step 4: Secure Data Transmission
Encrypt the message using $K_{QKD}$
Transmit data over the optimized path $P^*$
Decrypt at the destination and re-key if necessary.
```

4. Result and discussion

A wide range of network environments is used for the comprehensive simulations in order to assess the effectiveness of the proposed AQR-RNN-based BOA for routing in heterogeneous networks with QKD. The parameters used for the simulation are displayed in Table 3. Let's model a heterogeneous network with different node densities, mobility patterns, and energy constraints. The AI-Assisted Secure Routing (AISR), Secure Routing-Based Energy Optimization (SREO), Optimal Energy Conservation Routing (OECR), Optimized Group-Centric Data Routing (OGC-DR), Multipath Link Routing Protocol (MLRP), and other established protocols have been compared with the proposed architecture.

Table. 3: Simulation Parameters

Parameter	Value
Number of Nodes	200 – 1000
Simulation Area	1000m × 1000m
Transmission Range	250m
Packet Size	512 Bytes
Initial Energy per Node	2J
Mobility Model	Random Waypoint
Traffic Type	CBR (Constant Bit Rate)
Encryption Method	QKD-based Key Exchange

4.1. Packet delivery ratio (PDR) analysis

The percentage of packets that are successfully received at their destination in relation to the total number of packets transmitted is known as the packet delivery ratio, or PDR. Better dependability and more effective routing are indicated by a higher PDR. The simulation results over 100- 200 sensor nodes are shown in Table 4, and the graphical illustration is shown in Figure 6.

Table 4: PDR Analysis

Number of Nodes	Proposed (%)	MLRP (%)	OGC-DR (%)	OECR (%)	SREO (%)	AISR (%)
100	97.4	92.5	90.3	89.6	88.7	91.1
150	95.8	91.2	88.7	87.4	86.5	89.3
200	94.5	90.2	88.4	87.3	86.9	89.2

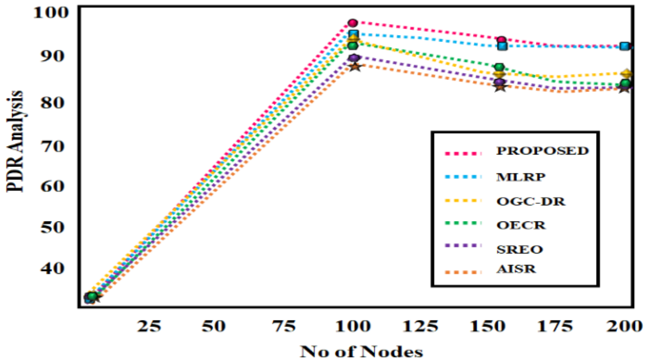

Fig. 6: Graphical Analysis of PDR.

According to the PDR results, the suggested framework continuously performs better than the current protocols for a range of network sizes. Due to its worldwide optimization through BOA, predictive routing with RNN, and quantum key distribution (QKD)-secured communication, which ensures minimum packet loss, BOA-RNN has a high PDR. As a result of congestion and redundant multipath transmissions, MLRP experiences excessive packet drops, which causes collisions. Even though OGC-DR and OECR optimize energy consumption, they are ineffective in high-traffic scenarios due to their lack of dynamic congestion-aware routing methods, which increases packet losses. SREO adds cryptographic processing overhead, which results in delays and packet expiration before delivery, even though it offers secure transmission. In spite of being AI-driven, AISR lacks BOA's optimization technique, which leads to less-than-ideal path selection under different network loads. These findings demonstrate that BOA-RNN is the most dependable routing mechanism among the protocols under comparison, achieving the highest PDR through adaptive routing, effective traffic management, and secure packet delivery.

4.2. End-to-end delay analysis

The amount of time it takes for a packet to travel from its origin to its destination is measured by its delay. Faster data transfer is ensured by a shorter delay, which is essential for real-time applications. The end-to-end delay simulation analysis is shown in Table 5, and the graphical illustration is shown in Figure 7.

Table 5: End-to-End Delay Analysis

Number of Nodes	Proposed (ms)	MLRP (ms)	OGC-DR (ms)	OECR (ms)	SREO (ms)	AISR (ms)
100	24.6	30.8	35.5	33.1	42.3	27.8
150	26.9	32.5	38.2	36.4	46.8	30.1
200	28.5	34.2	42.3	39.7	48.5	31.4

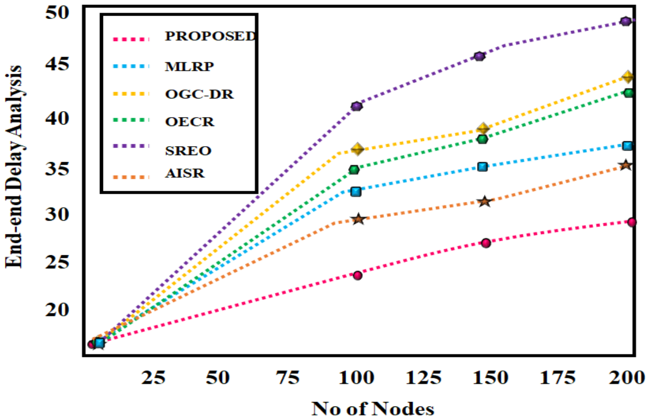

Fig. 7: Graphical Analysis of End-to-End Delay Analysis.

According to the End-to-End latency outcomes, BOA-RNN has the smallest latency because it uses BOA to make energy-efficient routing decisions and RNN-based predictive routing to dynamically choose paths free of congestion. Another factor contributing to BOA-RNN's low latency is its lightweight QKD encryption, which reduces the latency involved in cryptographic key exchange. However, MLRP experiences a higher latency because several redundant pathways result in extra queuing delays at intermediate nodes. Due to their lack of congestion-aware routing, OGC-DR and OECR have delays in route selection when traffic density rises.

Because of its computationally demanding security processes, SREO has a high delay. AISR uses AI-based adaptive routing to minimize delay somewhat, but it is unable to maintain optimal routing paths dynamically since it lacks a bio-inspired global search mechanism like BOA. According to these results, BOA-RNN efficiently reduces end-to-end latency, which makes it perfect for real-time applications in heterogeneous wireless sensor networks that are heterogeneous.

4.3. Energy consumption per node

The average amount of energy that a sensor node uses to send data is measured by energy consumption. A network with lower energy usage has a longer lifespan. The simulation analysis of energy consumption is shown in Table 6, and the graphical illustration is shown in Figure 8.

Table 6: Energy Consumption Analysis

Number of Nodes	Proposed (J)	MLRP (J)	OGC-DR (J)	OECR (J)	SREO (J)	AISR (J)
100	0.09	0.12	0.15	0.13	0.19	0.11
150	0.11	0.14	0.17	0.15	0.22	0.13
200	0.12	0.15	0.21	0.18	0.23	0.14

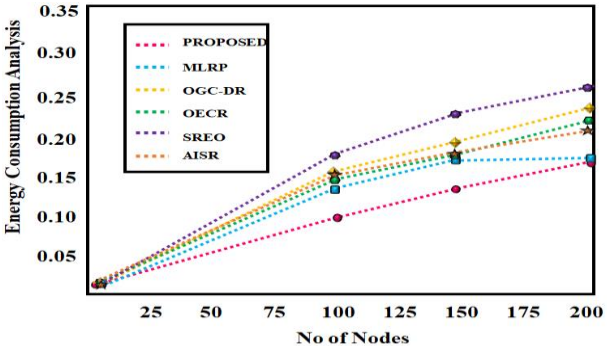

Fig. 8: Graphical Analysis of Energy Consumption.

According to Energy Consumption data, BOA-RNN uses the least amount of energy per node, guaranteeing effective power use and a longer network lifetime. The main cause of this is BOA's global energy-aware path selection, which distributes the load evenly over several nodes to avoid early energy depletion in any one area. Furthermore, by anticipating traffic congestion and improving packet forwarding choices to avoid unnecessary power waste, RNN eliminates redundant retransmissions. Because of its multipath transmission strategy, which involves nodes sending redundant copies of packets, MLRP uses a lot of energy. Despite their emphasis on energy efficiency, OGC-DR and OECR have problems with frequent re-clustering operations, which result in higher energy consumption. These results demonstrate that BOA-RNN is the most energy-efficient protocol, making it well-suited for large-scale and long-term deployments in HWSNs. SREO shows the highest energy consumption because security-related computations increase the processing overhead on sensor nodes, while AISR improves energy efficiency through AI-based adaptive routing but does not implement an explicit optimization mechanism like BOA, resulting in moderate energy waste.

4.4. Network lifetime analysis

Network lifespan is directly impacted by the amount of time until the first sensor node runs out of energy. The simulation analysis of network lifetime is shown in Table 7, and the graphical illustration is shown in Figure 9.

Table 7: Network Lifetime Analysis

Number of Nodes	Proposed (s)	MLRP (s)	OGC-DR (s)	OECR (s)	SREO(s)	AISR (s)
100	8756	7932	6890	7203	6789	7602
150	8432	7591	6548	6841	6437	7321
200	8123	7345	6452	6785	6321	7234

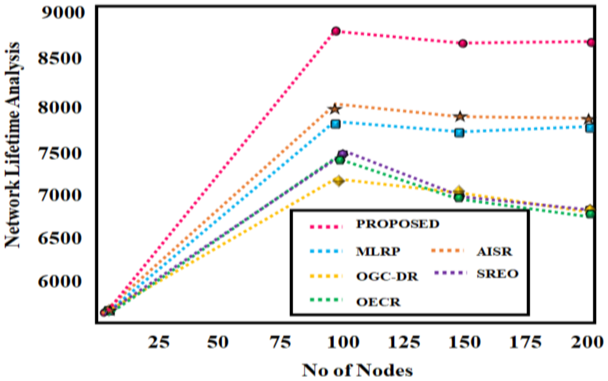

Fig. 9: Graphical Analysis of Network Lifetime Analysis.

The Network Lifetime results demonstrate that BOA-RNN significantly extends network lifespan compared to existing protocols. This is made possible by BOA's energy-efficient routing choices, which keep certain nodes from being overused and guarantee consistent energy depletion throughout the network. Further reducing power usage is achieved by minimizing retransmissions through RNN-based traffic prediction. MLRP has a shorter network lifetime due to excessive energy wastage in multipath routing, leading to premature node failures. To a certain degree, OGC-DR and OECR increase network lifetime; however, their static routing strategies perform poorly in dynamic traffic situations, leading to unequal energy consumption. SREO severely affects network longevity as its security features require additional energy, accelerating node fatigue. AISR moderately enhances network longevity but lacks an effective energy-balancing mechanism, making it less ideal than BOA-RNN. According to these findings, BOA-RNN is perfect for resource-constrained wireless sensor networks since it efficiently extends network lifetime by balancing energy usage and reducing unnecessary transmissions.

4.5. Routing overhead analysis

Routing overhead is defined as the total number of control or signaling packets generated in the process of route discovery and maintenance. High overhead reduces network efficiency, which is especially critical in large-scale developments. The results of routing overhead simulation analysis are seen in Table 9, and in graphical form in Figure 10.

Table 8: Routing Overhead

Number of Nodes	Proposed (%)	MLRP (%)	OGC-DR (%)	OECR (%)	SREO (%)	AISR (%)
200	8.7	18.3	15.4	16.2	17.5	14.6
400	9.2	20.1	16.3	17.9	19.3	16.8
600	9.9	21.3	17.6	18.5	20.2	17.5
800	10.3	22.6	18.9	19.1	21.7	18.4
1000	10.7	23.8	20.1	20.2	22.4	19.3

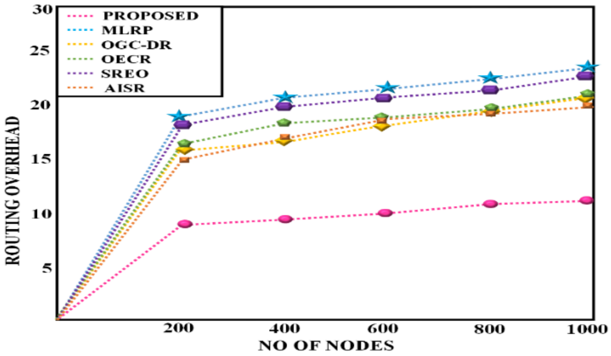

Fig. 10: Graphical Analysis of Routing Overhead.

Figure 10 compares network routing overhead across network sizes varying from 200 nodes to 1000 nodes, for the proposed BOA-AQR-RNN method and five existing routing methods. The proposed method consistently indicates a significant decrease in routing overhead over all node densities. The cost of routing is reduced significantly due to the proposed BOA for path selection based on stable and energy-efficient path characteristics, in conjunction with the AQR-RNN, which predicts when stable paths change and adapts the edge nodes of the path, thus reducing unnecessary route rediscovery. Existing protocols with higher overhead, such as MLRP and SREO, required higher routing costs due to forwarding via multiple pre-discovered paths. Due to the need to cryptographically authenticate a routing data packet, requiring more control messages because of multipath routing, this is particularly evident as node density increases. The proposed methods offer higher communication efficiency and scalability of the BOA-AQR-RNN method compared to five existing routing protocols in large-scale HWSN scenarios.

4.6. Security-based analysis

The additional processing time needed for encryption and secure data transfer is measured by security overhead. Reduced values signify effective security implementation. The simulation analysis of security analysis is shown in Table 9.

Table 9: Security-Based Analysis

Number of Nodes	Proposed (%)	SREO (%)	AISR (%)
100	7.5	15.3	10.2
150	7.8	16.1	11.3
200	8.1	16.7	12.5

The findings of Security-Based Analysis demonstrate that BOA-RNN is a very effective and safe routing system since it provides robust security protection with little overhead. The main cause of this is QKD-based encryption is which offers unbreakable cryptographic security without requiring an enormous amount of computing power. To ensure that encrypted communication is resistant to cyber threats and quantum computer attacks, QKD uses quantum principles for tamper-proof key exchange, in contrast to traditional cryptographic protocols that require complex mathematical operations. These results demonstrate that BOA-RNN successfully strikes a balance between security and efficiency, offering a reliable and scalable solution for next-generation heterogeneous wireless sensor networks. SREO provides strong security, but at the expense of high cryptographic processing overhead, which adversely affects energy efficiency and delay. AISR offers AI-based anomaly detection, which somewhat improves security, but it does not incorporate quantum-resistant encryption, making it vulnerable to post-quantum cryptographic threats.

By achieving higher packet delivery, lower delay, reduced energy consumption, extended network lifetime, and enhanced security, the simulation results across all key metrics validate that BOA-RNN is the best routing framework for secure, energy-efficient, and dynamically adaptive communication in heterogeneous wireless sensor networks, making it a strong contender for real-world deployment in critical IoT applications, industrial automation, and smart city infrastructure.

5. Conclusion

In this study, a novel BOA-AQR-RNN framework is developed that combines QKD for secure communication in heterogeneous networks, AQR-RNN for predictive adaptive routing, and BOA for global search-based energy-efficient path selection. The findings demonstrate that BOA-RNN achieves robust security with low overhead, higher PDR, lower end-to-end delays, lower energy consumption, and an extended network lifetime. The success of BOA- AQR-RNN is attributed to its adaptive learning-based predictive routing, congestion-aware path optimization, and quantum-resistant security mechanisms, which together ensure highly efficient and reliable data transmission. To ensure the framework's stability in high-density sensor networks and smart city applications, it must also be evaluated in heavily networked IoT environments with thousands of sensor nodes. This makes scaling improvements essential. Another exciting application is the incorporation of BOA- AQR-RNN with cutting-edge wireless technologies like edge computing and 6G, where AI-driven network slicing and edge intelligence may optimize resource allocation in dispersed systems and drastically lower routing latency. The proposed BOA-AQR-RNN framework is clearly scalable across all network densities up to 1000 nodes. The overhead is low, and using predictive optimization means the performance remains reasonable, even at higher node densities. These results confirm that this framework is suited for medium to large-scale HWSNs.

References

[1] Chen L, Chen Q, Zhao M, Chen J, Liu S, Zhao Y. "DDKA-QKDN: Dynamic on-demand key allocation scheme for quantum Internet of Things secured by QKD network." *Entropy*, Vol. 24, No. 2 (2022), pp. 149. https://doi.org/10.3390/e24020149.

[2] Akhtar MS, Krishnakumar G, Vishnu B, Sinha A. "Fast and secure routing algorithms for quantum key distribution networks." *IEEE/ACM Transactions on Networking*, Vol. 31, No. 5 (2023), pp. 2281-2296. https://doi.org/10.1109/TNET.2023.3246114.

[3] Nabati M, Mohsen M, Pourmina MA, “AGEN-AODV: an intelligent energy-aware routing protocol for heterogeneous mobile ad-hoc networks,” *Mobile Networks and Applications,* (2022), pp. 1-12. https://doi.org/10.1007/s11036-021-01821-6.

[4] Thakre D, Awaya S, “Performance Study of AODV, OLSR, and DSDV Routing Protocols in Mobile AD HOC Networks,” *International Journal of Microwave Engineering and Technology,* Vol. 10, No. 2, (2024), pp. 38-60p.

[5] Khedhiri K, Djabbour D, Cherif A, “The Performance of Stable Zones Protocol for Heterogeneous Wireless Sensor Networks,” *Engineering, Technology & Applied Science Research* Vol.14, No. 4, (2024), pp. 15876-15881. https://doi.org/10.48084/etasr.7716.

[6] Zhang W, Lan Y, Lin A, Xiao M, “An Adaptive Clustering Routing Protocol for Wireless Sensor Networks Based on A Novel Memetic Algorithm,” *IEEE Sensors Journal*, (2025). https://doi.org/10.1109/JSEN.2025.3526831

[7] Vijayaragavan P, Saravanan V, Suresh C, Manikavelan D, Maheshwari A, Vijayalakshmi K, Hrbac R, Demel L, Kolar V, Narayanamoorthi R. “FOAEAUC-SARP: A novel energy-efficient protocol integrating unequal clustering and intelligent routing for sustainable wireless sensor networks." *Results in Engineering,* Vol. 25 (2025), pp. 103806. https://doi.org/10.1016/j.rineng.2024.103806.

[8] Sharma T, Balyan A, Singh AK, “Machine Learning-Based Energy Optimization and Anomaly Detection for Heterogeneous Wireless Sensor Network,” *SN Computer Science,* Vol. 5, (2024), no. 6, pp. 751. https://doi.org/10.1007/s42979-024-03113-8.

[9] George M, Roberts MK, “Design of routing protocols for heterogeneous WSN based on multi-agent reinforcement learning,” In *2024 7th International Conference on Devices, Circuits and Systems (ICDCS)*, pp. 72-76. IEEE, 2024, https://doi.org/10.1109/ICDCS59278.2024.10561011.

[10] Iqbal S, Sujatha BR, “Secure authentication and key management based on hierarchical enhanced identity based digital signature in heterogeneous wireless sensor network,” *Wireless Networks,* Vol. 3, (2025), no. 1, pp. 127-147. https://doi.org/10.1007/s11276-024-03745-x.

[11] Wang Y, Zhang G, “[Retracted] EMEECP-IOT: Enhanced Multitier Energy-Efficient Clustering Protocol Integrated with Internet of Things-Based Secure Heterogeneous Wireless Sensor Network (HWSN),” *Security and Communication Networks*, No. 1 (2022), pp. 1667988. https://doi.org/10.1155/2022/1667988.

[12] Kumar DP, Kumar PG, “Implementation of optimal routing in heterogeneous wireless sensor network with multi-channel Media Access Control protocol using Enhanced Henry Gas Solubility Optimizer,” *International Journal of Communication Systems,* Vol. 38, No. 1 (2025), pp. e5980. https://doi.org/10.1002/dac.5980.

[13] Abd E-L, Bassem Abd-El-Atty AA, "Adaptive particle swarm optimization with quantum-inspired quantum walks for robust image security." *IEEE Access,* Vol. 11 (2023), pp. 71143-71153. https://doi.org/10.1109/ACCESS.2023.3286347

[14] Al Attar, TNA, Nawzad Mohammed R. "Optimization of Lattice-Based Cryptographic Key Generation using Genetic Algorithms for Post-Quantum Security." *UHD Journal of Science and Technology*, Vol. 9, No. 1 (2025), pp. 93-105. https://doi.org/10.21928/uhdjst.v9n1y2025.pp93-105.

[15] Sharma T, Ranjith Kumar M, Kaushal S, Chaudhary D, Saleem K, “Privacy aware post quantum secure ant colony optimization ad hoc on-demand distance vector routing in intent based internet of vehicles for 5G smart cities." *IEEE Access*, Vol. 11 (2023), pp. 110391-110399. https://doi.org/10.1109/ACCESS.2023.3311515.

[16] Muthusamy P, Rajan A, Praveena R, Navaneethakrishnan SR, Babu TR, Murugan KS, “Optimized Group-Centric Data Routing in Heterogeneous Wireless Sensor Networks for Enhanced Energy Efficiency,” *Journal of Cybersecurity & Information Management,* Vol. 14, No. 2, (2024). https://doi.org/10.54216/JCIM.140212.

[17] Bhanu D, Santhosh R, “Heterogeneous Wireless Sensor Network Design with Optimal Energy Conservation and Security through Efficient Routing Algorithm,” *Journal of Cybersecurity & Information Management,* Vol. 13, No. 2, (2024). https://doi.org/10.54216/JCIM.130211

[18] Nagaraju R, Goyal SB, Verma C, Safirescu CO, Mihaltan TC, “Secure routing-based energy optimization for IOT application with heterogeneous wireless sensor networks,” *Energies,* Vol. 15, No. 13, (2022), pp. 4777. https://doi.org/10.3390/en15134777.

[19] Qi S, Yang L, Ma L, Jiang S, Zhou Y, Cheng G, “MOMTA-HN: A Secure and Reliable Multi-Objective Optimized Multipath Transmission Algorithm for Heterogeneous Networks,” *Electronics,* Vol.13, No. 14, (2024), pp. 2697. https://doi.org/10.3390/electronics13142697

[20] Thangavelu A, Rajendran P, “Energy-Efficient Secure Routing for a Sustainable Heterogeneous IoT Network Management,” *Sustainability,* Vol. 16, No. 11, (2024), pp. 4756. https://doi.org/10.3390/su16114756.